Nowa polityka społeczna

ZAGROŻENIA CYBERPRZESTRZENI

KOMPLEKSOWY PROGRAM DLA PRACOWNIKÓW SŁUŻB SPOŁECZNYCH

redakcja

Joanna Lizut

Wyższa Szkoła Pedagogiczna

im. Janusza Korczaka w Warszawie

www.wspkorczak.eu

Zagrożenia cyberprzestrzeni

kompleksowy program dla pracowników służb społecznych

Warszawa 2014

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Zagrożenia cyberprzestrzeni

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Rada Programowa: prof. Julian Auleytner, prof. Mirosław Grewiński

Recenzenci: prof. Katarzyna Głąbicka, prof. Arkadiusz Karwacki

Redakcja: Joanna Lizut

Korekta: Danuta Dąbrowska

ISBN: 978-83-61121-80-0

Realizatorzy projektu:

Lider: Wyższa Szkoła Pedagogiczna
im. Janusza Korczaka w Warszawie
ul. Pandy 13, 02–202 Warszawa

Partner: Rezekne Higher Education Institution
Personality Socialization Research Institute (PSRI)
Atbrivosanas 115, LV4600 Rezekne, Latvia

Współpraca:

Naukowa i Akademicka Sieć Komputerowa
ul. Wąwozowa 18, 02–796 Warszawa

Honorowy Patronat Ministra Pracy i Polityki Społecznej

Ministerstwo Pracy i Polityki Społecznej

Publikacja powstała w ramach projektu pt. „PI-PWP Zagrożenia cyberprzestrzeni – nowe kompetencje pracownika socjalnego". Priorytet IX. Rozwój wykształcenia i kompetencji w regionach. Działanie: 9.2 Podniesienie atrakcyjności i jakości szkolnictwa zawodowego. Numer Umowy: UDA-POKL. 09.02.00-14.06211-00. Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.
Publikacja jest dystrybuowana bezpłatnie.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Zagrożenia cyberprzestrzeni

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Spis treści

I

II

III

IV

Table of contents

V

VI

A

O projekcie

O projekcie

Kluczowym celem projektu *Zagrożenia cyberprzestrzeni – nowe kompetencje pracownika socjalnego* jest implementacja innowacyjnego programu kształcenia, który ma za zadanie przygotować pracowników służb społecznych do pracy z osobami i rodzinami potrzebującymi pomocy społecznej w obszarze zagrożeń generowanych przez cyberprzestrzeń. Produkt ma na celu wypełnić lukę w obecnym systemie kształcenia kadr służb społecznych zagadnieniami związanymi z tą tematyką.

Wdrożenie innowacyjnego programu kształcenia wyposaży pracowników służb społecznych w szerszy zasób kompetencji i instrumentów wykonawczych. Projekt przyczyni się do zwiększenia skuteczności realizowanej polityki socjalnej.

OPIS I ZAŁOŻENIA PROJEKTU

WSP im. Janusza Korczaka w Warszawie wyszła z inicjatywą stworzenia innowacyjnego projektu, którego zadaniem jest podniesienie kompetencji pracowników socjalnych oraz zmiana postrzegania tego zawodu również jako bardziej odpowiadającego na zmieniające się potrzeby odbiorców. Dodatkowymi korzyściami wynikającymi z realizacji projektu będzie podniesienie świadomości społecznej na temat:

- zagrożeń stwarzanych przez media cyfrowe i technologie informacyjno-komunikacyjne,
- zagrożeń społecznych, wychowawczych, zdrowotnych, moralnych mających miejsce w cyberprzestrzeni.

Tematyka zagrożeń powodowanych przez cyberprzestrzeń, a szczególnie krzywdzenia przy użyciu Internetu, interaktywnych lub cyfrowych technologii, uzależnień od komputera, telefonu, gier oraz wielu innych problemów świata wirtualnego nie jest w wystarczającym stopniu nagłośniona, dlatego świadomość społeczeństwa w tym zakresie nadal jest bardzo niska. Niepokojącym zjawiskiem jest, że rodzice, opiekunowie, nauczyciele oraz osoby pełniące ważne role społeczne, w tym pracownicy socjalni nie posiadają odpowiedniej wiedzy, w jaki sposób rozpoznawać takie problemy jak uzależnienie do środków masowego przekazu, manipulacja w sieci, poszywanie się pod kogoś w Internecie, przejmowanie prywatnej treści i zawartości komputera czy kradzież i niekontrolowane wydatki. Co więcej, osoby te nie potrafią w sposób prawidłowy reagować w wypadku pojawienia się symptomów świadczących o tych problemach.

W ramach projektu pracownicy służb społecznych będą mogli wziąć udział w cyklu szkoleń obejmujących następujące zagadnienia:

- zagrożenia zdrowia psychicznego i fizycznego,
- zagrożenia społeczno-wychowawcze,
- zagrożenia związane z uzależnieniami,
- cyberprzestępstwa.

Sugerowane w projekcie założenia są zgodne z tematyką dla projektów innowacyjnych testujących w zakresie modernizacji oferty kształcenia zawodowego pracowników socjalnych. Poza wzmocnieniem kompetencji zawodowych pracowników socjalnych, realizacja projektu wywrze wpływ na modyfikację kierunków i specjalności na uczelniach humanistycznych i społecznych, zwłaszcza pedagogicznych kształcących służby społeczne.

Innowacyjność projektu

Dotychczas brakowało kompleksowych rozwiązań dotyczących profilaktyki i przeciwdziałania zagrożeniom, jakie niesie za sobą informatyzacja większości dziedzin współczesnego życia.

Projekt będzie uwzględniał komponent ponadnarodowy, zwłaszcza w zakresie rozwiązań prowadzonych w kraju partnera, czyli na Łotwie i możliwości ich upowszechniania na polskim gruncie.

Ostatecznym produktem projektu będzie program wydany w formie publikacji, w wersji papierowej oraz elektronicznej. To nowoczesne narzędzie w systemie kształcenia na odległość, oferowane przez WSP im. Janusza Korczaka w Warszawie będzie udostępniane

w ramach oferty edukacyjnej i kursów dla pracowników socjalnych. Grupa docelowa zostanie wyposażona w nowe narzędzia i nowe metody działania, co pozwoli na nabycie wielu nowych umiejętności. Oprócz tego realizacja projektu przyczyni się do wypełnienia luki w zapotrzebowaniu na profesjonalnie przygotowanych pracowników socjalnych.

Produkt finalny będzie opierał się na doświadczeniu specjalistów biorących udział w projekcie, ich wiedzy merytorycznej, jak również uwagach zgłaszanych przez grupę docelową. Głównym założeniem innowacyjnego projektu jest to, że finalne rezultaty zostaną wykorzystane w praktyce. Co więcej, produkt może przyczynić się do zwiększenia skuteczności realizowanej polityki socjalnej w Polsce i na Łotwie.

Adresaci projektu
Grupa docelowa zostanie podzielona na **użytkowników** i **odbiorców**.

Użytkownicy otrzymają nowe narzędzia, które będą mogli wykorzystać w swojej pracy w postaci innowacyjnego programu edukacyjnego w wersji papierowej i elektronicznej. Odbiorcy, czyli osoby pracujące w zawodzie pracownika socjalnego, dzięki nowej metodzie będą mogły rozwiązać swoje problemy w obszarze niemożności zaoferowania dostatecznych rozwiązań pomocowych osobom, które doświadczyły problemów stwarzanych przez media cyfrowe i technologie informacyjno-komunikacyjne.

Realizatorzy projektu
Realizatorami projektu *Zagrożenia cyberprzestrzeni – nowe kompetencje pracownika socjalnego* są Wyższa Szkoła Pedagogiczna im. Janusza Korczaka w Warszawie oraz Rezekne Higher Education Institution na Łotwie.

Wyższa Szkoła Pedagogiczna im. Janusza Korczaka w Warszawie jest jedną z najstarszych uczelni niepublicznych w Polsce. W ciągu 20-letniej historii istnienia, uczelnia utworzyła sześć placówek na terenie całego kraju. WSP im. Janusza Korczaka edukuje w obszarze szeroko pojętych nauk społecznych. Ponadto uczelnia oferuje krótkie formy kształcenia kierowane do osób dorosłych, seniorów, jak również młodzieży i dzieci w wieku szkolnym.

W swoje bogatej ofercie edukacyjnej WSP im. Janusza Korczaka proponuje naukę na czterech kierunkach studiów: pedagogika, politologia, filologia angielska i praca socjalna. Wszystkie kierunki studiów są dostępne również w formie Kształcenia na Odległość (KnO).

Misją uczelni jest kształcenie ustawiczne. Programy nauczania, jak również odpowiednio dobrane metody dydaktyczne mają na celu wykształcić otwartych i kreatywnych humanistów, którzy dostrzegają i rozumieją rzeczywistość publiczną, społeczną i gospodarczą. System dydaktyczny i naukowy opiera się na **wspólnych** wartościach, takich jak:
- równość w dostępie do wykształcenia,
- sprawiedliwe traktowanie,
- indywidualne podejście do studenta.

Partnerem Wyższej Szkoły Pedagogicznej im. Janusza Korczaka w Warszawie w projekcie innowacyjnym z komponentem ponadnarodowym jest Rezekne Higher Education Institution.

Rezekne Higher Education Institution (RHEI) jest wyższą instytucją naukową na Łotwie, która nie tylko kształci studentów, ale również angażuje się w badania i twórczość artystyczną. Uczelnia została utworzona w 1993 roku, na podstawie oddziałów Uniwersytetu Łotwy i Technicznego Uniwersytetu w Rydze. RHEI posiada duże doświadczenie w realizacji projektów dotyczących kształcenia zawodowego i ustawicznego.

Najważniejszym celem RHEI jest zapewnienie profesjonalnej edukacji wyższej zgodnie z poziomem rozwoju nauki i tradycjami kulturalnymi Łotwy. Zasady, którymi kieruje się uczelnia to:
- wolność pracy akademickiej oraz naukowej dla nauczycieli akademickich i studentów,
- wolny wybór dotyczący programów studiów, metod nauczania i tematów badań naukowych,
- wolność w wyrażaniu stanowisk naukowych i wyników badań, bez cenzury, pod warunkiem, że ta wolność nie jest sprzeczna z normami moralnymi, nie narusza praw innych osób i jest zgodna z prawem Republiki Łotewskiej.

Wstęp

1 Żyjemy w świecie, w którym media i nowe technologie w znaczący sposób wpływają na funkcjonowanie społeczeństwa. Możemy znacznie łatwiej się komunikować, korzystać z informacji, mieć dostęp do wiedzy. Jednocześnie musimy dostrzegać problemy związane z korzystaniem z nowoczesnych osiągnięć technologicznych. Przede wszystkim komunikowanie się przez Internet sprawia, iż zmieniają się tradycyjne postacie zagrożeń. Obserwujemy powstanie nowych patologii społecznych, dysfunkcji oraz problemów, zwłaszcza rodziny. Jednocześnie pojawiają się nowe kwestie społeczne, mające ścisły związek ze specyfiką świata wirtualnego. Nie tylko osoby młode, ale i starsze spędzają coraz więcej czasu w wirtualnej przestrzeni. Członkowie różnych grup społecznych są narażeni na uzależnienie się od najnowszych technologii, na to, że staną się ofiarami przestępstw takich jak kradzież informacji, fałszerstwo, hacking, cyberbulling i infoholizm. Nieodzowna jest zmiana podejścia do profilaktyki zagrożeń stwarzanych przez świat wirtualny. Tematyka zagrożeń powodowanych przez cyberprzestrzeń, a szczególnie krzywdzenia innych przy użyciu Internetu, interaktywnych lub cyfrowych technologii; uzależnień od komputera, telefonu, gier oraz wielu innych problemów świata wirtualnego nie jest w wystarczającym stopniu nagłośniona, dlatego świadomość społeczeństwa w tym zakresie nadal jest bardzo niska. Niepokojącym zjawiskiem jest fakt, że rodzice, opiekunowie, nauczyciele oraz osoby pełniące ważne role społeczne, w tym pracownicy socjalni, nie mają odpowiedniej wiedzy, w jaki sposób rozpoznawać takie problemy jak uzależnienie od środków masowego przekazu, manipulacja w sieci, podszywanie się pod kogoś w Internecie, przejmowanie prywatnej treści i zawartości komputera czy kradzież i niekontrolowane wydatki.

2 Wskazane wyżej zagadnienia pozostają w kręgu zainteresowań wielu nauk społecznych. Sam termin „cyberprzestrzeń", choć po raz pierwszy został użyty w powieści science fiction[1], dziś znajduje zastosowanie w pedagogice, psychologii, socjologii, w polityce społecznej czy naukach prawnych z naciskiem położonym na szczególnie istotne dla tych dziedzin aspekty. Nie wchodząc w rozważania definicyjne, można przyjąć, iż cyberprzestrzeń[2] jest „zależnym od czasu zbiorem połączonych systemów informacyjnych oraz ludzi/użytkowników wchodzących w interakcję z tymi systemami"[3]. Pola tej nowej przestrzeni działalności człowieka można próbować odnieść do obszarów aktywności charakterystycznych dla świata realnego (por. schemat 1).

Schemat 1. Typologia przestrzeni Internetu

Źródło: M. Szpunar, Przestrzeń Internetu - nowy wymiar przestrzeni społecznej, http://www.magdalenaszpunar.com/_publikacje/2008/przestrzen_internetu.pdf, data dostępu 10.02.2014. s. 3.

3 Choć schemat powyżej porządkuje zależności „świata realnego" i „świta wirtualnego", warto zaznaczyć fakt coraz większego wzajemnego przenikania się tych rzeczywistości.

---

[1] Termin „cyberprzestrzeń" po raz pierwszy użył W. Gibson w 1984 r. w powieści pt. *Neuromancer,* określając ten rodzaj przestrzeni jako „zbiorową halucynację" przeżywaną przez użytkowników wirtualnej, trójwymiarowej przestrzeni elektronicznego medium komunikacyjnego. Autor pisał, że cyberprzestrzeń jest „królestwem przestrzennych paradoksów", gdzie „tam nie ma tam". Wówczas, kiedy stworzył ten neologizm, nie miał ani komputera, ani tym bardziej dostępu do Internetu. Z biegiem czasu termin „cyberprzestrzeń" zaczęto odnosić do rzeczywistych sieci komputerowych.
Cyt. za. M. Berdel-Brudzińska, *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, m.ksiegarnia.lexisnexis.pl/.../pojecie_cyberprzestrzeni_we_wspolczesny, dostęp. 14.02.2014 .

[2] Inne terminy związane to: świat wirtualny, przestrzeń wirtualna, wirtualna rzeczywistość, przestrzeń Internetu.

[3] Definacja Centrum Doskonalenia Cyberobrony NATO: http://www.ccdcoe.org/articles/2010/ Ottis_Lorents_CyberspaceDefinition.pdf, data dostępu 12.11.2013.

4 Podobnie, pojęcia „zagrożenia", „ryzyko", „problem" odnajdujemy właściwie we wszystkich naukach społecznych. Trudno sobie wyobrazić, iż analizując różne aspekty współczesnego społeczeństwa i istniejących w nim kwestii społecznych (również w nowej ich formule związanej z wirtualną przestrzenią) można ograniczyć się wyłącznie do jednej z perspektyw. Dlatego też w opracowaniu odnaleźć można wątki związane z pracami z takich dziedzin jak: pedagogika, socjologia, psychologia, medycyna czy nauki techniczne. W poszczególnych artykułach pojawią się nazwiska m.in. klasyków socjologii takich jak E. Durkheim czy R. Merton, którzy postrzegali problemy społeczne jako efekt zakłóceń ładu społecznego i rezultat napięć społecznych oraz współczesnych autorów - zwłaszcza prace U. Becka, autora koncepcji społeczeństwa ryzyka, niezwykle istotnej dla tej publikacji.

5 W koncepcji niemieckiego socjologa, szczególnie ważne są rozważania poświęcone specyfice współczesnych relacji międzyludzkich, w których dominuje niepewność, zmienność, brak stabilnych fundamentów. Jak podkreśla autor, współczesny ład charakteryzuje indywidualizm, relatywizm, subiektywizm, na które znaczący wpływ ma rozwój technologii, sprzyjających odosobnieniu i osamotnieniu człowieka. Nowa przestrzeń aktywności, jaką jest wirtualny świat, oznacza nową jakość wymiany społecznej i więzi międzyludzkich. Choć zwiększa się sieć kontaktów, nie zawsze wzrasta ich trwałość i stabilność[4].

6 Bardzo trudno jest opisać zależności świata realnego i wirtualnego, nawiązywanych w tych światach, przeplatających się relacji i prowadzonych działań, dziś coraz bardziej światy „prawdziwe i wirtualne zdają się wzajemnie kolonizować i przenikać"[5]. Dla wielu użytkowników nie istnieje granica między tymi dwiema przestrzeniami, gdy równolegle istnieją grupy społeczne całkowicie wyłączone w przestrzeni wirtualnej (tzw. wykluczenie cyfrowe). Sama populacja korzystających z Internetu jest znacząco zróżnicowana. Fakt ten doczekał się już naukowych opracowań.

7 Na gruncie pedagogiki medialnej funkcjonuje typologia M. Prenskey'ego, w której zostały wyróżnione dwie kategorie użytkowników: cyfrowi autochtoni i cyfrowi imigranci. Do pierwszej grupy autor zaliczył wszystkich tych, dla których przestrzeń wirtualna nie jest kolejnym obszarem działań a naturalnym polem ich codziennej aktywności. Cyfrowi autochtoni bez problemu obsługują dostępne urządzenia medialne, z powodzeniem korzystają ze wszystkich dostępnych funkcji a wręcz wymyślają nowe ich zastosowania. Bez lęku i oporów sięgają po nowe technologie, a posiadane urządzenia mobilne traktują jak przedmioty osobiste. Tymczasem cyfrowi imigranci, choć korzystają z nowych technologii, poruszają się w ich świecie zdecydowanie gorzej. Urządzenia mobilne postrzegają analogicznie do sprzętów domowych (jako ułatwienie życia). Często ograniczają się do wykorzystywania podstawowych, standardowych funkcji. Traktują nowe technologie nieufnie[6].

8 Typologia M. Prenskey'ego odnosi się także do obszaru nauczania i komunikacji interpersonalnej, która jest istotnym elementem w relacji pomocy i polem zainteresowania takich dziedzin jak dydaktyka czy edukacja. Cyfrowi autochtoni i imigranci to grupy nastawione na zupełnie odmienne wzorce kształcenia i komunikacji społecznej. Pierwsi przedkładają obraz i dźwięk nad tekst, z którego rozumieniem mają problemy, zwłaszcza jeśli ten jest długi i skomplikowany. Dlatego preferują akcydentalne, krótkotrwałe uczenie się, eksperymentowanie, wielozadaniowość, oczekują szybkich efektów. Drudzy, przeciwnie, przekładają tekst nad obraz, lubią gdy jest on wydrukowany a nie odczytywany z ekranu. Są skłonni długo pracować na określony rezultat, odraczać nagrodę

[4] Por. U. Beck, *Społeczeństwo ryzyka*, Wydawnictwo Naukowe Scholar, Warszawa 2002.

[5] A. Tarkowski, cyt. za. M. Berdel-Brudzińska, *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, m.ksiegarnia.lexisnexis.pl/.../pojecie_cyberprzestrzeni_we_wspolczesny, data dostępu 14.02.2014 .

[6] M. Prenskey, cyt. za. Hojnacki L., *Pokolenie m-learningu – nowe wyzwanie dla szkoły*, „E-mentor", 1(13)/2006., s. 26

w czasie[7]. W tym kontekście ważne jest pytanie o możliwości porozumienia przedstawicieli różnych grup i warunki dla skutecznego niesienia pomocy, jako wyzwania dla działań służb społecznych.

9 W naukach społecznych pojęcie służby społecznej ma różny zakres. W polskiej literaturze naukowej pierwsi stosowali je H. Radlińska i A. Kamiński, którzy uważali, że jest ono synonimem terminu opieka społeczna. J. Rosner natomiast twierdził, że ma ono nieco szerszy zasięg i obejmuje „wszystkie instytucje i organizacje działające na polu polityki społecznej w ścisłym tego słowa znaczeniu, więc bez służby zdrowia, szkół i innych instytucji oświatowych i wychowawczych, instytucji sportowych i rekreacyjnych itp."[8]. Znane są także jeszcze szersze definicje, w których „służbami społecznymi są (…) nazywane zorganizowane, względnie trwałe i wyspecjalizowane zespoły ludzi działające w ścisłym związku lub w ramach pewnych instytucji i organizacji, których zadaniem jest wspomaganie jednostki, rodziny oraz innych grup i zbiorowości w sytuacjach, gdy nie mogą one z powodów subiektywnych lub obiektywnych zaspokoić swoich potrzeb na wystarczającym poziomie lub w zadowalającej formie"[9].

10 We wszystkich zaprezentowanych definicjach centralne miejsce zajmują pracownicy socjalni, jako przedstawiciele zawodu szczególnie nakierowanego na wielowymiarowe wsparcie i pomoc człowiekowi, korzystającego z dorobku wielu dziedzin. Dostrzegając wagę problemu i analizowanych w publikacji zagadnień zakładamy, iż przedstawiciele wszystkich związanych ze wsparciem profesji będą użytkownikami podręcznika, w tym: nauczyciele, dyrektorzy szkół, pracownicy świetlic, poradni psychologiczno-pedagogicznych, policjanci (por. schemat 2).

Schemat 2. Panorama służb społecznych

Źródło: M. Payne, *What is Professional Social Work?*, Policy Press, Bristol 2008, s. 116, cyt. za: A. Olech, *Praca socjalna a inne profesje: punkty styczne i rozłączne*, w: *Pracownicy socjalni i praca socjalna w Polsce, Między służbą społeczną a urzędem*, red. M. Rymsza, Instytut Spraw Publicznych, Warszawa 2011, s. 333.

11 Praca, jaką wykonują przedstawiciele służb społecznych, w tym przede wszystkim pracownicy socjalni, odnosi się do społecznego funkcjonowania jednostki, grupy i środowiska społecznego, nie może zatem pozostać obojętna wobec nowych problemów społecznych. Tymczasem coraz więcej osób, zwłaszcza najmłodszego pokolenia, ma kontakt z nowymi formami zagrożeń i wymaga niesienia adekwatnej pomocy, także świadczonej przez wyspecjalizowane instytucje i organizacje polityki społecznej. Doniesienia z badań wskazują na rosnącą skalę „cyber problemów". Z raportu Dyżurnet.pl, zespołu przyjmującego zgłoszenia o nielegalnych treściach w Internecie, przede wszystkim dotyczących pornografii dziecięcej, wynika, iż „w roku 2013 pracownicy zespołu przeanalizowali 6697 incydentów, co stanowiło wzrost o 25 procent w stosunku do roku poprzedniego. Miesięczna liczba incydentów wyniosła średnio 558, czyli ponad sto więcej w porównaniu z rokiem 2012, kiedy to średnia wynosiła 446 incydentów miesięcznie"[10]. Ryzyko dysfunkcyjnego korzysta-

[7] Tamże.

[8] Takie podejście zastosowano w pierwszej fazie projektu.

[9] B. Szatur-Jaworska, *Teoretyczne podstawy pracy socjalnej*, w: *Pedagogika Społeczna*, red. T. Pilch, I. Lepalczyk, Wydawnictwo „Żak", Warszawa, 2003, str. 118-119.

[10] Por. http://www.dyzurnet.pl/images/stories/PDF/raporty/

nia z Internetu jest zależne od poziomu wiedzy i dbałości osób dorosłych zaangażowanych w ochronę dzieci. Dziś wielu dorosłych, w tym pracowników służb społecznych nie potrafi w sposób prawidłowy reagować w przypadku pojawienia się symptomów świadczących o problemach związanych z cyberprzestrzenią. Choć to najmłodsi użytkownicy są grupą szczególnie narażoną na zagrożenia związane z korzystaniem z komputera i urządzeń mobilnych, warto postrzegać te kwestie szeroko. Mogą one dotyczyć wszystkich użytkowników, bez względu na wiek. Główne znaczenie ma poziom ich wiedzy i umiejętności.

12 Współczesne wyzwania stojące przed pomocą społeczną wskazują na potrzebę wyposażenia pracowników służb społecznych w nowe kompetencje. Odpowiedzią na te potrzeby jest publikacja, którą Państwu przekazujemy – kompleksowy program rozwoju pracowników służb społecznych, która pozwoli skutecznie przygotować ich do pracy z osobami i rodzinami potrzebującymi pomocy społecznej w obszarze zagrożeń generowanych przez cyberprzestrzeń.

13 Opracowanie ma na celu wypełnienie luki w obecnym systemie kształcenia kadr służb społecznych zagadnieniami związanymi z tą tematyką. Opiera się na sprawdzonych teoriach, wynikach badań i zaleceniach ze szczebla administracji centralnej[11] oraz środowiskowej (lokalnej) w zakresie potrzeb kształcenia i doskonalenia specjalistycznych kadr[12].

W ramach publikacji wyodrębniono sześć części obejmujących następujące zagadnienia:

- służby społeczne wobec zagrożeń cyberprzestrzeni,
- zagrożenia zdrowia psychicznego i fizycznego,
- zagrożenia społeczno-wychowawcze,
- zagrożenia związane z uzależnieniami,
- cyberprzestępstwa i nadużycia,
- kształcenie.

14 Przyjęta struktura publikacji pozwala na dostarczenie wiedzy osobom, które zajmują się lub chcą się zajmować kształceniem kadr służb społecznych, obejmując zarówno tematykę zagrożeń cyberprzestrzeni jak i problematykę kształcenia w tym zakresie. Zagrożenia zostały przedstawione w sposób, który nie tylko przybliża charakter zjawiska, jego skalę i częstotliwość występowania, ale również pomaga postawić diagnozę problemu, proponuje procedury wdrożenia pomocy, powołuje się na już istniejące najlepsze praktyki. Każdy z rozdziałów posiada bazę ćwiczeń utrwalających poznaną wiedzę. Dzięki swojej perspektywiczności publikacja pozwala na budowanie programów kształcenia, idealnie dostosowanych do potrzeb konkretnych grup, jednocześnie rekomendując programy szkoleniowe.

15 Należy zatem podkreślić, iż ten nowoczesny program dedykowany pracownikom służb społecznych pozwala zrealizować jednocześnie wszystkie cele procesu kształcenia, takie jak:

- **dostarczanie wiedzy**, dzięki zawartości **merytorycznej** modułów od pierwszego do czwartego, w których w sposób wyczerpujący i przystępny zostały omówione takie zagadnienia jak: cyberprzemoc, uzależnienia od nowych technologii i mediów, pedofilia w sieci, seksting, przestępstwa w sieci i wiele innych;
- wzmocnienie **umiejętności praktycznych**, przede wszystkim poprzez możliwość wykorzystania podczas zajęć zawartych w module szóstym autorskich propozycji ćwiczeń i możliwości odniesienia do przykładów i indywidualnych przypadków;
- **formowanie i promowanie ogólnych kompetencji społecznych** przede wszystkim poprzez wzmacnianie umiejętności związanych z rozwiązywaniem konfliktów i radzeniem

raport_2013.pdf, dostęp 28.02.2014 , s. 11.

[11] *Rządowy Program Ochrony Cyberprzestrzeni RP* (2010) proponuje nowe działania społeczno-profilaktyczne w edukacji dla bezpieczeństwa w cyberprzestrzeni, zaś *Polityka Bezpieczeństwa Cyberprzestrzeni RP* (2012) kładzie nacisk na racjonalizację programów kształcenia studentów i doskonalenia kwalifikacji specjalistycznych.

[12] Badanie ilościowe zostało przeprowadzone w woj. mazowieckim w ramach projektu *PI-PWP Zagrożenia cyberprzestrzeni – nowe kompetencje pracownika socjalnego*, M. Jóźko, *Diagnoza i analiza pracowników instytucji kształcących i szkolących kadry służb społecznych, w tym pracowników socjalnych*, Lokalne Badanie Społeczne, Warszawa 2012.

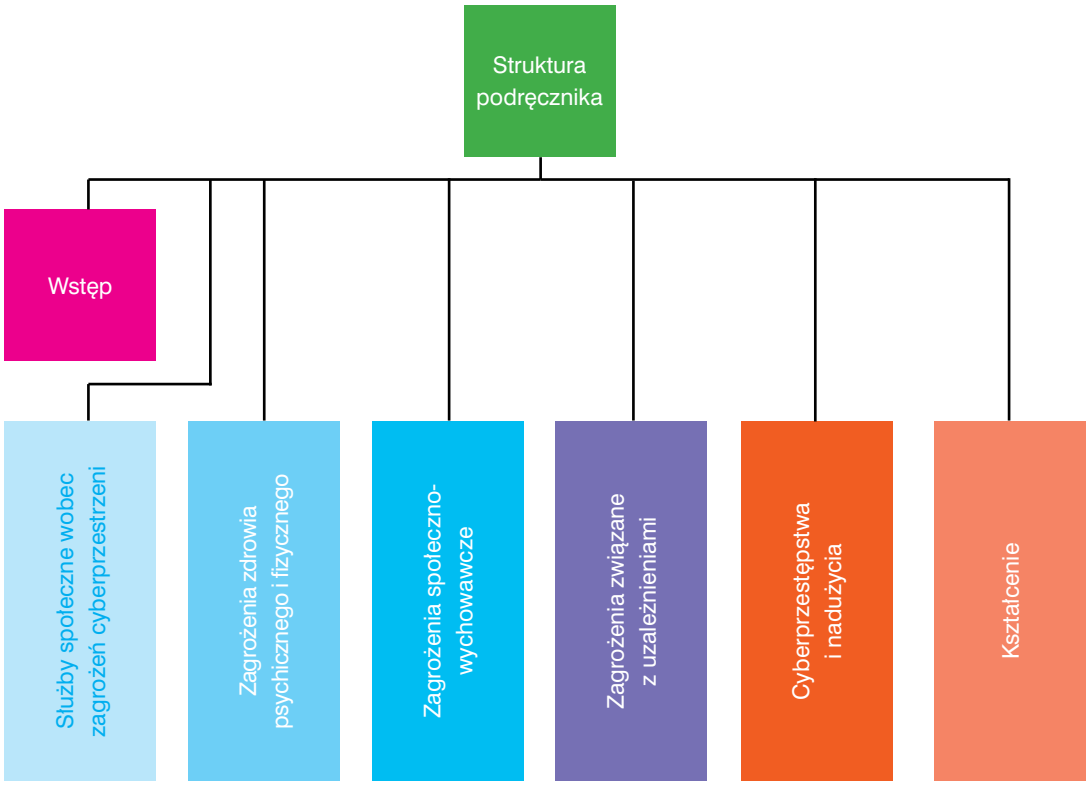
sobie w sytuacjach trudnych (moduł szósty kształcenie).

Ponadto załączniki – pomocniczo, wskazując instytucje i prawne podstawy odnoszące się do zagrożeń cyberprzestrzeni – wzmacniają znajomość treści z zakresu systemu wsparcia osób dotkniętych problemami związanymi ze światem wirtualnym.

10 Publikacja w sposób kompleksowy odpowiada na potrzeby kształcenia i doskonalenia kadr, obejmując obszary: zdrowotne, społeczne, wychowawcze, psychologiczne, technologiczne i prawne zagrożeń generowanych przez cyberprzestrzeń. Interdyscyplinarność opracowania polegająca na połączeniu zagadnień z zakresu polityki społecznej, pracy socjalnej, pedagogiki z innymi obszarami, jakimi są informatyka, prawo telekomunikacyjne, technika, w skuteczny sposób odpowiada na potrzeby użytkowników. Tak skonstruowany program i przyjęty sposób prezentacji materiału pozwoli nauczycielom szeroko wykorzystywać program edukacyjny oraz stworzy możliwość samokształcenia samym pracownikom służb społecznych i innych odbiorców zainteresowanych tymi zagadnieniami.

Joanna Lizut

Schemat 3.
Struktura podręcznika



Źródło: opracowanie własne

ROLA I MIEJSCE
NOWYCH ZAGROŻEŃ CYBERPRZESTRZENI I ŚWIATA WIRTUALNEGO W KONTEKŚCIE POLITYKI SPOŁECZNEJ

Józef Bednarek

1 WPROWADZENIE

Najnowsze przemiany informacyjno-komunikacyjne i edukacyjne są, i w jeszcze większym stopniu muszą być, przedmiotem badań, kształcenia i doskonalenia kompetencji pracowników socjalnych oraz przedstawicieli innych instytucji, zwłaszcza polityki społecznej, funkcjonujących w przestrzeni społecznej i internetowej.

2 Obecnie pojawia się szczególna potrzeba poszerzenia wiedzy każdego z nas jako członków społeczeństwa, w szczególności jednak specjalistów kształconych dla potrzeb cyfrowej szkoły oraz jej absolwentów.

3 CYFROWA SZKOŁA

Wprowadzenie szkoły cyfrowej wynika z potrzeby minimalizowania luki, jaka pojawiła się pomiędzy tradycyjną i konwencjonalną edukacją, a wprost wykładniczo rozwijającymi się najnowszymi technologiami informacyjno-komunikacyjnymi i mediami cyfrowymi oraz ich nowymi szansami wdrażania i zastosowania w kształceniu. Nie bez powodu już w 2008 r. w „Strategii rozwoju społeczeństwa informacyjnego”[1] podkreślono, że do 2013 r. pojawi się wizja społeczeństwa informacyjnego w Polsce jako: „aktywnego społeczeństwa osiągającego wysoką jakość życia w perspektywie osobistej i społecznej. Jej urzeczywistnienia upatruje się w realizacji trzech następujących kierunków strategicznych w obszarach: człowiek, gospodarka i państwo:

- Człowiek: Przyśpieszenie rozwoju kapitału intelektualnego i społecznego Polaków dzięki wykorzystaniu technologii informacyjnych i komunikacyjnych.
- Gospodarka: Wzrost efektywności, innowacyjności i konkurencyjności firm, a tym samym polskiej gospodarki na globalnym rynku oraz ułatwienie komunikacji i współpracy między firmami dzięki wykorzystaniu najnowszych ww. technologii.
- Państwo: Wzrost dostępności i efektywności usług administracji publicznej przez wykorzystanie technologii ww. do przebudowy procesów wewnętrznych administracji i sposobu świadczenia usług”[2].

4 W ostatnich dokumentach normatywnych Unii Europejskiej i Polski podkreśla się pilną konieczność podejmowania działań mających optymalizować poszukiwanie racjonalnych rozwiązań w tym obszarze.

6 Główna teza podejmowanych rozważań została sformułowana w postaci stwierdzenia: szkoła cyfrowa jest i musi być nowym przedmiotem kształcenia i wielu badań prowadzonych w naukach ścisłych, zwłaszcza informatyce, technologiach informacyjnych, ale także naukach społecznych, zwłaszcza pedagogicznych, w których akcentuje się szanse i zagrożenia stwarzane przez cyberprzestrzeń.

Do zasadniczych przesłanek wskazujących na potrzebę przygotowania tego opracowania dla potrzeb instytucji polityki społecznej i pracowników socjalnych zaliczyć należy:

- **naukowe** – wzbogacenie teorii i praktyki edukacyjnej, zwłaszcza kształcenia na wszystkich jego poziomach, oraz modyfikacja dotychczasowych, tradycyjnych rozwiązań oświatowych i w badaniach na temat cyfrowej szkoły, w których w coraz większym stopniu stosuje się powszechnie wdrażane technologie informacyjne[3];

1 Strategia rozwoju społeczeństwa informacyjnego, szs.mac.gov.pl, data dostępu 13.02.2014.

2 *Społeczeństwo informacyjne w liczbach, rok 2013*, Wyd. Departament Społeczeństwa Informacyjnego Ministerstwa Administracji i Cyfryzacji, Warszawa 2013, s. 7.

3 Badania społeczne nt. *Komponent badawczy rządowego programu CYFROWA SZKOŁA*, na zlecenie

- **cywilizacyjne** – związane z przemianami i istotnym wzrostem znaczenia wiedzy (informacji) w procesie globalizacji oraz z wejściem Polski do Unii Europejskiej. Media będące podstawą funkcjonowania społeczeństwa wiedzy są dziś wszechobecne;
- **informacyjne** – ich istota wiąże się z potrzebą natychmiastowej dostępności za pośrednictwem mediów cyfrowych do wiedzy (informacji) ogólnej i specjalistycznej stającej się coraz silniejszym wyznacznikiem postępu, rozwoju społeczno-ekonomicznego i statusu każdego człowieka;
- **komunikacyjne** – największy i najważniejszy przełom edukacyjny, łączący się z mediami interaktywnymi, Internetem, telewizją cyfrową, telefonią komórkową;
- **informatyczne** – wyrażają się w dynamicznym rozwoju mediów interaktywnych i coraz doskonalszych technologii, które stają się powszechnymi narzędziami współczesnej edukacji, zwłaszcza doskonalenia ogólnego i zawodowego oraz zdobywania nowych kompetencji;
- **społeczne** – zmienia się tradycyjna struktura społeczna, relacje społeczne, realizowane zadania, nakładają się na siebie kultury słowa mówionego oraz drukowanego, audiowizji i multimedialności oraz interakcyjności, cyberprzestrzeni i świata wirtualnego, a także systemów automatyki i robotyki, a dostęp do technologii informatycznych pozwala na doskonalenie kwalifikacji osób dorosłych poprzez innowacyjne rozwiązania;
- **ekonomiczne** – coraz więcej osób zajmuje się wiedzą i informacją, dotyczy to również różnorodnych usług informacyjno-komunikacyjnych, telepracy, gospodarki cyfrowej, e-administracji, e-usług, niestandardowych form zatrudnienia zmieniających filozofię i wyzwania dotychczasowego kształcenia studentów i doskonalenia zawodowego. Powstają nowe specjalności i specjalizacje związane z mediami cyfrowymi i technologiami informatycznymi, a także działalnością różnorodnych instytucji o takim charakterze;
- **pedagogiczne** – każdy nauczyciel, pedagog, wykładowca, kierownik (dyrektor) czy jakikolwiek przełożony ma większe możliwości kształtowania postaw, doskonalenia umiejętności i przekazywania wiedzy. Także uczeń coraz częściej korzysta z dostępu do nowych źródeł wiedzy;
- **dydaktyczne** – następuje zmiana roli nauczyciela we współczesnej szkole (uczelni), której charakter także się zmienia z klasycznego na cyfrowy.

7 Podsumowując, poza wymienionymi przesłankami, istnieje jeszcze wiele innych, chociażby historyczne, antropologiczne, kulturowe, ideologiczne, polityczne, kulturalne, etyczne, prawne, zdrowotne, profilaktyczne, resocjalizacyjne. Wszystkie one determinują nie tylko kolejne przemiany, ale i konieczność różnorodnych działań związanych z potrzebą wprowadzania szkoły cyfrowej, także związanych z ww. obszarami.

8 Powyższe przesłanki wskazują na wyjątkowo wielkie i dynamicznie przemiany, mające określone implikacje społeczno-edukacyjne, w których wykładniczo istotne jest znaczenie informacji i wiedzy oraz najnowszych technologii stanowiących podstawę tworzenia cyfrowej szkoły. One też, przedstawione w sposób bardzo ogólny, mają swoje podstawy teoretyczne związane z wieloma obszarami wiedzy społecznej, humanistycznej, pedagogicznej, psychologicznej, socjologicznej, etycznej oraz informatycznej i medialnej, jak również innych dyscyplin. **Stanowią one wielkie wyzwanie dla realizowanej polityki społecznej i konkretnych działań pracowników służb społecznych**.

MAiC zostało przeprowadzone wśród uczniów klas IV roku szkolnego 2012/213.

1 OGÓLNA CHARAKTERYSTYKA ZAGROŻEŃ

Problematyka wyzwań cywilizacyjnych, społeczno-kulturowych, edukacyjno-wychowawczych i wielu innych nigdy dotąd nie była tak ważna, jak obecnie. Ich znaczenie i miejsce wynika z wyjątkowej dynamiki różnorodnych przemian, zwłaszcza informacyjno-technologicznych. Z tego powodu podejmowane zagadnienia są przedmiotem zainteresowania przedstawicieli wszystkich dyscyplin naukowych, poszczególnych środowisk akademickich, nauczycieli i pedagogów oraz wielu innych specjalistów związanych z profilaktyką, diagnozą i terapią oraz legislacją. Są one także podstawą doskonalenia różnorodnych teorii, koncepcji, głoszonych idei, przyjmowanych strategii, raportów, dyrektyw, a także założeń kształcenia w postaci planów i programów oraz działalności naukowo-badawczej środowisk akademickich. Stanowią bogaty obszar refleksji teoretycznej i powstających koncepcji oraz jednocześnie działań praktycznych realizowanych przez nauczycieli. Wynikają one z nowych wyzwań multimedialnego kształcenia ustawicznego.

2 **Czym zatem jest wyzwanie**? Nie ma jednoznacznego określenia tego pojęcia. Każdy badacz, bez względu na dyscyplinę naukową, różnorodne uwarunkowania, ideologię i światopogląd, inaczej będzie je określał i definiował. **Można jednak przyjąć, że wyzwanie jest pewną wizją bliższej i dalszej przyszłości. Jest także rodzajem szczególnego nacisku na teorie i każde działanie (praktykę) w celu podejmowania konkretnej działalności przez społeczeństwo międzynarodowe, regionalne, lokalne, środowiskowe i poszczególne osoby, ale przede wszystkim instytucje naukowo-badawcze, środowiska akademickie i edukacyjne odpowiedzialne za kształcenie, także ustawiczne, każdego człowieka**.

3 Komitet Nauk Pedagogicznych Polskiej Akademii Nauk systematycznie podejmuje analizy tradycyjnych i nowych problemów, których trafna diagnoza daje szansę znalezienia właściwych rozwiązań i poprawy stanu rzeczy[4]. W wypadku zaś nauczania-uczenia się, na podstawie głównych trendów światowych, a także dotychczasowych reform edukacyjnych[5] oraz najnowszych wyzwań wprowadza się nowe podstawy programowe[6] w celu jak najlepszego przygotowania najmłodszych pokoleń do nowych wyzwań, związanych z dalszymi studiami czy też pracą zawodową. Uwaga ta dotyczy w sposób szczególny pracowników służb społecznych, w tym pracowników socjalnych, funkcjonujących w przestrzeni społecznej i stykających się z problemami cyfrowego społeczeństwa.

4 W tym miejscu należy podkreślić, że współczesny świat, jego rozwój i funkcjonowanie w nim człowieka zmieniły się na niespotykaną skalę. Dynamika tych przeobrażeń, w każdej dziedzinie, będzie jeszcze większa, powszechna, ale też nie w pełni przewidywalna. Jej przyczyną są najnowsze media cyfrowe i technologie informacyjno-telekomunikacyjne. To one, w jeszcze większym stopniu niż w poprzednich wiekach, powodują chaos aksjologiczny, zjawisko globalizacji i nie-

[4] Por. m.in. T. Lewowicki (red.), *Gorące problemy edukacji w Polsce*, Komitet Nauk Pedagogicznych Polskiej Akademii Nauk i WSP ZNP, Warszawa 2007.

[5] Cz. Kupisiewicz, *Projekty reform edukacyjnych w Polsce. Główne tezy i wpływ na funkcjonowanie szkolnictwa*, seria Krótkie wykłady z pedagogiki, Wyd. Naukowe PWN, Warszawa 2006; Cz. Kupisiewicz (red.), M. Kupisiewicz (współpraca), R. Nowakowska-Siuta, *Drogi i bezdroża polskiej oświaty w latach 1945—2005. Próba wybiórczo-retrospektywnego spojrzenia*, Komitet Prognoz „Polska 2000 Plus" przy Prezydium PAN, Warszawa 2005.

[6] Od września 2009 r. wprowadzono nowe podstawy programowe wychowania przedszkolnego oraz kształcenia ogólnego w szkołach podstawowych, gimnazjach i liceach. W tym też roku pojawiła się ośmiotomowa publikacja na temat tej podstawy.

pewności, szybkie przenikanie różnych informacji, trudności w adaptowaniu się ludzi do nowych wyzwań, rodzenie się nowych zagrożeń, jakże odmiennych od dotychczasowych, z którymi w przeszłości też sobie człowiek nie radził. Nie bez powodu liczni badacze wszystkich dyscyplin naukowych tego obszaru wiedzy podkreślają znaczenie tych nowych problemów. Wszystkie raporty i inne dokumenty mające charakter strategii, projektów i deklaracji akcentują ich znaczenie. Najnowszy raport „Polska 2030" podkreśla, że coraz ważniejsze jest uczenie się przez całe życie i we wszystkich obszarach. Nowego wymiaru nabiera zatem kształcenie ustawiczne nie tylko studentów, ale i każdego człowieka w każdym okresie jego rozwoju, a więc przez całe życie (etap edukacji szkolnej, równoległej i dorosłych). Trwałe miejsce w tym rozwoju mają media cyfrowe, a tendencje w tym zakresie wskazują, że ich rola w przygotowaniu studenta i nauczyciela, w tym także akademickiego, do twórczej aktywności zawodowej systematycznie i coraz bardziej dynamicznie będzie rosła.

5 Dynamikę rozwoju tego społeczeństwa potwierdzają nowe cywilizacyjne przemiany ilościowe i jakościowe. Są one związane z przemianami i istotnym wzrostem znaczenia wiedzy (informacji) w procesie globalizacji oraz z wejściem Polski do Unii Europejskiej. Media cyfrowe stanowią podstawę funkcjonowania społeczeństwa już nie tylko informacyjnego – ale, co ważniejsze – społeczeństwa wiedzy. Stają się one trwałym elementem funkcjonowania każdej rodziny i innych instytucji edukacyjnych, aktywności społeczno-zawodowej, kultury i wypoczynku. One też dokonały największego przełomu w rozwoju cywilizacyjnym – żadne inne wydarzenie w przeszłości, w tak istotnym stopniu i tak szybko nie wpłynęło na życie, edukację i pracę ludzi na całym świecie. Można stwierdzić, że dziś nie ma odwrotu od cyfrowej cywilizacji.

Nowa rola i miejsce edukacji cyfrowej wyraża się w potrzebie zapewnienia natychmiastowej dostępności za pośrednictwem mediów cyfrowych do wiedzy (informacji) ogólnej i specjalistycznej stającej się coraz silniejszym wyznacznikiem postępu, rozwoju społeczno-ekonomicznego i statusu każdego człowieka, ale także korzystania przez niego z ich możliwości. Dostęp do wiedzy i możliwości jej przetwarzania oraz upowszechniania determinuje społeczne i ekonomiczne powodzenie jednostki. Umożliwia bowiem ustawiczne doskonalenie kwalifikacji ogólnych i specjalistycznych. W wydanych ostatnio monografiach i innych opracowaniach podkreśla się znacznie szerszy kontekst społeczeństwa wiedzy i jej społeczno-edukacyjnych wyzwań, zaś w pozycjach wydanych we wcześniejszych latach, a dotyczących mediów akcentuje się rolę techniki i technologii, następnie informatyki czy Internetu. Dynamika nowych przemian jest potwierdzana w przyjmowaniu nowych określeń w ostatnich kilkudziesięciu latach tego społeczeństwa i jego zróżnicowanych charakterysty.

6 Obecnie można przyjąć, że pojęcie społeczeństwo informacyjne, a ostatnio społeczeństwo wiedzy, to nowe społeczeństwo korzystające z zasobów naukowych i edukacyjnych wszystkich obszarów wiedzy, znajdujących zastosowanie także w kształceniu uczniów zdolnych i niepełnosprawnych[7], ale też wykluczonych społecznie i starszych. Najnowsze technologie nie tylko zmieniają funkcjonowanie człowieka, ale również relacje społeczne. A więc nie bez powodu pojęcie społeczeństwa informacyjnego zostało wprowadzone przez ekonomistów i socjologów z zamia-

[7] Por. J. Łaszczyk (red.), *Komputer w kształceniu specjalnym: wybrane zagadnienia*, WSiP, Warszawa 1998; J. Łaszczyk M. Jabłonowska (red.), *Uczeń zdolny wyzwaniem dla współczesnej edukacji*, Wyd. APS, Warszawa 2008; J. Bednarek, *Społeczeństwo informacyjne i media w opinii osób niepełnosprawnych*, Wyd. APS, Warszawa 2005.

rem scharakteryzowania nowego statusu ogólnoludzkiej społeczności.

Społeczeństwo informacyjne charakteryzuje się więc:

- wysokim stopniem korzystania z wiedzy i informacji w życiu codziennym;
- użytkowaniem jednorodnej lub kompatybilnej technologii informacyjnej na użytek potrzeb własnych i społeczno-ekonomicznych;
- umiejętnością przekazywania, odbierania, a także szybszej wymiany danych cyfrowych bez względu na odległość;
- w dziedzinie ekonomicznej dotychczasowe postacie produkcji zostają zastąpione podstawowym towarem, jakim jest wiedza i informacja, a te są najważniejsze w gospodarce cyfrowej[1]. Powyższym wymogom powinna sprostać nie tylko edukacja medialna, ale i edukacja cyfrowa.

7 Uogólniając liczne definicje oraz powyższe określenia można stwierdzić, że społeczeństwo informacyjne to nowy twór społeczny, charakteryzujący się szybkim rozwojem technologii teleinformatycznych, umożliwiających komunikację i dostęp do informacji na bardzo szeroką, niespotykaną dotychczas skalę. Społeczeństwo radykalnie się zmienia w kierunku jeszcze większej mobilności, utechnicznienia, uinformacyjnienia i usieciowienia.

8 Nowe wyzwania społeczno-edukacyjne wiążą się z nadaniem nowej roli i miejsca aktywnemu funkcjonowaniu człowieka w cyberprzestrzeni. Do charakterystycznych aktywności i cech społeczeństwa wiedzy można zaliczyć m.in.:

1) czas wolny dzieci, bawiących się gadżetami elektronicznymi i grami komputerowymi;

2) kształcenie, w którym obok tradycyjnego nauczyciela, wykorzystuje się Internet, edukację na odległość, aplikacje multimedialne;

3) pracę, realizowaną w cyberprzestrzeni, e-biznes, e-administrację, e-usługi, pozwalające na niestandardowe i elastyczne formy zatrudnienia i aktywności zawodowej, do czego wykorzystuje się tworzenie informacji, jej przetwarzanie i wykorzystanie;

4) produkcję, a w niej: rozwój sektora ICT, wzrost jego znaczenia w funkcjonowaniu pozostałych branż, w tym także wzrost wydatków inwestycyjnych na najnowsze technologie, serwicyzację i cyfryzację gospodarki i usług teleinformatycznych;

5) kulturę i sztukę globalną, multimedialną i wirtualną o charakterze globalnym, a w nowej ekspresji artystycznej wykorzystuje się techniki informacyjne;

6) sieciowość, dla której charakterystyczne są: sieć jako model współczesnego społeczeństwa i powstanie społeczności wirtualnych.

9 Rewolucja informatyczna i rodzące się społeczeństwo wiedzy stały się zjawiskiem globalnym, wywierającym wpływ na wszystkie sfery życia społecznego, w tym także kształcenie i wychowanie, które bezwzględnie musi uwzględniać nowe wyzwania. Wskazuje się wiele zaleceń i sugestii dotyczących kierunków, metod i środków naprawy polskiej oświaty, uwzględniających także przemiany informacyjno-informatyczne. To właśnie badania i edukacja stymulują skalę i jakość różnorodnych przeobrażeń

[8] Por. M. Goliński, *Społeczeństwo informacyjne – geneza koncepcji i problematyka pomiaru,* Oficyna Wydawnicza SGH, Warszawa 2011.

społeczno-ekonomicznych. Są przyczyną wielu nowych problemów, które nie tylko stwarzają nowe możliwości, ale i zagrożenia.

10 J. Morbitzer stwierdza m.in. „Dzięki nowoczesnym mediom elektronicznym pokonaliśmy czas i przestrzeń (choć wszystko zaczęło się od telegrafu, który słusznie jest nazywany „wiktoriańskim Internetem"), co przyniosło rozległe konsekwencje, zarówno w wymiarze pozytywnym, jak i negatywnym. Jesteśmy świadkami głębokich przemian kulturowych, wszyscy też doświadczamy coraz bardziej zjawiska braku czasu – tak dalece, że powszechną dolegliwością staje się prokrastynacja – odkładanie czynności i zadań na później. W efekcie więc – dodaje J. Morbitzer – przestajemy nadążać za zmianami, które przecież sami generujemy – szkołę nazywamy konserwatywną, a my nie czujemy się komfortowo, w tym nadmiernie szybko się zmieniającym świecie, który światowej sławy polski socjolog Zygmunt Bauman nazwał „płynną nowoczesnością"[9].

11 M. Tanaś przytacza argumenty przemawiające za wykorzystaniem komputerów w nauczaniu. Zalicza do nich: „wzrost efektów kształcenia, zaangażowanie sfery emocjonalno-wolicjonalnej, polisensoryczność, multimedialność, interaktywność, symulacyjność, komunikacyjność, podatność na edycję i multiplikację, wizualizację"[10]. Z tych też powodów uczenie się za pomocą komputera przynosi wiele korzyści. Jedną z nich jest zwiększenie efektywności samokształcenia, które jest niezbędne do prawidłowego funkcjonowania w zmieniającej się rzeczywistości. Szkoła nie może być tylko miejscem przekazywania gotowej wiedzy, jej zadaniem jest także wyrobienie w uczniach umiejętności samodzielnego poszukiwania informacji i ich oceny. Ponadto dzięki komputerowi możemy zaprezentować uczniom procesy lub zjawiska, które są niemożliwe do zaobserwowania w naturalnym środowisku, gdyż zachodzą zbyt wolno lub zbyt szybko. Komputery mogą być użytkowane jako środek pomagający nauczycielowi w nauczaniu, uczniowie zaś mogą je wykorzystywać w procesie uczenia się, zarówno w klasie podczas wykonywania ćwiczeń pod nadzorem nauczyciela, jak i poza szkołą.

12 Wśród wielu korzyści zastosowania mediów, a w szczególności komputera, w kształceniu, A. Hankała wymienia:

1) możliwość indywidualizowania przebiegu uczenia się zachodzącego w toku nauczania, a więc dostosowanie jego tempa i zakresu do możliwości ucznia;

2) uzyskanie natychmiastowej informacji zwrotnej w toku uczenia się, co wpływa na utrzymanie motywacji do nauki;

3) szybkie wykrycie słabych i mocnych stron ucznia;

4) stwarzanie warunków do opanowania ćwiczeń i umiejętności, od prostych do złożonych, obejmujących rozwiązywanie problemów[11].

13 Z powyższej analizy wyzwań wynika, że przedmiotem dalszej ana-

[9] J. Morbitzer Przedmowa w: Morbitzer, E. Musiał (red.) *Człowiek, Media, Edukacja*, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie, Kraków 2012, s. 1.

[10] M. Tanaś, *Media w katalogu środków dydaktycznych,* w: B. Siemieniecki (red.), *Pedagogika medialna,* Wyd. Naukowe PWN, Warszawa 2007, s. 164–165.

[11] Por. A. Hankała, *Psychologiczne i społeczne zagrożenia związane z zastosowaniem mediów i technologii informacyjnej w edukacji,* w: M. Tanaś (red.), *Pedagogika @ środki informatyczne i media*, WSP ZNP, Warszawa 2004, s. 73–74.

lizy należy uczynić dwa kolejne rozważania.

14 NOWY PRZEDMIOT I CEL KSZTAŁCENIA ORAZ BADAŃ EDUKACJI CYFROWEJ

Nowy przedmiot i cel badań wynika z kilku najważniejszych powodów, mających istotne znaczenie dla wyjątkowego i interdyscyplinarnego obszaru globalnych przemian. Ich wyszczególnienie i krótka interpretacja są ważne ze względu na wielowymiarowy kontekst teoretyczny skłaniający do refleksji pedagogicznych, jak i innowacyjnych działań edukacyjnych jednostki i społeczeństwa.

15 Naukowy kontekst polega nie tylko na wzbogaceniu teorii i praktyki edukacyjnej, zwłaszcza kształcenia ustawicznego, ale także na potrzebie modyfikacji dotychczasowych, tradycyjnych rozwiązań badawczych, edukacyjnych, oświatowych i komunikacyjnych, w których w coraz większym stopniu stosuje się powszechnie wdrażane media cyfrowe i interaktywne technologie informacyjne. Można zakładać, że dalsze badania empiryczne, zarówno ilościowe, jak i jakościowe, także w sieci, nad nowymi szansami i wyzwaniami wynikającymi z dynamicznego rozwoju najnowszych technologii zintensyfikują podejmowane już działania nad skuteczniejszym wykorzystaniem coraz bardziej dostępnych mediów cyfrowych i interaktywnych technologii informacyjno-komunikacyjnych. Przesłanki te mają charakter uniwersalny, gdyż dotyczą właśnie nauki i prawdy. Ta zaś dotyczy także przemian cywilizacyjnych.

16 Szeroki jest kontekst przedmiotu i celu badań edukacji cyfrowej. Jej liczne relacje z cyberprzestrzenią i wirtualną rzeczywistością przedstawia B. Siemieniecki, wskazując zarówno pytania, jak odmiany tej pierwszej. „Pierwsza z nich polega na odwzorowaniu ciała w multimedialnym obrazie, … druga ujmuje obrazy ciała realnego prezentowane w sieci…, a trzecia dotyczy mariażu człowieka z technologią informacyjno-komunikacyjną”[12]. W badaniach i kształceniu dotyczących funkcjonowania człowieka, zwłaszcza najmłodszego pokolenia, w cyberprzestrzeni i świecie wirtualnym[13] – można uwzględnić następujące obszary analiz teoretycznych i wyników badań empirycznych:

17 Geneza i rozwój cyberprzestrzeni i świata wirtualnego wymuszających konieczność badań w zakresie edukacji cyfrowej. W ostatnich latach cyberprzestrzeń nabiera coraz to większego wymiaru i znaczenia nie tylko w badaniach, ale i w działaniu. Powinna być ona przedmiotem zainteresowania i refleksji nauczycieli, pedagogów, psychologów i przedstawicieli innych dyscyplin zajmujących się wychowaniem, a nawet przedstawicieli innych nauk humanistycznych, społecznych, cybernetycznych itp.

18 Miejsce i znaczenie cyberprzestrzeni i świata wirtualnego w edukacji cyfrowej. Podobnie jak środki techniczne, media i multimedia, ale także ostatnio media interaktywne i cyfrowe, tak również cyberprzestrzeń znajduje zastosowanie w edukacji, nauce i działaniu człowieka.

---

[12] B. Siemieniecki, *Rzeczywistość wirtualna a edukacja*, w: T. Lewowicki, B. Siemieniecki, (red.), *Cyberprzestrzeń i edukacja,* Multimedialna Biblioteka Pedagogiczna, Wyd. Adam Marszałek, Toruń 2012, s. 22–23.

[13] Por. T. Lewowicki, B. Siemieniecki, (red.), *Cyberprzestrzeń i edukacja,* Multimedialna Biblioteka Pedagogiczna, Wyd. Adam Marszałek, Toruń 2012; zob. także inne publikacje, w: T. Lewowicki, B. Siemieniecki, (red.), *Cyberprzestrzeń i edukacja,* Multimedialna Biblioteka Pedagogiczna, Wyd. Adam Marszałek, Toruń 2012; E. Bendyk, *Antymatrix, Człowiek w labiryncie sieci*, Wyd. WAB, Warszawa 2004; A. Andrzejewska, J. Bednarek, (red.) *Możliwości i zagrożenia świata wirtualnego,* Wyd. Akademickie ŻAK, Warszawa 1999.

19 Rola cyberprzestrzeni i świata wirtualnego w kształtowaniu ideałów, wartości i postaw najmłodszego pokolenia. Manipulacja, w tym także manipulacja w cyberprzestrzeni obejmuje każdy system i proces kształcenia. Nie są wolne od niej instytucje (rodzina, szkoła i inne placówki oświatowe) i sytuacje wychowawcze.

20 Skutki cyberprzestrzeni i świata wirtualnego w kształtowaniu osobowości i rozwoju człowieka. Chodzi głównie o wiedzę z zakresu kształtowania osobowości oraz stosunków interpersonalnych w każdym środowisku społecznym. W jej ramach funkcjonuje cyberprzestrzeń i to nie bez znaczenia dla rozwoju człowieka. Wywiera ona nie tylko istotny wpływ na poznawanie wiedzy, ale również postawę, przekonania, zainteresowania.

21 Procesy związane z nowymi możliwościami cyberprzestrzeni i świata wirtualnego, a pośrednio także z manipulacją i psychomanipulacją wywołującymi negatywne skojarzenia. Mają one związek nie tylko z upowszechnianiem wiedzy (w jakim celu?), ale także zainteresowań poznawczych, kształtowania wartości i ich przeżywania, umiejętności kształtowania nawyków, sprawności działania, które są w największym stopniu możliwe tylko w świecie rzeczywistym.

22 Złożony i niejasny obszar oraz rodzaj działań dezinformacyjnych w wirtualnej rzeczywistości, poszczególnych grup interesów, autorów reklam, producentów filmów, gier komputerowych. Warto zatem jednoznacznie stwierdzić, iż o rozwoju osobowości dzieci i młodzieży przesądza obok wielu czynników, w sposób wyjątkowy, sposób korzystania z wirtualnych gier komputerowych, których istota wynika z nowych możliwości cyberprzestrzeni.

23 Zakres zagrożeń w cyberprzestrzeni, z którą mają styczność nie tylko uczniowie, ale także pedagodzy i nauczyciele, którzy też w ramach nauczania-uczenia się mogą stosować pewne mechanizmy manipulacji, wykorzystują do tego celu nie tylko manipulacje językowe, manipulacje faktami, ale i manipulacje emocjami, ostatnio coraz częściej także media, multimedia i cyberprzestrzeń, np. aplikacje i prezentacje multimedialne.

24 Powyższe analizy dotyczą kształcenia i badań realizowanych we wszystkich instytucjach zajmujących się przygotowaniem najmłodszego pokolenia do bezpiecznego funkcjonowania w cyberprzestrzeni, są to:

- Rzecznik Praw Dziecka,
- Rzecznik Praw Obywatelskich,
- Polski Komitet ds. UNESCO,
- UNICEF,
- Fundacja Dzieci Niczyje,
- Naukowo Akademicka Sieć Komputerowa,
- Zespół Dyżurnet.pl,
- Przedstawiciele Producentów Oprogramowania Interaktywnego,
- Polskie Towarzystwo Badania Gier,
- Porozumienie „Dzieci pod Ochroną”,
- Stowarzyszenie Producentów i Dystrybutorów Oprogramowania Rozrywkowego,
- Helsińska Fundacja Praw Człowieka,
- Grupa Telekomunikacja Polska,
- Fundacja Grupy TP,
- PC Polska Sp. z o.o.,
- Polska Izba Informatyki i Telekomunikacji,
- Google,
- Microsoft,
- IBM Polska,
- Centrum Metodyczne Pomocy Psychologiczno-Pedagogicznej,
- Polska Izba Wydawców Prasy,
- Fundacja ABCXXI – „Cała Polska Czyta Dzieciom”,
- inne fundacje, organizacje, stowarzyszenia itp.

25 OBSZARY ZAGROŻEŃ CYBERPRZESTRZENI

W kontekście wielu zalet należy mieć świadomość nowych wielu zagrożeń o charakterze globalnym, powszechnym i niezwykle dynamicznym. A. Andrzejewska zalicza do nich zagrożenia zdrowia psychicznego i fizycznego, zagrożenia moralne: zagrożenia społeczno-wychowawcze, zagrożenia tradycyjnymi i nowymi substancjami chemicznymi z inspiracji sieci, infoholizm i gry komputerowe[14].

26 W płaszczyźnie kształcenia szczególne niebezpieczeństwa wynikają z zagrożeń poznawczo-intelektualnych, związanych z działalnością poznawczą i nauką szkolną, które obejmują: zagrożenia sfery poznawczej, (uniformizacja i/lub redukcja doświadczenia), ograniczenia w zakresie postrzegania problemów, dominację materiału obrazowego nad materiałem słownym, zalew gotowych hipermedialnych informacji niepozwalających na ich twórcze tworzenie i zastosowanie oraz brak możliwości podejmowania racjonalnych decyzji i działań.

27 W wielu najnowszych pozycjach autorskich i pod redakcją podkreśla się rolę i miejsce mediów w społeczeństwie informacyjnym[15]. Ich dość różnorodny kontekst dotyczący relacji wolności a zniewolenia jest podejmowany przez M. Baranowskiego i B. Mikę[16]. Media globalne mają ścisły związek z mediami lokalnymi[17]. Warto dodać, że nauki o mediach w 2011 r. znalazły się w dziedzinie nauk społecznych wśród dziewięciu dyscyplin. Obecnie są nimi pedagogika, psychologia, socjologia, nauki o polityce publicznej, nauki o polityce, nauki o bezpieczeństwie, nauki o obronności, nauki o poznaniu i komunikacji społecznej i w końcu nauki o mediach[18].

28 W dokumentach tych Komisja Europejska wyraża zaniepokojenie, że zarówno młodzi, jak i starsi Europejczycy mogą być pozbawieni korzyści oferowanych przez społeczeństwo informacyjne o niezmiernie wysokim poziomie technologicznym, jeśli nie zostaną zwiększone wysiłki na rzecz udostępnienia im narzędzi do korzystania z obrazów, dokumentów dźwiękowych i tekstów oraz ich analizy i oceny, a także służące wyrobieniu umiejętności wykorzystania nowych i tradycyjnych mediów. Stwierdza, że kraje UE i sektor mediów muszą podjąć działania wobec komunikatów medialnych, na które napotykają (reklamy, filmy, treści internetowe)[19].

29 Nowe możliwości i uzależnienia od przebywania w cyberprzestrzeni oraz świecie wirtualnym związane są z interakcyjnością, symulacją, modelowaniem itp. świata rzeczywistego w świecie wirtualnym i tworzeniem przez każdego własnego przekazu oraz korzystaniem z propozycji przedstawionych w sieci przez innych użytkowników[20].

---

[14] Por. J. Bednarek (red.), *Człowiek w obliczu szans cyberprzestrzeni*, Wyd. Difin, Warszawa 2014; A. Andrzejewska, *Dzieci i młodzież w sieci zagrożeń realnych i wirtualnych,* Wyd. Difin, Warszawa 2014; J. Bednarek, A. Andrzejewska (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Wyd. Difin, Warszawa 2014; A. Andrzejewska, *(Nie)Bezpieczny komputer – od euforii do uzależnień,* Wyd. APS, Warszawa 2008.

[15] Por. E. Jaski, (red.), *Media w społeczeństwie informacyjnym*, Wyd. SGGW, Warszawa 2011.

[16] Por. M. Baranowski, B. Mika, (red.) *Społeczeństwo sieciowe – miedzy wolnością a zniewoleniem*, Wyższa Szkoła Nauk Humanistycznych i Dziennikarstwa, Poznań 2012.

[17] Por. A. Rogulska, *Media globalne – media lokalne. Zagadnienia z obszaru pedagogiki medialnej i edukacji regionalnej*. Oficyna Wydaw. „Impuls", Kraków 2012.

[18] Rozporządzenie z 8 sierpnia 2011 r. MNiSzW w sprawie obszarów wiedzy, dziedzin nauki i sztuki.

[19] http://ec.eu/avpolicy/media literacy/indeks en.htm. zob. też http:// ec.europa.eu/i2010europa

[20] S. Levinstone, *Nowe media*, Wydawnictwo WAM, Kraków 2010, s. 14–15.

30 Poniżej zaprezentowano próbę klasyfikacji obszarów zagrożeń cyberprzestrzeni. Jest ich nie tylko dużo, ale i są mało znane. Obejmują one kilkadziesiąt różnorodnych zagrożeń, których liczba systematycznie rośnie. Nasze kompetencje ich rozpoznawania, dostrzegania zależności pomiędzy nimi a racjonalnym działaniem w zakresie profilaktyki, a także minimalizowania negatywnych skutków są na niskim poziomie. Zostały one zestawione w dwóch (A i B) zasadniczych obszarach.

31 A. ZAGROŻENIA CYBERPRZESTRZENI I ŚWIATA WIRTUALNEGO[21]:

1. Zdrowia psychicznego i fizycznego: dolegliwości wzroku, wady słuchu, dolegliwości układu kostno-mięśniowego, dolegliwości cieśni nadgarstka, dolegliwości kciuka, schorzenia innych narządów, autodestrukcja, samookaleczenie, samobójstwa w cyberprzestrzeni, zaburzenia rozwoju psychofizycznego człowieka.

2. Społeczno-wychowawcze:cyberbullying – przemoc i agresja w sieci, hazard w sieci, Second Life, sekty w świecie wirtualnym, handel żywym towarem i organami, zaburzenie kontaktów interpersonalnych, funkcjonowanie człowieka w świecie robotów humanoidalnych, miejsce człowieka w społeczeństwie nadzorowanym.

3. Zagrożenia moralne: cyberpornografia, prostytucja w sieci, cyberpedofilia, cyberseks, seksting, galerianki w sieci, gadżety erotyczne, tatuaże, implanty, nadzorowanie i kontrola człowieka, subkultury młodzieżowe, kibice.

4. Infoholizm i zagrożenia gier komputerowych.

5. Poznawczo-intelektualne: filmy dla dzieci, korzystanie z gadżetów elektronicznych i in.; związane z brakiem przeżywania, rozwiązywania problemów i działaniem w zakresie poznawania i opanowania wiedzy. W płaszczyźnie kształcenia szczególne niebezpieczeństwa wynikają z zagrożeń poznawczo-intelektualnych, związanych z działalnością poznawczą i nauką szkolną, które obejmują: zagrożenia sfery poznawczej, (uniformizacja i/lub redukcja doświadczenia), ograniczenia w zakresie postrzegania problemów, dominację materiału obrazowego nad materiałem słownym, zalew gotowych hipermedialnych informacji, niepozwalających na ich twórcze tworzenie i zastosowanie oraz brak możliwości podejmowania racjonalnych decyzji i działań[22]. Z zagrożeniami w cyberprzestrzeni mają styczność nie tylko uczniowie, ale także pedagodzy i nauczyciele, którzy też w ramach nauczania-uczenia się mogą stosować pewne mechanizmy manipulacji, wykorzystują do tego celu nie tylko manipulacje językowe, manipulacje faktami, ale i manipulacje emocjami, ostatnio coraz częściej także media, multimedia i cyberprzestrzeń, np. sekwencje filmów czy prezentacji multimedialnych.

6. Zagrożenia (choroby) informacyjne:
   a) ze strony nadawcy: brak poczucia odpowiedzialności za nadawany komunikat (informację, treść), niedostateczna troska o prawdziwość komunikatu, przekazywanie komunikatu sekwencjami, a nie w cało-

[21] Podejmowane analizy zawierają zróżnicowany stopień ich uogólnienia, ze względu na dokładną analizę niektórych z nich w tekście książki.

[22] Por. A. Hankała, *Psychologiczne i społeczne zagrożenia związane z zastosowaniem mediów i technologii informacyjnej w edukacji,* w: M. Tanaś (red.), *Pedagogika @ środki informatyczne i media*, WSP ZNP, Warszawa 2004, s. 73–74.

ści, urojenie informacyjne, generowanie informacji na podstawie własnych domysłów niepopartych faktami (plotki);

b) ze strony poszukującego informacji (adresat): frustracja informacyjna, samotność informacyjna, stres informacyjny, przeciążenie informacyjne;

c) ze strony odbiorcy informacji: bezkrytyczny odbiór informacji i przekazywanie często bez zrozumienia i internalizacji; życzeniowy obiór informacji, selekcja dawek informacji, intencjonalność, ignorowanie informacji będących w konflikcie z oczekiwaniami i doświadczeniami odbiorcy i in.[23].

7. Zagrożenia substancjami chemicznymi z inspiracji sieci: bigoreksja, narkotyki, napoje energetyzujące, dopalacze, suplementy diety, lekarstwa i inne.

8. Zagrożenia sztucznej inteligencji i robotów humanoidalnych[24].

9. Zagrożenia społeczeństwa nadzorowanego czy kontrolowanego.

32 B. PRZESTĘPCZOŚĆ, RYZYKOWNE ZACHOWANIA I BEZPIECZEŃSTWO TELEINFORMATYCZNE OBEJMUJĄCE:

Przestępstwa przeciwko ochronie informacji.

- podsłuch komputerowy,
- sabotaż komputerowy,
- łamanie praw autorskich.
- wirusy komputerowe,
- przechowywanie i zajęcie przechowywanych danych komputerowych,
- wirtualne przestępstwa finansowe.

33 Z pewnością nie są to wszystkie wyżej wymienione szanse i zagrożenia cyberprzestrzeni, ich liczba systematycznie rośnie.

34 Powyższa prezentacja próby klasyfikacji zagrożeń pozwala stwierdzić, że jest ich nie tylko dużo, ale i są mało znane. Także nasze kompetencje ich rozpoznawania, dostrzegania zależności pomiędzy nimi, a racjonalnym działaniem w zakresie profilaktyki, a także minimalizowania negatywnych skutków są na niskim poziomie. Poniżej zaprezentowano nową rolę i zadania pomocy społecznej.

35 ROLA I ZADANIA POMOCY SPOŁECZNEJ W KONTEKŚCIE NOWYCH ZAGROŻEŃ

Szybko zmieniająca się sytuacja społeczno-gospodarcza sprawia, że jest coraz więcej osób, które z różnych powodów nie są w stanie samodzielnie funkcjonować. Uwaga ta dotyczy także wpływu zagrożeń cyberprzestrzeni na podstawowe funkcje i zadania rodziny. Obowiązek pomocy takim osobom spoczywa na całym społeczeństwie. **Każde odpowiedzialne państwo, w tym także Polska, prowadzi politykę społeczną, która według definicji K. Głąbickiej jest „działalnością państwa, samorządów i organizacji pozarządowych, której celem jest poprawa położenia materialnego, asekuracja przed ryzykami życiowymi i wyrównywanie szans życiowych grup społeczeństwa ekonomicznie i socjalnie najsłabszych”**[25]. Pomoc społeczna jest jedną z wielu dziedzin

[23] W. Babik, *O niektórych chorobach powodowanych przez informacje* (bg,uwb.edu.pl/download/ei- białystok.ppt).

[24] I. Belda, *Umysł, maszyny i matematyka. Sztuczna inteligencja i wyzwania, które przed nią stoją*, Toruń 2012.

[25] K. Głąbicka, *Polityka społeczna państwa polskiego u progu członkostwa w Unii Europejskiej*, Radom 2004, s. 11.

wchodzących w zakres polityki społecznej. Jej głównym celem jest:

- „wyrównywanie warunków życia i pracy poprzez zaspokajanie potrzeb ludności w różnym wieku,
- tworzenie równego dostępu do korzystania z obywatelskich praw,
- usuwanie nierówności społecznych,
- asekuracja przed ryzykiem życiowym”[26].

36 W Polsce zagadnienia związane z pomocą społeczną reguluje ustawa z dnia 12 marca 2004 r. o pomocy społecznej. Zgodnie z artykułem 2 pkt. 1 tej ustawy „**pomoc społeczna jest instytucją polityki społecznej państwa mającą na celu umożliwienie osobom i rodzinom przezwyciężenie trudnych sytuacji życiowych, których nie są w stanie pokonać wykorzystując własne uprawnienia, zasoby i możliwości**”[27].

37 Przyczyn uprawniających do korzystania z pomocy społecznej jest bardzo wiele. Należą do nich: „ubóstwo, sieroctwo, bezdomność, potrzeba ochrony macierzyństwa, bezrobocie, niepełnosprawność, długotrwała choroba, bezradność w sprawach opiekuńczo-wychowawczych i prowadzenia gospodarstwa domowego, zwłaszcza w rodzinach niepełnych lub wielodzietnych, alkoholizm lub narkomania, trudności w przystosowaniu do życia po opuszczeniu zakładu karnego oraz klęski żywiołowe lub ekologiczne”[28].

38 W znowelizowanej w 2004 r. ustawie o pomocy społecznej wśród przyczyn uprawniających do pomocy społecznej znalazły się ponadto: brak umiejętności w przystosowaniu do życia młodzieży opuszczającej placówki opiekuńczo-wychowawcze, trudności w integracji osób, które otrzymały status uchodźcy oraz zdarzenia losowe i sytuacje kryzysowe.

39 Zgodnie z art. 15 ustawy o pomocy społecznej działania mające na celu udzielenie wsparcia osobom uprawnionym polegają na:

„1) przyznawaniu i wypłacaniu przewidzianych ustawą świadczeń;
2) pracy socjalnej;
3) prowadzeniu i rozwoju niezbędnej infrastruktury;
4) analizie i ocenie zjawisk rodzących zapotrzebowanie na świadczenia z pomocy społecznej;
5) realizacji zadań wynikających z rozeznanych potrzeb społecznych;
6) rozwijaniu nowych form pomocy społecznej i samopomocy w ramach zidentyfikowanych potrzeb”[29].

40 Z analizy powyższych możliwości pomocy wynika, że kolejną i ważną, choć nieusankcjonowaną formalnoprawnie jest obszar związane z nowymi potrzebami i możliwościami wsparcia w ramach pomocy społecznej w zakresie szans, zwłaszcza zagrożeń cyberprzestrzeni i świata wirtualnego.

41 Świadczenia pomocy społecznej ze względu na miejsce jej udzielania można podzielić na:

- pomoc środowiskową,
- pomoc instytucjonalną.

[26] Tamże, s. 12.

[27] Ustawa o pomocy społecznej z dnia 12 marca 2004 r., Dz.U. 2004 r. Nr 64, poz. 593, z późn. zmianami.

[28] P. Błędowski, *Pomoc społeczna*, w: A. Kurzynowski (red.), *Polityka społeczna*, Warszawa 2003, s. 236.

[29] Ustawa o pomocy społecznej, z dnia 12 marca 2004 r., Dz.U. 2004 r. Nr 64, poz. 593, z późn. zmianami.

42 Pomoc środowiskowa polega na udzielaniu jej w miejscu zamieszkania osoby potrzebującej. Świadczeniami w tej formie są „zasiłek okresowy, zasiłek celowy (w formie pieniężnej lub rzeczowej, zasiłek celowy na ekonomiczne usamodzielnienie się osoby lub rodziny, usługi opiekuńcze lub sprawienie pogrzebu”[30].

43 Istnieją sytuacje, gdy nie można zapewnić osobie potrzebującej właściwej opieki w miejscu zamieszkania. Wówczas istnieje możliwość umieszczenia takiej osoby w domu opieki społecznej. Jest to forma instytucjonalnej pomocy. P. Błędowski wyróżnił jeszcze jedną formę pomocy tzw. półotwartą. Polega ona na udzielaniu pomocy „w placówkach, w których osoby korzystające przebywają przez określony czas (np. dzienne domy pobytu dla osób starszych, placówki terapeutyczne, ośrodki interwencji)”[31].

44 Pomoc społeczna realizowana jest przez jednostki organizacyjne administracji rządowej i samorządowej. Zadania należące do kompetencji gminy wykonują ośrodki pomocy społecznej. Jednostkami realizującymi zadania powiatu są powiatowe centra pomocy rodzinie. Kompetencje województwa realizowane są poprzez organy administracji rządowej – wydziały polityki społecznej urzędów wojewódzkich, oraz samorządowej – regionalne ośrodki polityki społecznej w urzędach marszałkowskich.

45 Jednostkami organizacyjnymi bezpośrednio realizującymi zadania z zakresu pomocy społecznej, w tym także w wypadku zagrożeń cyberprzestrzeni są:

1 Placówki opiekuńczo-wychowawcze, których celem jest zapewnienie potrzebującym dzieciom i młodzieży opieki i wychowania. Ze względu na rodzaj sprawowanej pomocy placówki te dzielą się na:
   - placówki wsparcia dziennego,
   - placówki interwencyjne,
   - placówki rodzinne,
   - placówki specjalistyczne.

2 Ośrodki adopcyjno-opiekuńcze, których zadaniem jest udzielanie wsparcia rodzinom naturalnym, zastępczym lub adopcyjnym w zakresie poradnictwa, szkoleń i terapii.

3 Ośrodki wsparcia – działalność ich polega na udzielaniu pomocy środowiskowej o charakterze półotwartym w celu pozostawienia osób potrzebujących w ich środowisku. Zadania te realizowane są przez:
   - środowiskowe domy pomocy społecznej,
   - dzienne domy pomocy społecznej,
   - noclegownie,
   - ośrodki opiekuńcze.

4. Ośrodki interwencji kryzysowej – przeznaczone są dla osób i rodzin w sytuacjach kryzysowych lub ofiar przemocy. Pomoc realizowana jest poprzez porady psychologiczne, prawne czy też zabezpieczenie noclegu przez całą dobę.

Domy pomocy społecznej, mające na celu zapewnienie całodobowej opieki osobom, które z różnych przyczyn nie są w stanie funkcjonować w swoim środowisku.

47 W ramach tych jednostek organizacyjnych ważnym i nowym ich obszarem działania jest bieżąca analiza nowych zadań z zakresu polityki społecznej.

[30] P. Błędowski, *Pomoc społeczna* , w: A. Kurzynowski (red.), *Polityka społeczna*, Warszawa 2003, s. 243.

[31] Tamże.

48 W wypadku zagrożeń cyberprzestrzeni dokształcanie i doskonalenie powinno obejmować następujące obszary wiedzy, umiejętności i kompetencji społecznych:

1) teoretyczne podstawy powstawania różnorodnych nowych zagrożeń, patologii i uzależnień,
2) przyczyny, przebieg i skutki zagrożeń,
3) analiza zakresu i skali zagrożeń,
4) nowe kompetencje i działania pracowników socjalnych.

49 Nowe zadania wymienione powyżej stają się wielkim wyzwaniem w kontekście tradycyjnych i nowych problemów polityki społecznej.

50 **NOWE PROBLEMY POLITYKI SPOŁECZNEJ I PRACY SOCJALNEJ**

Problemy te, mające także charakter społeczny i socjalny, są najważniejsze, gdyż dotyczą ludzi, zarówno społeczności globalnej, jak i regionalnej oraz poszczególnych grup czy osób[32]. Są one także ściśle powiązane z nowymi szansami i wyzwaniami cyberprzestrzeni i świata wirtualnego. Wynikają bezpośrednio i pośrednio z wielu powodów, a ostatnio poważną ich przyczyną jest niebezpieczna luka informacyjna, będąca skutkiem różnicowania się społeczeństwa, a nie jego ujednolicania. W krajach rozwiniętych powszechnym zjawiskiem staje się „twórcza destrukcja". Jest to łagodne określenie gospodarczego „trzęsienia ziemi", jakie musiało przeżyć społeczeństwo, które zastępowało prostą technikę i pracochłonną produkcję tzw. high-tech. Twórcza destrukcja, wynikająca z dokonujących się przemian społecznych i ekonomicznych, najsilniej dała się we znaki pracownikom niemającym wyższego wykształcenia[33].

51 W ciągu ostatnich piętnastu lat zatrudnienie w przemyśle stalowym w USA i Unii Europejskiej spadło o ponad 50%. Najszybszą transformację społeczeństwa powodują nowoczesne technologie z dziedziny informacji elektronicznej i łączności. Multimedia oferują cyfrowy zapis głosu, obrazu i tekstu, danych liczbowych, dostarczają informacje na płytach CD-ROM, a także online – na bieżąco, w formie poczty elektronicznej, komputerowego systemu zakupów, wideotelefonów, interakcyjnych gier i filmów. Usługi te są dostarczane do firm lub osób prywatnych siecią komputerową (komputery osobiste ma w Stanach Zjednoczonych co piąte gospodarstwo domowe, w krajach Unii Europejskiej – co dziesiąte), a także za pośrednictwem sieci telefonicznej, przez „inteligentną" czy interaktywną telewizję bądź za pomocą Internetu.

52 W tej sytuacji nasuwają się następujące problemy:

- Jakie przyjmować strategie rozwoju polityki społecznej w sensie globalnym, regionalnym i narodowym (z poszanowaniem wartości narodowościowych, kulturowych, etnicznych, rasowych i religijnych), aby minimalizować rosnące dysproporcje pomię-

[32] Por. m.in.: J. Auleytner, *Polish Social Forging of a Social Order,* WSP TWP, Warszawa 2006; M. Grewiński, *Wielosektorowa polityka społeczna, O przeobrażeniach państwa opiekuńczego,* WSP TWP, Warszawa 2009; M. Grewiński, A. Karwacki (red.), *Strategie w polityce społecznej,* Mazowieckie Centrum Polityki Społecznej, Warszawa 2009; M. Grewiński (współredaktor), *Praca socjalna w środowisku lokalnym,* WSP TWP, Warszawa 2009; J. Kowalewski, P. Szukalski (red.), *Pomyślne starzenie się w perspektywie nauk o pracy i polityce społecznej,* Zakład Demografii i Gerontologii Społecznej UŁ, Łódź 2008; M. Bąkiewicz, M. Grewiński (red.), *System lokalnej pomocy społecznej,* Warszawa 2010, N. Nyczkało, (red.) M. Kopsztejn, D. Szeligiewicz-Urban (red. polskiego wydania), *Praca socjalna, wydanie podręcznikowe*, Siemianowice Śląskie 2011.

[33] W. Cellary, *Przemiany społeczne i gospodarcze,* w: *Polska w drodze do globalnego społeczeństwa informacyjnego. Raport o rozwoju społecznym,* Program Narodów Zjednoczonych ds. Rozwoju (UNDP), Warszawa 2002.

dzy działaniami w ramach polityki społecznej i pracy socjalnej realizowanych w UE i Polsce?

- Kto i jak może zmniejszyć skalę konfliktu świadomościowego pomiędzy potrzebami a możliwościami polityki społecznej w kontekście nowych potrzeb wynikających z wyzwań społeczno-wychowawczych i technologiczno-medialnych, z uwzględnieniem nowych światowych wyzwań cywilizacyjnych związanymi z nowymi szansami i wyzwaniami e-społeczeństwa, cyfrowej edukacji w zakresie bezpiecznego korzystania z najnowszych technologii informacyjno-komunikacyjnych i mediów cyfrowych?

- Jak przygotowywać instytucje polityki społecznej do nowych funkcji i realizowanych zadań wynikających z nowych zagrożeń cyberprzestrzeni i świata wirtualnego?

- Jak i kiedy w dokumentach formalnoprawnych należy uwzględnić nową rolę pracowników socjalnych w kontekście niebezpieczeństw przestrzeni internetowej?

53 Ponadto należy rozwiązać problemy związane z kształceniem i doskonaleniem kwalifikacji pracowników socjalnych, poza przedmiotem analiz dotyczącym zagrożeń cyberprzestrzeni i świata wirtualnego, ale związanym z ich funkcjonowaniem w e-społeczeństwie i e-gospodarce, wymienić należy:

a) społeczne aspekty powszechnego wprowadzenia usług elektronicznych (m.in. e-administracja, e-usługi, e-handel);
b) wirtualizację kształcenia i doskonalenia na różnych poziomach edukacyjnych (e-learning, e-booki, transmisje on-line);
c) przygotowanie specjalistów, konsultantów, dydaktyków do aktywnego uczestnictwa w procesie kształcenia i doskonalenia kadr w zakresie wirtualnego kształcenia (metodologia i narzędzia wirtualnego kształcenia);
d) aplikowanie o środki europejskie poprzez portale (PARP, urzędy marszałkowskie). Składanie zdalnych wniosków poprzez generatory wniosków aplikacyjnych i ich zdalne rozliczanie (e-Płatnik, generatory wniosków płatniczych).

54 Celowym jest również pozyskiwanie nowych specjalistów, co pociąga za sobą konieczność postępowania planowego, ciągłej modyfikacji założeń funkcjonowania, zwłaszcza szkolenia i doskonalenia kadr polityki społecznej.

55 W założeniach tych i programach kształcenia należy dążyć do kształtowania i doskonalenia kompetencji kluczowych z zakresu informatyki uwzględnionych w „Zaleceniu Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie". Zostały one zdefiniowane jako umiejętne i krytyczne wykorzystywanie technologii społeczeństwa informacyjnego w każdej aktywności człowieka. Chodzi o wykorzystanie komputerów do uzyskiwania, oceny, przechowywania, tworzenia, prezentowania i wymiany informacji oraz do porozumiewania się i uczestnictwa w sieciach współpracy za pośrednictwem Internetu. Mają one szczególne znaczenie dla osób dorosłych systematycznie doskonalących swoje kompetencje w ramach kształcenia ustawicznego.

56 W zaleceniu podkreślono, iż kompetencje informatyczne wymagają solidnego rozumienia i znajomości natury, roli i możliwości technologii społeczeństwa informacyjnego w codziennych kontekstach: w życiu osobistym i społecznym, a także w pracy zawodowej. Do nich należą m.in.:

- kształtowanie innowacyjnych postaw zmierzających do podejmowania działań na rzecz pomniejszania luki między rozwijającą się cywilizacją informatyczną, a jej wymiarem humanistycznym,

- przygotowanie technologiczne do samoedukacji, w którym to procesie będzie się stosować nowe technologie informatyczne,

- kształtowanie odpowiednich postaw otwartości na nowe zjawiska i procesy związane z przemianami gospodarczymi, społecznymi, kulturowymi i obyczajowymi, powodowanymi najnowszymi technologiami,

- tworzenie w toku kształcenia strategii promocji społeczeństwa informacyjnego z jednoczesnym przeciwdziałaniem i minimalizowaniem wszelkich zagrożeń,

- przygotowanie do pracy na odległość odpowiedniej kadry nauczycielskiej, instruktorów, mentorów i in.

57 **WYZWANIA PRZYGOTOWANIA DZIECI I MŁODZIEŻY DO FUNKCJONOWANIA W CYFROWYM SPOŁECZEŃSTWIE**

Problematyka szans mieści się w obszarze zainteresowań wielu dyscyplin naukowych, a wśród nich pedagogiki, edukacji medialnej, e-edukacji, technologii informacyjno-komunikacyjnych, w informatyce, kreatywności, a także aktywności w cyberprzestrzeni i świecie wirtualnym oraz profilaktyce. Wielkim wyzwaniem i znaczeniem jest zmiana modelu nauki i szkolnictwa wyższego, w którym media cyfrowe i technologie interaktywne pełnią niekwestionowane funkcje. Nie bez powodu wyznacznikiem XXI w. staje się nowy model nauki odpowiadający na konkretne potrzeby społeczne, rynku i gospodarki – model nauki sprzyjający innowacyjności to rola przyszłej uczelni.

58 Do tych nowych wyzwań szkoła tradycyjna, i w jeszcze większym stopniu cyfrowa, musi przygotować dzieci i młodzież.

59 W licznych dokumentach podkreślono rolę i miejsce najnowszych mediów cyfrowych, technologii interaktywnych w badaniach i kształcenia w zakresie edukacji cyfrowej, życiu społecznym, gospodarce, sztuce i kulturze, czasie wolnym oraz znaczenie nowych kompetencji społeczno-komunikacyjnych, medialnych i informacyjno-komunikacyjnych we współczesnym świecie. Należą do nich m.in.:

60 Strategia „Europa 2020" zmierzająca do wyjścia z kryzysu i mająca przygotować unijną gospodarkę na wyzwania następnego dziesięciolecia. Nakreślono w niej wizję wysokiego poziomu zatrudnienia, gospodarki niskoemisyjnej, wydajności i spójności społecznej, który ma zostać osiągnięty na szczeblu unijnym i krajowym.

61 W 2009 r. UE znowelizowała ramy regulacyjne łączności elektronicznej, a w 2010 r. ogłosiła Europejską Agencję Cyfrową, która stanowi jedną z siedmiu inicjatyw flagowych „Europy 2020" – dziesięcioletniej unijnej strategii na rzecz wzrostu. W strategii tej zwrócono uwagę na rozwój w UE, który ma być nie tylko zrównoważony i sprzyjający włączeniu społecznemu, a może przede wszystkim, rozwój ten może też być inteligentny"[34]. Eksponuje się zatem badania naukowe i innowacje technologiczne oraz inne działania przygotowujące grunt

[34] J. M. Zurao Barroso, *Słowo wstępne,* w: *Komunikat Komisji „Europa 2020". Strategie na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu*, Komisja Europejska, KOM (2010) wersja ostateczna.

pod przekształcanie gospodarki przemysłowej w gospodarkę opartą na wiedzy, a wiec taką, w której wiedza ma wartość jako środek produkcji i źródło dobrobytu.

62 W dokumencie tym Komisja Europejska określa siedem najważniejszych obszarów problemowych, w których podkreśla się szanse przygotowania w dla potrzeb cyfrowej przyszłości. Są nimi:

1. Dynamiczny jednolity rynek cyfrowy.
2. Interoperacyjność i normy, chodzi o zapewnienie interoperacyjności urządzeń, usług, aplikacji i baz danych.
3. Zaufanie i bezpieczeństwo, w elektronicznej UE, jako fundament Europejskiej Agendy.
4. Szybki i bardzo szybki dostęp do Internetu w przystępnej cenie.
5. Badania i innowacje, mające na celu minimalizowanie zbyt dużego dysonansu między UE a USA. W tym celu niezbędna jest nowa, tym razem cyfrowa alfabetyzacja.
6. Zwiększenie umiejętności wykorzystania technologii cyfrowych włączenia społecznego.
7. Korzyści z TIK dla społeczeństwa UE[35].

63 Działania w tych obszarach, w tym także badawcze i kształceniowe w zakresie edukacji cyfrowej mają być ważnym krokiem na drodze do utworzenia rynku komunikacji elektronicznych. Pakiet reform regulacyjnych niezbędnych w dążeniu do budowy społeczeństwa cyfrowego, eliminowania wykluczonych cyfrowo, osób starszych i niepełnosprawnych.

[35] Tamże, s. 8–39.

64 PODSUMOWANIE

Nie bez powodu obecnie tak istotne jest znaczenie najnowszych mediów i technologii pozwalających na tworzenie wiedzy, jej przekaz i zastosowanie oraz legislacja najnowszych dokumentów w Polsce. W najnowszym raporcie M. Boniego *Polska 2030*, w wyzwaniu szóstym *Gospodarka oparta na wiedzy i rozwój kapitału intelektualnego* podkreśla się nie tylko potrzebę uczenia się przez całe życie (life-long learning), ale również potrzebę uczenia się we wszystkich rolach życiowych (life-wide learning), a także to, że o innowacyjności polskiej gospodarki w 2030 r. zadecyduje obecna efektywność systemu edukacyjnego. „Zaskakujące, że premia za edukację w Polsce wciąż wyraźnie rośnie. Wynika to przede wszystkim z rosnącego wskutek przemian technologicznych zapotrzebowania na osoby wykwalifikowane na rynku pracy”[36]. Akcentuje się również, iż „każdy uczeń powinien mieć własny projekt doskonalenia osobistego, który planując cele edukacyjne zarówno w sferze kompetencji poznawczych, jak i kluczowych postaw, szanuje osobisty rytm uczenia się”[37]. Nowym dokumentem jest strategia długookresowa *Polska 2030. Trzecia fala nowoczesności*. Najnowsze analizy badań młodzieży zawarto w kolejnym raporcie, w którym podjęto kwestie dotyczące nowych mediów i zachowań ryzykownych młodzieży.

Cele szczegółowe najnowszego Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2011 – 2016 realizowane są m.in. poprzez powszechną edukację społeczną oraz specjalistyczną w zakresie bezpieczeństwa w świecie realnym i cyberprzestrzeni oraz świecie wirtualnym. Programy w zakresie działań obej-

[36] M. Boni, *Diagnoza Polska 2030*, Warszawa 2009, s. 221.

[37] Tamże, s. 223.

mują:

1) szkolenia pełnomocników ds. ochrony cyberprzestrzeni;
2) racjonalizację programów kształcenia studentów i doskonalenia kwalifikacji specjalistycznych;
3) kształcenie kadry urzędniczej oraz ustanowienie dodatkowych kryteriów obsady stanowisk administracji publicznej.

W kontekście powyższych analiz istotne jest znaczenie profilaktyki (prewencji), diagnozy i terapii ww. zagrożeń i patologii społecznych.

BIBLIOGRAFIA:

Andrzejewska A., Bednarek J., (red.) *Możliwości i zagrożenia świata wirtualnego*, Wyd. Akademickie ŻAK, Warszawa 1999.

Auleytner J., *Polish Social Forging of a Social Order*, WSP TWP, Warszawa 2006;

Grewiński M., *Wielosektorowa polityka społeczna, O przeobrażeniach państwa opiekuńczego*, WSP TWP, Warszawa 2009;

Grewiński M., Karwacki A. (red.), *Strategie w polityce społecznej*, Mazowieckie Centrum Polityki Społecznej, Warszawa 2009;

Grewiński M. (współredaktor), *Praca socjalna w środowisku lokalnym*, WSP TWP, Warszawa 2009;

Kowalewski J., Szukalski P. (red.), *Pomyślne starzenie się w perspektywie nauk o pracy i polityce społecznej, Zakład Demografii i Gerontologii Społecznej* UŁ, Łódź 2008;

Bąkiewicz M., Grewiński M. (red.), *System lokalnej pomocy społecznej*, Warszawa 2010,

Nyczkało N., (red.) Kopsztejn M., Szeligiewicz-Urban D. (red. polskiego wydania), *Praca socjalna, wydanie podręcznikowe*, Siemianowice Śląskie 2011.

Babik W., *O niektórych chorobach powodowanych przez informacje* (bg,uwb.edu.pl/download/ei- białystok.ppt).

Baranowski M., Mika B., (red.) *Społeczeństwo sieciowe – między wolnością a zniewoleniem*, Wyższa Szkoła Nauk Humanistycznych i Dziennikarstwa, Poznań 2012.

Bednarek J. (red.), *Człowiek w obliczu szans cyberprzestrzeni*, Wyd. Difin, Warszawa 2014;

Andrzejewska A., *Dzieci i młodzież w sieci zagrożeń realnych i wirtualnych*, Wyd. Difin, Warszawa 2014.

Bednarek J., Andrzejewska A.(red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Wyd. Difin, Warszawa 2014;

Andrzejewska A, *(Nie)Bezpieczny komputer – od euforii do uzależnień*, Wyd. APS, Warszawa 2008.

Belda I., *Umysł, maszyny i matematyka. Sztuczna inteligencja i wyzwania, które przed nią stoją*, Toruń 2012.

Bendyk E., *Antymatrix, Człowiek w labiryncie sieci*, Wyd. WAB, Warszawa 2004.

Błędowski P., *Pomoc społeczna*, w: Kurzynowski A. (red.), *Polityka społeczna* (red.), Warszawa 2003.

Boni M., *Diagnoza Polska 2030*, Warszawa 2009.

Cellary W., *Przemiany społeczne i gospodarcze*, w: *Polska w drodze do globalnego społeczeństwa informacyjnego. Raport o rozwoju społecznym, Program Narodów Zjednoczonych ds. Rozwoju (UNDP)*, Warszawa 2002.

Durao Barroso J. M., *Słowo wstępne,* w: *Komunikat Komisji „Europa 2020". Strategie na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu*, Komisja Europejska, KOM (2010). Wersja ostateczna.

Głąbicka K., *Polityka społeczna państwa polskiego u progu członkostwa w Unii Europejskiej*, Radom 2004.

Goliński M., *Społeczeństwo informacyjne – geneza koncepcji i problematyka pomiaru*, Oficyna Wydawnicza SGH, Warszawa 2011.

Hankała A., *Psychologiczne i społeczne zagrożenia związane z zastosowaniem mediów i technologii informacyjnej w edukacji*, w: M. Tanaś (red.), *Pedagogika @ środki informatyczne i media*, WSP ZNP, Warszawa 2004.

Jaski E., (red.), *Media w społeczeństwie informacyjnym*, Wyd. SGGW, Warszawa 2011.

Kupisiewicz Cz., *Projekty reform edukacyjnych w Polsce. Główne tezy i wpływ na funkcjonowanie szkolnictwa*, Seria Krótkie wykłady z pedagogiki, Wyd. Naukowe PWN, Warszawa 2006;

Kupisiewicz Cz. (red.), Kupisiewicz M. (współpraca), Nowakowska-Siuta R., *Drogi i bezdroża polskiej oświaty w latach 1945—2005. Próba wybiórczo-retrospektywnego spojrzenia*, Komitet Prognoz „Polska 2000 Plus" przy Prezydium PAN, Warszawa 2005.

Levinstone S., *Nowe media*, Wydawnictwo WAM, Kraków 2010.

Lewowicki T. (red.), *Gorące problemy edukacji w Polsce*, Komitet Nauk Pedagogicznych Polskiej Akademii Nauk i WSP ZNP, Warszawa 2007.

Lewowicki T., Siemieniecki B., (red.), *Cyberprzestrzeń i edukacja*, Multimedialna Biblioteka Pedagogiczna, Wyd. Adam Marszałek, Toruń 2012; zob. także inne publikacje, w: T. Lewowicki, B. Siemieniecki, (red.), *Cyberprzestrzeń i edukacja*, Multimedialna Biblioteka Pedagogiczna, Wyd. Adam Marszałek, Toruń 2012;

Łaszczyk J. (red.), *Komputer w kształceniu specjalnym: wybrane zagadnienia*, WSiP, Warszawa 1998.

Łaszczyk J., Jabłonowska M. (red.), *Uczeń zdolny wyzwaniem dla współczesnej edukacji*, Wyd. APS, Warszawa 2008.

Bednarek J., *Społeczeństwo informacyjne i media w opinii osób niepełnosprawnych*, Wyd. APS, Warszawa 2005.

Morbitzer J., E. Musiał (red.) *Człowiek, Media, Edukacja,* Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie, Kraków 2012.

Rogulska A., *Media globalne – media lokalne. Zagadnienia z obszaru pedagogiki medialnej i edukacji regionalnej*. Oficyna Wydaw. „Impuls", Kraków 2012.

Siemieniecki B., *Rzeczywistość wirtualna a edukacja*, w: Lewowicki T., Siemieniecki B., (red.), *Cyberprzestrzeń i edukacja*, Multimedialna Biblioteka Pedagogiczna, Wyd. Adam Marszałek, Toruń 2012

Tanaś M., *Media w katalogu środków dydaktycznych*, w: Siemieniecki B. (red.), Pedagogika medialna, Wyd. Naukowe PWN, Warszawa 2007,

DOKUMENTY:

Rozporządzenie z 8 sierpnia 2011 r. MNiSzW w sprawie obszarów wiedzy, dziedzin nauki i sztuki.

Ustawa o pomocy społecznej z dnia 12 marca 2004 r., Dz.U. 2004 r. Nr 64, poz. 593, z późn. zmianami.

STRONY INTERNETOWE:

http://ec.eu/avpolicy/media literacy/indeks en.htm. zob. też http:// ec.europa.eu/i2010europa

http://ec.eu/avpolicy/media literacy/indeks en.htm. zob. też http:// ec.europa.eu/i2010europa

SŁUŻBY SPOŁECZNE WOBEC ZAGROŻEŃ CYBERPRZESTRZENI

CYBERZAGROŻENIA
JAKO NOWE WYZWANIE DLA DZIAŁALNOŚCI PRACOWNIKÓW SŁUŻB SPOŁECZNYCH – Z PERSPEKTYWY PRAKTYKA

Ewa Flaszyńska

1 WPROWADZENIE

W ciągu ostatnich dwudziestu lat Internet oraz szerzej rozumiana cyberprzestrzeń miały, mają i mieć będą ogromny wpływ na wszystkie przejawy funkcjonowania społeczeństwa. Ze względu na skalę ich wpływu na życie społeczne, ograniczony dostęp do Internetu lub jego brak oraz nieumiejętność posługiwania się technologiami cyfrowymi stawiają wybrane grupy społeczne w niekorzystnej sytuacji. Dostęp do Internetu wskazywany jest jako element właściwego poziomu życia mieszkańców, a jego brak – na przykład w małych miejscowościach i wsiach – jest uznawany za jedną z głównych barier rozwojowych danego obszaru. Globalizacja i nowe technologie powodują więc, że dziś każdy powinien mieć możliwość dostępu do Internetu i tym samym do przepływu informacji, co uważane jest współcześnie za pewien standard. Brak tego dostępu jest dziś postrzegany jako jedna z głównych przyczyn narażania całych grup społecznych na wykluczenie. W tym wypadku wykluczenie informatyczne.

2 Obok ogromnych korzyści, jakie niesie za sobą informatyzacja, w tym dostęp do informacji i wiedzy wyrównujący w pewnym stopniu szanse edukacyjne, pojawiają się jednak istotne nieznane wcześniej zagrożenia, które dotykają wszystkich grup społecznych. W lutym 2013 r. Komisja Europejska wydała komunikat, w którym napisano, że liczba incydentów naruszających bezpieczeństwo cybernetyczne, zamierzonych bądź przypadkowych, wzrasta w alarmującym tempie, a zagrożenia te mogą mieć różne źródła – w tym przestępcze, jak również mogą być efektem niezamierzonych błędów[1]. Komisja Europejska wskazała, że zapewnienie bezpieczeństwa cybernetycznego jest wspólnym obowiązkiem różnych podmiotów, w tym w szczególności podmiotów publicznych. Użytkownicy końcowi – w tym wypadku korzystający z Internetu obywatele – odgrywają kluczową rolę w zapewnianiu bezpiecznego korzystania z sieci i informacji: muszą oni być świadomi zagrożeń, na jakie są narażeni w Internecie i muszą mieć możliwość podejmowania prostych kroków w celu obrony przed nimi[2].

3 OBRAZ ZJAWISKA W POLSCE

W Polsce z dostępu do Internetu korzysta ponad 10 mln użytkowników. Znakomita większość (87%) korzysta z sieci regularnie (co najmniej raz w tygodniu), a dwie trzecie codziennie[3]. Zagrożenia związane z informatyzacją to nowe fakty, które pojawiły się również w obszarze pomocy społecznej i są wyzwaniem dla działalności pracowników służb społecznych. Wyzwania te często wymagają całkowicie nowych rozwiązań, bądź znacznego przekonstruowania działania instytucji oraz instrumentów, którymi dotychczas posługiwali się pracownicy socjalni.

4 Zacznijmy jednak od tego, że w naszej krajowej rzeczywistości wciąż zderzają się dwie Polski. Pierwsza, w której pracownicy służb społecznych na wszystkich szczeblach, począwszy od krajowego, a skończywszy na lokalnym, przeszkoleni są i wyposażeni w nowe technologie informatyczne, biorąc jednocześnie udział w publicznej debacie o sposobie wdrażania usług elektronicznych dla osób fizycznych, przedsiębiorców oraz urzędów administracji publicznej w obszarach dedykowanych szeroko rozumianemu zabezpieczeniu społecznemu i rodzinie[4]. I druga Polska, w któ-

[1] *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*, Wspólny Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Komisja Europejska, Bruksela, 7.2.2013 JOIN(2013) 1 final, s.3.

[2] Tamże.

[3] V. Szymanek, *Społeczeństwo informacyjne w liczbach 2013*, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013, s.37.

[4] Ministerstwo Pracy i Polityki Społecznej uruchamia właśnie portal Emp@tia, którego założeniem jest załatwianie niemal wszystkich spraw online.

rej nadal wielu pracowników ośrodków pomocy społecznej, szczególnie z małych gmin, nie ma w pracy własnego komputera bądź też nie umie z niego korzystać. Dlatego trzeba podkreślić, że niezależnie od dyskusji i podejmowanych działań na rzecz przeciwdziałania zagrożeniom, które niesie ze sobą informatyzacja, w wielu wypadkach i w wielu miejscach w Polsce należy odpowiednio i często od podstaw przygotować do funkcjonowania w nowej rzeczywistości instytucje działające w sferze społecznej i ludzi pracujących w nich. W obliczu nowych potrzeb społecznych i postępu społecznego, a jednocześnie nowych, wynikających z tych zjawisk zagrożeń, praca pracowników służb społecznych nabiera innego znaczenia, stanowiąc w wielu wypadkach podstawowy i najważniejszy instrument przeciwdziałania tym zagrożeniom. Obecnie często mówi się o niedostatecznym rozwoju usług pomocy i integracji społecznej, natomiast należy pamiętać, że zasadniczo nie wynika on z faktu, iż katalog ustawowych zadań jest niepełny, ale z braku wyposażenia pracowników służb społecznych we właściwe, adekwatne do stanu rozwoju, instrumenty i narzędzia oraz wiedzę.

5 PRACOWNICY SŁUŻB SPOŁECZNYCH WOBEC NOWYCH ZAGROŻEŃ

Wobec nowych technologii i nowych wyzwań społecznych ogromnego znaczenia nabiera wdrożenie innowacyjnego programu rozwoju przygotowującego pracowników służb społecznych do pracy z rodzinami oraz osobami potrzebującymi pomocy w obszarze zagrożeń generowanych przez cyberprzestrzeń. W systemie kształcenia pracowników społecznych w Polsce zagadnienia związane z cyberprzestrzenią dotychczas nie były poruszane. A przecież od tego, na ile udzielana pomoc jest zróżnicowana co do jej form i zakresu, na czym każda z tych form w praktyce polega, zależy w jakim stopniu misja służb społecznych może być osiągana. Dlatego też wyposażenie pracowników służb społecznych w szerszy zasób kompetencji i instrumentów wykonawczych, będących cechami specyficznymi usługi, jaką jest praca socjalna staje się niezbędne i jak najbardziej zasadne. Pomoc osobom wykluczonym wymaga wielowymiarowego podejścia, które nie będzie możliwe, jeśli osoby oferujące tę pomoc nie będą wyposażone w odpowiednie kompetencje i uaktualnianą wiedzę. Działania zaradcze podejmowane przez coraz bardziej świadomą tych zagrożeń kadrę kierowniczą wielu instytucji realizujących politykę społeczną nie zastąpią niezbędnych działań systemowych.

6 Zjawiska uzależnienia od Internetu i innych niebezpieczeństw czyhających w cyberprzestrzeni na dzieci, młodzież i dorosłych występują ze zróżnicowanym natężeniem w Polsce. Wszyscy, nie tylko klienci pomocy społecznej, narażeni są na stanie się ofiarą przestępstw takich jak kradzież informacji (phishing), fałszerstwo, nieuprawniony dostęp do komputera przez osoby trzecie (hacking), nękanie przy użyciu Internetu (cyberbullying) i uzależnienie od ciągłego dostępu do informacji (infoholizm). Rozluźnienie więzi rodzinnych i samotność, brak akceptacji, patologie występujące w rodzinach czy też brak stałego zajęcia sprzyjają uzależnieniu od komputera. Internet uzależnia tak łatwo, ponieważ gromadzi wiele różnych zasobów i pozwala na wiele form aktywności. Staje się substytutem deficytów występujących w życiu realnym, stąd też osoby wykluczone społecznie są szczególnie narażone na tego rodzaju zagrożenia.

7 Wiele osób i rodzin korzystających z pomocy pracowników służb społecznych jest ze środowisk dotkniętych wielorakimi, często nakładającymi się problemami lub znajduje się w szczególnej sytuacji. Sytuacje te wymagają długofalowych działań zarówno w formie zintensyfikowanej pracy socjalnej, jak

również poradnictwa specjalistycznego oraz współpracy wielu instytucji i organizacji. Biorąc pod uwagę ogół pracowników służb społecznych, tymi z nich, dla których cyberzagrożenia mogą być szczególnym wyzwaniem w pracy zawodowej są pracownicy socjalni i asystenci rodziny. To oni wykonują pracę socjalną, działając na rzecz jednostek, rodzin, grup i środowisk społecznych, znajdujących się w trudnej sytuacji życiowej. Zgodnie z zapisem art. 6 pkt 12 ustawy o pomocy społecznej, **praca socjalna oznacza działalność zawodową ukierunkowaną na pomoc osobom i rodzinom we wzmacnianiu i odzyskaniu zdolności do funkcjonowania w społeczeństwie oraz na tworzeniu warunków sprzyjających temu celowi**[5]. Systematyczne spotkania pracowników socjalnych z członkami rodzin mają na celu wsparcie rodziny w jej prawidłowym funkcjonowaniu oraz w rozwiązywaniu bieżących problemów. Wizyty w środowisku umożliwiają obserwację aktualnej sytuacji rodziny oraz weryfikację zaplanowanych działań, jak również są okazją do motywowania rodziny do podejmowania zmian. Asystenci rodziny realizują swoje zadania poprzez pogłębioną pracę socjalną, pracę socjalno-terapeutyczną, mediacje oraz administrowanie usługami służb społecznych. Asystenci wspierają rodziny w codziennych czynnościach. Podejmują próby wyeliminowania barier utrudniających prawidłowe funkcjonowanie klientów oraz zmniejszenie deficytów intrapsychicznych, jak również minimalizowanie zjawiska wyuczonej bezradności. Pracują nad podniesieniem szans klientów w dostosowaniu się do obecnych wymogów życia społecznego i zawodowego oraz nad zwiększeniem szans na integrację ze społeczeństwem.

8 Analiza obowiązków tych dwóch grup zawodowych w zderzeniu z aktualnymi wyzwaniami, nasuwa oczywisty wniosek, że bardzo ważne jest, by umiały one nieść również pomoc osobom poszkodowanym i dotkniętym zjawiskami takimi, jak szeroko rozumiane cyberzagrożenia (w tym szczególnie cyberprzemoc).

Przypomnijmy zatem, że do podstawowych zagrożeń informatycznych, z którymi mogą się zetknąć pracownicy służb społecznych, w tym pracowników socjalnych, należą:

- uzależnienie od Internetu, ale też uzależnienie od komputera w ogóle – np. od gier komputerowych,
- kontakt z nielegalnymi materiałami (np. przedstawiającymi seksualne wykorzystanie dzieci, rasizm, ksenofobię) lub szkodliwymi treściami (np. pornografia, przemoc),
- uwodzenie za pośrednictwem Internetu (grooming),
- nękanie za pośrednictwem sieci (cyberprzemoc),
- przesyłanie swoich nagich lub półnagich zdjęć (sexting),
- kradzież lub nieświadome udostępnianie informacji (np. numerów kart, adresów, haseł itp.).

9 Jak wynika z badań, już ponad 100 tys. Polaków jest uzależnionych od Internetu, a kolejnych 750 tys. jest na to poważnie narażonych. Problem najczęściej dotyka osób młodych (90 proc. ma mniej niż 34 lata). Dzieci zaczynają korzystać z Internetu i komputera coraz wcześniej. Średnio, gdy mają około dziewięciu lat[6]. Dostęp do gier przez In-

[5] Ustawa z dnia 12 marca 2004 r. o pomocy społecznej, Dz.U. nr 64, poz. 593 z późn. zmianami.

[6] Badania CBOS wykonane na zlecenie Funduszu Rozwiązywania Problemów Hazardowych, CBOS, 2011–2 012.

ternet może prowadzić do rozwoju niekorzystnych zjawisk społecznych, w tym rozpowszechnienia się uzależnienia od hazardu. Zagrożenia związane z używaniem Internetu często prowadzą również do zaburzeń psychicznych, charakteryzujących się gwałtownymi i nieprzewidywalnymi wahaniami nastroju, od niepohamowanej agresji po głęboką depresję, prowadząc w krótkim czasie do nieodwracalnych zmian w osobowości. Wtedy z pomocą musi wkroczyć już nie tylko pracownik socjalny, ale również psycholog czy psychiatra.

10 PODSUMOWANIE

Pod wpływem nowych technologii zmieniają się tradycyjne postacie zagrożeń wywołujące patologie społeczne i dysfunkcje oraz marginalizację rodziny, a jednocześnie pojawiają się nowe, mające ścisły związek z wykorzystaniem komputera i Internetu. Jako zamiennik realnego świata powstaje świat urojony, pozwalający tylko pozornie uciec od trosk dnia codziennnego. W nim coraz częściej i coraz dłużej przebywają dzieci i osoby dorosłe. Nie ulega więc wątpliwości, że edukacja pracowników służb społecznych w zakresie identyfikowania i przeciwdziałania zjawisku cyberzagrożeń przekłada się na efektywniejszą pomoc i wsparcie rodzin doświadczających problemów związanych ze światem wirtualnym. Pogłębiona wiedza z zakresu psychologicznych mechanizmów uzależnienia i zjawiska współuzależnienia oraz umiejętność jej stosowania w codziennej pracy z klientem pomocy społecznej są bardzo ważne. Badania pokazują, że pracownicy kształcący służby społeczne pytani o zagrożenia generowane przez media cyfrowe i technologie informacyjno-komunikacyjne zdają sobie z nich sprawę. Jednak wiedzę o tych zagrożeniach na poziomie ogólnym posiedli głównie z telewizji i prasy. Ośmiu na dziesięciu ankietowanych nie zna jakiegokolwiek podręcznika o zagrożeniach cyberprzestrzeni i sposobach przeciwdziałania negatywnym skutkom tego zjawiska, 2/3 badanych nie słyszało o jakichkolwiek działaniach mających na celu ochronę przed zagrożeniami cyberprzestrzeni, podejmowanymi w obecnym systemie pomocy społecznej, chociaż aż 96 proc. badanych uważa, że posiadanie wiedzy na temat zagrożeń cyberprzestrzeni jest istotne dla pracowników służb społecznych[7]. Zebrane w badaniu informacje o potrzebach szkoleniowych pracowników świadczą o dużym zapotrzebowaniu na szkolenia, niezależnie od faktu, czy pracownicy mają już za sobą udział w szkoleniach, czy nie. Wszyscy respondenci mają świadomość braków w wiedzy i umiejętnościach z zakresu pracy z osobą zagrożoną cyberprzemocą.

11 Unia Europejska już od wielu lat promuje innowacje i modernizację w polityce społecznej państw członkowskich. Wykluczenie w różnych sferach życia społecznego dotyka ciągle w Europie milionów ludzi. W Strategii „Europa 2020" Unia Europejska zakłada wydźwignięcie co najmniej 20 mln osób z sytuacji zagrożenia ubóstwem i wykluczeniem społecznym do 2020 r.[8]. Przed polską polityką społeczną, w związku z cyberzagrożeniami, stoją również nowe, poważne wyzwania.

---

[7] M. Jóźko, *Diagnoza i analiza pracowników instytucji kształcących i szkolących kadry służb społecznych w tym pracowników socjalnych*, Raport z badań ilościowych, Wyższa Szkoła Pedagogiczna TWP w Warszawie, Warszawa 2013.

[8] *Komunikat Komisji Europa 2020. Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu,* Bruksela, 3.3.2010, KOM(2010), 2020 wersja ostateczna.

BIBLIOGRAFIA:

Jóźko M., *Diagnoza i analiza pracowników instytucji kształcących i szkolących kadry służb społecznych w tym pracowników socjalnych*, Raport z badań ilościowych, Wyższa Szkoła Pedagogiczna TWP w Warszawie, Warszawa 2013.

Komunikat Komisji Europa 2020. Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu, Bruksela, 3.3.2010, KOM(2010), 2020 wersja ostateczna.

Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, Wspólny Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Komisja Europejska, Bruksela (07.02.2013).

Szymanek V., *Społeczeństwo informacyjne w liczbach 2013*, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013.

Ustawa z dnia 12 marca 2004 r. o pomocy społecznej, Dz.U. nr 64, poz. 593 z późn. zmianami.

ZADANIA POLICJI,
SZKOŁY, POMOCY SPOŁECZNEJ I INNYCH SŁUŻB SPOŁECZNYCH WOBEC CYBERZAGROŻEŃ

Ewa Flaszyńska

1 WPROWADZENIE

W Polsce nie ma jednej instytucji odpowiedzialnej za przeciwdziałanie cyberprzestępczości. Kompetencje w tym zakresie zostały dodane jako obowiązki i zadania uzupełniające do instytucji na co dzień dbających o bezpieczeństwo narodowe, przestrzeganie prawa i ochronę obywateli. Zapewnianiem i rozwijaniem zdolności jednostek organizacyjnych administracji publicznej do ochrony przed cyberzagrożeniami zajmuje się Rządowy Zespół Reagowania na Incydenty Komputerowe. Zespół działa od 1 lutego 2008 r.[1].

2 ZADANIA WYBRANYCH SŁUŻB SPOŁECZNYCH

Odpowiedzialność za koordynację działań przeciw cyberprzestępczości spoczywa na Ministerstwie Administracji i Cyfryzacji. Natomiast odpowiedzialność za podejmowanie działań przeciw cyberterroryzmowi, jako szczególnym przypadkom cyberprzestępstw, sprawuje Szef Agencji Bezpieczeństwa Wewnętrznego. Do podmiotów odpowiedzialnych za zapewnienie bezpieczeństwa cyberprzestrzeni w Polsce zalicza się także Ministerstwo Spraw Wewnętrznych, Ministerstwo Obrony Narodowej, Służbę Kontrwywiadu Wojskowego oraz podmioty sektora prywatnego. Propozycje działań o charakterze prawno-organizacyjnym, technicznym i edukacyjnym, których celem jest zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni zostały zapisane w „Rządowym Programie w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016"[2]. Jednym z priorytetów Programu jest konieczność uwrażliwienia obywateli na problem bezpieczeństwa teleinformatycznego, podnoszenia ich świadomości odnośnie bezpiecznych metod korzystania z Internetu. Każdy użytkownik komputera powinien pamiętać o tym, że korzystanie z globalnej sieci, oprócz niekwestionowanych korzyści niesie za sobą także szereg zagrożeń, z którymi się on zetknie. Dlatego tak ważne jest szerzenie wśród całego społeczeństwa świadomości istnienia niebezpieczeństw w globalnej sieci oraz konieczność przeciwdziałania cyberzagrożeniom[3].

3 ZNACZENIE DZIAŁAŃ POLICJI

W walkę z cyberprzestępczością zaangażowana jest głównie policja. W jej strukturach funkcjonuje Wydział Wsparcia Zwalczania Cyberprzestępczości Biura Kryminalnego Komendy Głównej Policji. Do jego obowiązków należy: rozpoznawanie i monitorowanie obszarów zagrożonych cyberprzestępczością; współdziałanie z administratorami i właścicielami sieci komputerowych, przedsiębiorcami telekomunikacyjnymi oraz podmiotami świadczącymi usługi drogą elektroniczną w sprawach o ustalenia operacyjne; identyfikowanie, dla krajowych i zagranicznych organów ścigania, sprawców przestępstw o znacznym stopniu skomplikowania, popełnianych z wykorzystaniem nowych technologii informatycznych; inicjowanie wdrażania narzędzi informatycznych służących zwalczaniu cyberprzestępczości; inicjowanie przedsięwzięć ukierunkowanych na usprawnianie systemu wymiany informacji o ustaleniach związanych z cyberprzestępczością[4]. Policja przyjmuje, że każda działalność w Internecie, na skutek której użytkownik czuje się źle, zagrożony, ośmieszony – słowem niekomfortowo, jest cyberprzemocą. Cyberprzemoc jest skodyfikowana w przepisach karnych. Podstawowym aktem prawnym, na którym opiera się walka policji z cyberprzestępczością w Polsce jest ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.). Wydział Wsparcia Zwalczania Cyberprzestępczości Biura Kryminalnego Komendy

[1] www.cert.gov.pl

[2] *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016,* Warszawa 2010.

[3] Tamże, s. 19–20.

[4] www.kgp.gov.pl

Głównej Policji współpracuje w tym zakresie z policjantami w terenie (w województwach, miastach itp.). Ponadto policjanci Komendy Głównej Policji współpracują z instytucjami międzynarodowymi. Policja, obok bieżącej pracy, organizuje szkolenia i spotkania, których tematami są szeroko rozumiane zagrożenia występujące w sieci oraz związane z telefonią komórkową.

4 DZIAŁALNOŚĆ INNYCH SŁUŻB

Ważnymi partnerami dla instytucji rządowych i innych podmiotów odpowiedzialnych za bezpieczeństwo teleinformatyczne w działaniach zmierzających do zwiększenia bezpieczeństwa w cyberprzestrzeni są podmioty administracji samorządowej, w tym instytucje oświatowe (i to nie tylko szkoły, ale także placówki oświatowo-wychowawcze takie jak szkolne schroniska młodzieżowe, młodzieżowe ośrodki wychowawcze, młodzieżowe ośrodki socjoterapii, specjalne ośrodki szkolno-wychowawcze oraz specjalne ośrodki wychowawcze dla dzieci i młodzieży wymagających stosowania specjalnej organizacji nauki, metod pracy i wychowania) i szeroko rozumianej pomocy społecznej (ośrodki pomocy społecznej, powiatowe centra pomocy rodzinie, placówki specjalistycznego poradnictwa, w tym rodzinnego, ośrodki wsparcia, ośrodki interwencji kryzysowej, placówki opiekuńczo-wychowawcze – domy dziecka, placówki wsparcia dziennego itp.).

5 Wraz z upowszechnieniem się dostępu do Internetu w domach, szkołach i miejscach pracy oraz zmianą sposobu przeprowadzania ataków komputerowych, świadomość i wiedza na temat sposobów przeciwdziałania i zwalczania zagrożeń stanowią kluczowe elementy walki z tymi zagrożeniami. Ciągle rosnąca liczba użytkowników sieci Internet, a także wzrost roli jaką pełni Internet w życiu człowieka pozwala prognozować rosnące niebezpieczeństwo wynikające z istniejących zagrożeń. Niepokojącym jest fakt, że szczególnie młodzież bardzo często wykorzystuje nowe rozwiązania technologiczne w sposób niekontrolowany, a uzależnienie od Internetu rozwija się stopniowo i niezauważalnie, wypierając dotychczasowe zainteresowania i obowiązki dziecka.

6 Z uwagi na fakt, że uzależnienie od Internetu, a tym samym większe narażanie się na cyberzagrożenia, staje się coraz powszechniejszym problemem społecznym, do najważniejszych działań możemy zaliczyć działania profilaktyczne mające na celu poszerzenie wiedzy w tym zakresie, podejmowane przez instytucje oświatowe i szeroko rozumianej pomocy społecznej.

7 EDUKACJA DZIECI I MŁODZIEŻY

Dzieci i młodzież to grupa najbardziej podatna na wpływy, stąd edukacja w zakresie cyberzagrożeń powinna rozpocząć się już od najmłodszych lat. Wraz z możliwością korzystania przez dzieci i młodzież z nowych rozwiązań technologicznych (nowe pomoce dydaktyczne tj. komputery, tablety, e-booki) coraz częściej można się spotkać z opinią, że tzw. cyberzagrożenia powoli zaczynają wypierać inne czyny karalne z polskich szkół. Celem działań edukacyjnych powinno być wytworzenie pewnych nawyków, które uchronią najmłodszych przed zagrożeniami czyhającymi na nich w sieci (np. przed zawieraniem niebezpiecznych znajomości, niecenzuralnymi treściami, piractwem, uzależnieniem od Internetu). Wiedzę na temat zagrożeń z cyberprzestrzeni dziecko powinno uzyskiwać przede wszystkim w szkole podczas nauki na wszystkich poziomach edukacji. Ogromna w tym rola nauczycieli. Od roku 2004 ich kształcenie w ramach specjalizacji odbywa się zgodnie z rozporządzeniem Ministra Edukacji Narodowej, określającym standardy

kształcenia nauczycieli[5]. W ramach zajęć obowiązkowych na studiach wyższych nauczyciele uzyskują podstawową wiedzę z zakresu technologii informacyjnej, w tym również bezpiecznego i świadomego korzystania z systemów teleinformatycznych. Zadaniem ich jest inicjowanie i propagowanie działań na rzecz bezpieczeństwa dzieci i młodzieży w Internecie, głównie podczas lekcji. Ale też podczas spotkań z rodzicami, bowiem to na rodzicach spoczywa odpowiedzialność za przygotowanie dzieci do funkcjonowania w społeczeństwie informacyjnym. Rodzice powinni sami posiąść więc odpowiednią wiedzę na temat zagrożeń oraz metod ich eliminowania.

8 POMOC SPOŁECZNA

Zadania instytucji pomocy społecznej sprowadzają się obecnie głównie do wykrywania uzależnień od Internetu i przestępstw w sieci, zgłaszania ich do odpowiednich instytucji oraz przekazywanie dzieciom i młodzieży a także ich rodzicom i opiekunom zasad bezpiecznego korzystania z sieci internetowej oraz zwiększenie świadomości społecznej dotyczącej zagrożeń związanych z cyberzagrożeniami. O tym, że służby społeczne muszą być zaznajomione z problematyką cyberzagrożeń świadczą choćby statystyki. W 2012 roku pomocą społeczną objęto 8,4% mieszkańców Polski. Ze świadczeń pomocy społecznej, niezależnie od ich rodzaju, liczby i źródła finansowania, w 2012 r. skorzystało 1 926 328 osób. Osoby te pochodziły z 1 218 692 rodzin, natomiast liczba wszystkich osób w tych rodzinach wyniosła 3 250 112. Ponadto 210 347 rodzin skorzystało z pomocy wyłącznie w postaci pracy socjalnej[6]. Jak pokazują statystyki, wśród rodzin objętych pomocą społeczną najczęściej występującym typem jest rodzina z dziećmi. Według metodologii przyjętej dla potrzeb unijnej Strategii Europa 2020, w Polsce ubogich lub wykluczonych dzieci (w wieku 0–17 lat) było ponad 2,1 miliona. Stanowiły one około 30% wszystkich dzieci w tym wieku[7].

9 PODSUMOWANIE

Bardzo ważne jest więc wyposażenie pracowników służb społecznych w odpowiednią wiedzę, tak aby praktykowana przez nich praca socjalna i pomoc specjalistyczna obejmowała czynności nakierowane bezpośrednio na wywoływanie w rodzinie pożądanych zmian, często stosowanie metodycznej pracy z indywidualnym przypadkiem, bądź profesjonalne zarządzanie zindywidualizowanym pakietem usług. Praca socjalna jest bowiem oparta na osobistej relacji pracownika-specjalisty i klienta. Działalność zawodowa pracownika służb społecznych wymaga więc stosunkowo szerokiego zestawu czynności specjalistycznych. A z nowymi zadaniami związanymi z nowymi technologiami wiąże się również podnoszenie jakości świadczonych usług społecznych.

10 Spoglądając na zadania policji, szkoły, pomocy społecznej i innych instytucji wobec cyberzagrożeń można powiedzieć, że najważniejsza obecnie jest edukacja pracowników administracji publicznej (rządowej i samorządowej) w zakresie zagadnień dotyczących bezpieczeństwa sieci. Ważna jest również kampania społeczna edukacyjno-prewencyjna realizowana za pośrednictwem środków masowego przekazu, przeprowadzanie rozmaitych akcji informacyjnych i kampanii edukacyjnych.

---

[5] Rozporządzenie Ministra Edukacji Narodowej z dnia 7 września 2004 r. w sprawie standardów kształcenia nauczycieli, Dz. U. Nr 207, poz. 2110.

[6] Dane Ministerstwa Pracy i Polityki Społecznej, www.mpips.gov.pl.

[7] Por. *Krajowy Program Przeciwdziałania Ubóstwu i Wykluczeniu Społecznemu 2020. Nowy wymiar aktywnej Integracji,* Ministerstwo Pracy i Polityki Społecznej, Warszawa 2013, s.9.

BIBLIOGRAFIA:

Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016, Warszawa 2010.

Rozporządzenie Ministra Edukacji Narodowej z dnia 7 września 2004 r. w sprawie standardów kształcenia nauczycieli, Dz. U. Nr 207, poz. 2110.

Krajowy Program Przeciwdziałania Ubóstwu i Wykluczeniu Społecznemu 2020. Nowy wymiar aktywnej Integracji, Ministerstwo Pracy i Polityki Społecznej, Warszawa 2013.

SŁUŻBY SPOŁECZNE WOBEC ZAGROŻEŃ CYBERPRZESTRZENI

BEZPIECZEŃSTWO
W SIECI – DZIAŁANIA NASK

Michał Chrzanowski
Tomasz Jordan Kruk

1 WPROWADZENIE

W niniejszym artykule opisano działania, inicjatywy i projekty instytutu badawczego NASK, czyli Naukowej i Akademickiej Sieci Komputerowej, mające na celu zwiększenie poziomu bezpieczeństwa korzystania z Internetu i samego Internetu. W artykule omówiono następujące zagadnienia:

- działalność i projekty realizowane przez funkcjonujący w ramach NASK zespół CERT Polska zajmujący się bezpieczeństwem teleinformatycznym w sieci Internet,
- temat bezpieczeństwa systemu nazw domenowych (DNS) w kontekście zarządzanej przez NASK domeny .pl i związane z tym inicjatywy NASK,
- działalność funkcjonującego w ramach NASK zespołu Dyżurnet.pl zajmującego się przyjmowaniem zgłoszeń o nielegalnych treściach w Internecie.

2 BEZPIECZEŃSTWO UŻYTKOWNIKÓW SIECI – DZIAŁALNOŚĆ CERT POLSKA

W strukturze NASK funkcjonuje zespół CERT Polska – pierwszy powstały w Polsce zespół reagowania na incydenty (ang. Computer Emergency Response Team). Aktywnie operując od 1996 roku w środowisku zespołów reagujących, stał się rozpoznawalnym i doświadczonym podmiotem w dziedzinie bezpieczeństwa komputerowego. Od początku istnienia rdzeniem działalności zespołu jest obsługa incydentów bezpieczeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej. Od 1998 roku CERT Polska jest członkiem międzynarodowego forum zrzeszającego zespoły reagujące – FIRST, a od roku 2000 należy do grupy roboczej europejskich zespołów reagujących – TERENA TF-CSIRT i działającej przy niej organizacji Trusted Introducer. W 2005 roku z inicjatywy CERT Polska powstało forum polskich zespołów abuse – Abuse FORUM, natomiast w 2010 r. CERT Polska dołączył do Anti-Phishing Working Group, stowarzyszenia gromadzącego firmy i instytucje aktywnie walczące z przestępczością w sieci.

3 Do głównych zadań zespołu CERT Polska należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci,
- aktywne reagowanie w wypadku wystąpienia bezpośrednich zagrożeń dla użytkowników,
- współpraca z innymi zespołami CERT w Polsce i na świecie,
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego,
- działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa, analizy złośliwego oprogramowania, systemów wymiany informacji o zagrożeniach,
- rozwijanie własnych narzędzi do wykrywania, monitorowania, analizy i korelacji zagrożeń,
- regularne publikowanie Raportu CERT Polska o bezpieczeństwie polskich zasobów Internetu,
- działania informacyjno-edukacyjne zmierzające do wzrostu świadomości w zakresie bezpieczeństwa teleinformatycznego, w tym:
  - publikowanie informacji o bezpieczeństwie w serwisie http://www.cert.pl/ oraz w serwisach społecznościowych Facebook i Twitter;

- organizacja corocznej konferencji o bezpieczeństwie sieci SECURE;
- niezależne analizy i testy rozwiązań z dziedziny bezpieczeństwa teleinformatycznego.

4 Poza standardową rolą przyjmowania zgłoszeń i reagowania na incydenty komputerowe, zespół – we współpracy z innymi komórkami NASK, w szczególności Pracownią Metod Bezpieczeństwa Sieci i Informacji z Pionu Naukowego NASK oraz z Działem Rozwoju Oprogramowania NASK – realizuje również projekty badawczo-wdrożeniowe, których rezultatem jest oprogramowanie wspierające CERT Polska, jak i inne instytucje zajmujące się bezpieczeństwem komputerowym w wynajdywaniu, przeciwdziałaniu i reagowaniu na ataki i inne incydenty komputerowe. Projekty te często mają charakter unikatowy w skali światowej, a CERT Polska jest rozpoznawany na świecie jako jeden z najbardziej kompetentnych ośrodków zajmujących się bezpieczeństwem sieci. Pracownicy CERT Polska mieli wiodącą rolę w wytworzeniu wielu merytorycznych dokumentów europejskiej agencji ENISA.

5 Wśród wielu realizowanych przez CERT Polska projektów warto wyróżnić:

n6 zbudowaną w całości przez CERT Polska platformę służącą do gromadzenia, przetwarzania i przekazywania informacji o zdarzeniach bezpieczeństwa w sieci. W ciągu roku przez platformę przetwarzane są dziesiątki milionów zdarzeń bezpieczeństwa z Polski i całego świata. n6 funkcjonuje w pełni automatycznie. Jej celem jest efektywne, niezawodne i szybkie dostarczenie dużych ilości informacji o zagrożeniach bezpieczeństwa właściwym podmiotom: właścicielom, administratorom i operatorom sieci. Źródłem danych systemu n6 jest wiele kanałów dystrybucyjnych dostarczających informacje o zdarzeniach bezpieczeństwa. Zdarzenia te wykrywane są w wyniku działań systemów wykorzystywanych przez różne podmioty zewnętrzne (takie jak inne zespoły CERT, organizacje bezpieczeństwa, producenci oprogramowania, niezależni eksperci od bezpieczeństwa, itp.) oraz systemów monitorowania obsługiwanych przez CERT Polska. Większość informacji aktualizowanych jest codziennie, niektóre częściej. Dodatkowym źródłem informacji o sieciach klienta mogą być wyniki działań operacyjnych CERT Polska. Dotyczy to również działań operacyjnych innych podmiotów – dane otrzymane jednorazowo z zewnątrz, za zgodą źródła mogą być dodawane do systemu w celu redystrybucji.

HoneySpider Network jest wspólnym projektem CERT Polska, rządowego CERT–u holenderskiego GOVCERT. NL oraz akademickiego operatora holenderskiego SURFnet. Projekt ma na celu zbudowanie nowych oraz wykorzystanie istniejących technik klienckich systemów honeypot do wykrywania ataków na aplikacje klienckie, w szczególności przeglądarki WWW. Projekt powstał w odpowiedzi na obserwacje nowego trendu w propagacji zagrożeń internetowych właśnie poprzez luki w aplikacjach klienckich, a nie jak dotychczas w aplikacjach serwerowych. System wykorzystuje zarówno rozwiązania niskointeraktywne (roboty emulujące przeglądarki), jak i rozwiązania wysokointeraktywne (przeglądarki uruchamiane i automatycznie sterowane z poziomu rzeczywistych systemów operacyjnych). Ideą systemu jest przeglądanie sieci Internet przez odpowiednio przygotowane automaty symulujące użytkownika Internetu z przeglądarką stron WWW

i prowokowanie do zainfekowania przeglądarki i systemu w celu uzyskania możliwości analizy kodu infekującego złośliwego oprogramowania.

Arakis – system wczesnego ostrzegania o zagrożeniach w sieci. Jego głównym zadaniem jest wykrywanie i opisywanie zautomatyzowanych zagrożeń występujących w sieci na podstawie agregacji i korelacji danych z różnych źródeł, w tym rozproszonej sieci systemów honeypot, sieci darknet, systemów firewall oraz systemów antywirusowych. Arakis jest próbą odpowiedzi na ataki dnia zerowego. Arakis stał się podstawą wspólnego przedsięwzięcia NASK i ABW nazwanego ARAKIS-GOV, które zostało wdrożone w ponad sześćdziesięciu jednostkach administracji centralnej. Rozwiązanie ARAKIS-GOV zostało nagrodzone w 2010 roku godłem Teraz Polska w kategorii innowacje. Aktualnie CERT Polska wraz z innymi komórkami NASK realizuje drugą unowocześnioną wersję systemu Arakis.

WOMBAT – niedawno zakończony projekt realizowany ze środków badawczych w ramach 7. Programu Ramowego Unii Europejskiej. Celem projektu było utworzenie globalnego systemu monitorowania i analizy zagrożeń internetowych, w szczególności złośliwego oprogramowania, które w ostatnich latach stało się potężnym narzędziem w rękach cyberprzestępców. Projekt powstał przy współpracy specjalistów ds. bezpieczeństwa z wielu podmiotów europejskich i innych zaangażowanych w działania monitorujące oraz zwiększające bezpieczeństwo Internetu. Badano nowe metody analizy zagrożeń pojawiających się masowo w Internecie, identyfikacji źródeł i przyczyn ich występowania. W projekcie wykorzystano m.in. informacje rejestrowane przez globalny rozproszony system rozwiązań honeypot Leurre.com, dane z największej na świecie kolekcji złośliwego oprogramowania zgromadzone przez firmę Hispasec w ramach projektu Virustotal, dane udostępnione przez zespół CERT Polska pochodzące z systemów Arakis oraz HoneySpider Network, jak również informacje pozyskane z globalnego systemu DeepSight Threat Management firmy Symantec.

6 BEZPIECZEŃSTWO USŁUG SIECI – OCHRONA SYSTEMU NAZW DOMENOWYCH

Naukowa i Akademicka Sieć Komputerowa pełni rolę krajowego rejestru nazw internetowych w domenie .pl, prowadząc rejestrację nazw domen nie tylko w domenie .pl, ale także w 152 domenach drugiego poziomu: domenach regionalnych (np. warszawa.pl) i funkcjonalnych (np. edu.pl).

7 NASK jest zarządcą domeny .pl w ogólnoświatowym systemie internetowych nazw domenowych. System nazw domenowych (DNS, ang. *Domain Name System*) stanowi zestawienie powiązań, które można przyrównać do książki telefonicznej zawierającej zamiast par: nazwa abonenta i jego numer telefonu, pary: nazwa komputera i odpowiadający jej adres IP. Nadrzędną funkcją systemu DNS jest zamiana wygodnych dla użytkowników nazw i adresów, reprezentowanych przez nazwy domenowe na skojarzone z nimi adresy IP – identyfikatory numeryczne, które jednoznacznie określają logiczną lokalizację w sieci danego komputera bądź innego urządzenia. Przykładowo ciąg znaków *www.nask.pl* to właśnie nazwa domenowa, a system DNS zajmuje się między innymi przechowywaniem relacji i tłumaczeniem nazwy domenowej na odpowiadający jej adres IP, w tym wypadku 195.187.240.100.

8 DNS jest usługą krytyczną dla funkcjonowania Internetu. Prak-

tycznie wszystkie pozostałe usługi, w tym poczta elektroniczna czy sieć WWW, polegają na dostępności prawidłowo funkcjonującego systemu DNS. Gdy system DNS przestaje działać, zazwyczaj przestają działać wszystkie bez wyjątku pozostałe usługi sieciowe – nawet jeżeli dostęp do sieci na poziomie niskopoziomowych protokołów sieciowych funkcjonuje prawidłowo.

9 DNS jest też systemem ogromnej skali. Według danych przedstawionych przez portal DomainTools w lutym 2011 r. było 321 mln nazw domenowych zarejestrowanych w domenie .com, 35 mln nazw domenowych zarejestrowanych w domenie .net oraz 21 mln nazw domenowych zarejestrowanych w domenie .org. Na przełomie 2012 i 2013 r. liczba zarejestrowanych domen w NASK przekroczyła dwa i pół miliona.

10 Przy projektowaniu pierwotnej koncepcji i architektury systemu DNS nie położono szczególnego nacisku na jego bezpieczeństwo. Istnieją zarówno techniki, jak i gotowe narzędzia pozwalające bardziej wyrobionym technicznie użytkownikom Internetu na zakłócanie stabilnej pracy DNS przy wykorzystaniu luk w jego bezpieczeństwie. Przykładem mogą być ataki polegające na podstawianiu fałszywych informacji DNS w celu nieautoryzowanego przejęcia domeny lub skierowania połączeń do specjalnie przygotowanego złośliwego serwera – np. serwującego podrobioną stronę banku lub wirusy.

11 Metodą przeciwdziałania zagrożeniom dla infrastruktury klienckiej jest wymuszenie uwierzytelniania źródła i kontroli integralności danych przesyłanych w pakietach – cel ten osiągnąć można poprzez wdrożenie rozwiązania DNSSEC. DNSSEC jest rozszerzeniem bezpieczeństwa systemu DNS, wprowadzającym mechanizm autoryzacji i zapewnienia integralności wiadomości przesyłanych w systemie DNS. DNSSEC jest protokołem opartym na cyfrowych podpisach, wykorzystującym sprawdzone mechanizmy kryptograficzne bazujące na kluczach asymetrycznych. Protokół zabezpiecza informacje DNS przed sfałszowaniem i modyfikacją, oferując dodatkowo możliwość wykorzystania go jako infrastruktury do dystrybucji kluczy publicznych. Użytkownik systemu może mieć pewność, że otrzymał dane wiarygodne, pochodzące z właściwego źródła i niezmienione w trakcie przesyłania.

12 DNSSEC wprowadzając mechanizm autoryzacji i nienaruszalności danych w DNS, może skutecznie chronić użytkowników Internetu przed sfałszowanymi danymi, które wprowadzane są do systemu DNS, na przykład w celu dokonania kradzieży informacji lub manipulowania przy różnych typach transakcji internetowych, jak chociażby zakupy elektroniczne.

13 Jak trudnym zagadnieniem jest samo wdrożenie właściwych mechanizmów zabezpieczających DNS, niech świadczy historia DNSSEC. Otóż pierwsze poważne podatności DNS zostały wykryte już w roku 1990, a w 1995 ukazał się artykuł, który pokazywał metody wykorzystywania tych podatności. W 1997 r. opublikowano RFC 2065, *Domain Name System Security Extensions*, a w 1999 poprawioną i w ówczesnej ocenie gotową do wdrożenia wersję rozwiązania w postaci dokumentu RFC 2535. Jednak dopiero od 2008 roku można mówić o domkniętej kompletnej i poprawnej koncepcji rozwiązania DNSSEC. Koncepcja formalnie dojrzewała przez 11 lat.

14 NASK uważnie monitorował i testował ewoluujące propozycje zabezpieczania systemu domen internetowych. Pierwsze eksperymenty z DNSSEC rozpoczęto już w 2005 roku. W 2010 r. po pełnej analizie zagadnienia

zainicjowano prace zmierzające do produkcyjnego zabezpieczenia administrowanych przez NASK domen protokołem DNSSEC. Produkcyjne zabezpieczenie domeny .pl oraz wybranych pozostałych, administrowanych bezpośrednio przez NASK wdrożono w 2012 roku.

15 BEZPIECZEŃSTWO NAJMŁODSZYCH – DYŻURNET.PL I INNE INICJATYWY

NASK stara się dbać o bezpieczeństwo Internetu i jego użytkowników nie tylko poprzez działania i inicjatywy w warstwie technicznej, ale również w warstwie popularyzatorskiej i społecznej, ze szczególną troską o dobro najmłodszych internautów.

To właśnie dzieci najszybciej zaadaptowały cyfrowy styl życia. Według badania z 2007 roku „Dzieci aktywne on-line" (Megapanel i Gemius SA):

- niemal co drugie dziecko to tak zwany *heavy user* (korzysta z Internetu codziennie lub prawie codziennie),
- 11% wszystkich Internautów to dzieci między 7 a 14 rokiem życia,
- 34% to młodzi ludzie między 15 a 24 rokiem życia,
- 70% dzieci korzystających z Internetu tworzy swoją internetową przestrzeń, korzystając z serwisów społecznościowych,
- ponad 70% dzieci gra w gry online.

16 Według przeprowadzonego na ogromną skalę (25 142 respondentów) europejskiego badania EU Kids Online z 2011 r.[1]:

98% dzieci korzysta z Internetu przynajmniej raz w tygodniu, z czego 74% codziennie lub prawie codziennie,

52% aż taki odsetek dzieci w Polsce ma swój komputer prywatny, podczas gdy średni poziom w Europie to 34%,

60% dzieci w Polsce korzysta z serwisów społecznościowych,

63% to odsetek rodziców, którzy – mimo że ich dzieci doświadczyły cyberprzemocy – odpowiedzieli, iż ich dziecko nie ma takich doświadczeń,

54% aż tylu rodziców nie wiedziało, że ich dziecko spotkało się na żywo z kimś poznanym przez Internet.

17 Wyniki powyższych badań uzasadniają szczególną wagę przykładaną przez NASK do zapewniania bezpiecznego korzystania z sieci najmłodszym jej użytkownikom – dzieciom. Problem jest poważny, gdyż poza ewidentnymi korzyściami edukacyjnymi i atrakcyjną formą rozwijającego spędzania czasu, Internet niesie dla jego młodych użytkowników wiele możliwych rodzajów ryzyka i potencjalnych zagrożeń:

- kontakt ze szkodliwymi treściami (pornografia, treści brutalne, rasizm, ksenofobia, propagowanie anoreksji, samobójstw),
- uwodzenie dzieci za pośrednictwem Internetu (grooming),
- pornografia dziecięca,
- nękanie za pośrednictwem sieci (cyberprzemoc),
- prostytucja dziecięca,
- złamanie prawa lub/ i narażenie na straty finansowe,
- uzależnienie od Internetu.

18 Zespół Dyżurnet.pl jest działającym w NASK punktem kontaktowym, który przyjmuje zgłoszenia dotyczące nielegalnych treści w Internecie. Do zadań zespołu należy m.in. analiza treści wskazanych przez użytkowników, wykonanie dokumentacji technicznej, przesłanie informacji do policji, prokuratury, administratorów serwisów internetowych czy też zagranicznych punktów

1 L. Kirwil *Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo – część 2.* Częściowy raport z badań EU Kids Online II przeprowadzonych wśród dzieci w wieku 9—16 lat i ich rodziców, SWPS – EU Kids Online – PL, Warszawa 2011.

kontaktowych zrzeszonych w inicjatywie INHOPE. Od początku powstania w 2005 roku zespół przeanalizował ponad 27 tysięcy zgłoszeń.

19 Zespół Dyżurnet.pl jest również elementem Polskiego Centrum Programu Safer Internet, realizowanego w ramach programu Komisji Europejskiej Safer Internet, który ma za zadanie promowanie bezpiecznego korzystania z nowych technologii przez dzieci i młodzież, a także walkę z treściami nielegalnymi.

20 Projekt Komisji Europejskiej Safer Internet jest programem Komisji Europejskiej, którego główny cel to promocja bezpiecznego korzystania z nowych technologii i Internetu wśród dzieci i młodzieży. Cele szczegółowe projektu obejmują między innymi: działania na rzecz zwalczania nielegalnych treści i spamu w Internecie oraz problematykę związaną z zagrożeniami wynikającymi z użytkowania telefonów komórkowych, gier online, wymiany plików P2P i innych form komunikacji online (czaty, komunikatory, itp.).

21 Polskie Centrum Programu Safer Internet (PCPSI) powołano w styczniu 2005 r., a NASK jest koordynatorem Centrum. Działania podejmowane przez PCPSI obejmują:

- kampanie medialne,
- szkolenia i konferencje,
- edukację dzieci i młodzieży,
- organizację Dnia Bezpiecznego Internetu,
- realizację projektów badawczych,
- współpracę krajową i międzynarodową.

22 Ponadto NASK jest pomysłodawcą i realizatorem wielu innych projektów, w tym m.in. „Bądźmy bezpieczni w Internecie", „Przygody Plika i Foldera w Sieci" i konkursu na plakat „Tworzymy bezpieczny Internet". W 2011 roku działalność edukacyjna została rozszerzona o program „Senior dla Seniora", skierowany do osób w kategorii wiekowej 50+. Zainaugurowany został również program „Kursor", dotyczący bezpiecznego korzystania z nowych technologii, multimediów oraz zastosowania edutainment w praktyce szkolnej i życiu codziennym. Oferta edukacyjna skierowana jest do wielu odbiorców w różnych grupach wiekowych – do dzieci, młodzieży oraz dorosłych: rodziców, opiekunów, nauczycieli, wykładowców akademickich, a także do pracowników instytucji publicznych oraz do przedstawicieli wymiaru sprawiedliwości. Działania edukacyjne i popularyzatorskie mające na celu zwiększenie świadomości w zakresie bezpieczeństwa dzieci i młodzieży w Internecie realizowane są w dziale Akademia NASK.

23 NASK aktywnie uczestniczy także w takich wydarzeniach jak Festiwal Nauki oraz Piknik Naukowy, który corocznie organizowany jest przez Polskie Radio S.A. i Centrum Nauki Kopernik.

24 PODSUMOWANIE

Dokonano przeglądu aktualnych inicjatyw i aktywności NASK w zakresie zwiększania bezpieczeństwa Internetu i użytkowników Internetu. Więcej zawsze aktualnych informacji można uzyskać na stronach źródłowych, składowych powyższego zestawienia typów działań:
CERT Polska – http://www.cert.pl/
DNS w domenie .pl – http://www.dns.pl/
Dyżurnet.pl – http://www.dyzurnet.pl/
oraz oczywiście na stronie głównej NASK: http://www.nask.pl/.

BIBLIOGRAFIA:

Kruk T. J., *Informatyczne problemy bezpieczeństwa w Internecie* w: *Internet. Ochrona wolności, własności i bezpieczeństwa*, Szpor G. (red.), CH Beck, 2011 r.

Chrzanowski M., Kruk T. J., *Bezpieczeństwo domen internetowych - system DNSSEC* w: *Cyberprzestępczość i ochrona informacji*, Hołyst B., Pomykała J., (red.), Wydawnictwo WSM, 2012 r.

Chrzanowski M., Kruk T. J., *Bezpieczeństwo systemu nazw domenowych* w: *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, Szpor G., Wiewiórowskiego W. R., (red.), CH Beck, 2012 r.

Internet Security Threat Report, Symantec, 04.2012, http://www.symantec.com/

Badanie Dzieci aktywne on-line, n=831, Megapanel PBI i Gemius SA, 2007 r.

Badanie EU KIDS ONLINE/2010 w 25 krajach Europy, n=23420

Raporty z działalności CERT Polska, www.cert.pl/raporty

Raporty dotyczące rynku domen w Polsce, www.dns.pl/news/press.html

Raporty z działalności Dyżurnet.pl, www.dyzurnet.pl/pobierz.html

DZIAŁANIA FUNDACJI
DZIECI NICZYJE

1 WPROWADZENIE

Korzystanie z Internetu jest obecnie codziennością dzieci i młodzieży w Polsce. Badania EU Kids Online II[1] pokazują, że 98% polskich dzieci w wieku 9—16 lat loguje się przynajmniej raz na tydzień, a 74% codziennie, 24% 1—2 razy w tygodniu. Mimo że polskie dzieci stosunkowo późno przeżywają swoją pierwszą przygodę z Internetem (9 lat), to wiek ten stale obniża się.

2 DZIAŁALNOŚĆ FUNDACJI DZIECI NICZYJE

Problem internetowych zagrożeń został na większą skalę dostrzeżony w ostatnich latach i w związku z rosnącą popularnością sieci wśród najmłodszych użytkowników stał się przedmiotem troski wielu podmiotów. Fundacja Dzieci Niczyje zajęła się tematyką bezpieczeństwa dzieci i młodzieży w Internecie w 2004 roku. Wtedy to ruszyła pierwsza w Polsce kampania poruszająca problem internetowych zagrożeń pod hasłem „Nigdy nie wiadomo, kto jest po drugiej stronie" i zainicjowany został program „Dziecko w Sieci". Celem programu jest zwrócenie uwagi dorosłych i dzieci na problem bezpieczeństwa online, nauczenie najmłodszych bezpiecznego poruszania się po Internecie oraz pomoc im w sytuacjach zagrożenia w sieci.

3 POLSKIE CENTRUM SAFER INTERNET

Od stycznia 2005 roku Fundacja Dzieci Niczyje wraz z NASK tworzą **Polskie Centrum Programu Safer Internet**, które realizuje kompleksowe działania na rzecz bezpieczeństwa dzieci i młodzieży online (w ramach programu Komisji Europejskiej „Safer Internet"). Głównym partnerem większości działań jest Fundacja Orange.

4 W ramach Polskiego Centrum Programu Safer Internet realizowane są jednocześnie trzy projekty:

• **Saferinternet.pl** – kompleksowe działania edukacyjne i medialne na rzecz bezpiecznego korzystania z Internetu i nowych technologii przez dzieci i młodzież; www.saferinternet.pl

• **Helpline.org.pl** – projekt, w ramach którego udzielana jest pomoc młodym internautom, rodzicom i profesjonalistom w wypadkach zagrożeń związanych z korzystaniem z Internetu oraz telefonów komórkowych przez dzieci i młodzież; www.helpline.org.pl

• **Dyzurnet.pl** – punkt kontaktowy, tzw. hotline, przyjmujący zgłoszenia o treściach nielegalnych w Internecie, takich jak: pornografia dziecięca, rasizm i ksenofobia.
www.dyzurnet.pl

5 Saferinternet.pl

W ramach projektu Saferinternet.pl realizowane są kompleksowe działania edukacyjne i medialne na rzecz bezpiecznego i odpowiedzialnego korzystania z nowych mediów przez dzieci i młodzież. Projekt prowadzony jest przez FDN i NASK. Koordynatorem projektu jest FDN. Głównym partnerem większości realizowanych w jego ramach działań jest Fundacja Orange.

6 Kampanie medialne

Kampanie medialne mają na celu nagłaśnianie zagrożeń związanych z korzystaniem z Internetu przez dzieci oraz promowanie wśród dzieci, młodzieży i ich rodziców postaw sprzyjających bezpieczeństwu młodych internautów. Celem kampanii medialnych jest również promocja oferty Polskiego Centrum Programu Safer Internet.

[1] L. Kirwil, *Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo – część 2. Częściowy raport z badań EU Kids Online II przeprowadzonych wśród dzieci w wieku 9—16 lat i ich rodziców*. Warszawa 2011, SWPS – EU Kids Online – PL

Wybrane kampanie medialne:

• **Nigdy nie wiadomo, kto jest po drugiej stronie** – 2004 r.
– kampania poświęcona problemowi uwodzenia dzieci w Internecie.

• **Dyżurujemy przy Internecie** – 2006 r.
– kampania mająca na celu promocję oferty Dyżurnet.pl i uwrażliwienie internautów na istnienie nielegalnych treści publikowanych w Internecie, w szczególności pornografii dziecięcej.

• **Internet to okno na świat. Cały świat** – 2007 r., 2009 r.
– kampania poruszająca problem kontaktów dzieci z niebezpiecznymi treściami w sieci.

• **Stop cyberprzemocy** – 2008 r.
– kampania dotycząca problemu przemocy rówieśniczej z użyciem Internetu i telefonów komórkowych.

• **Baw się w Sieci. Bezpiecznie** – 2009 r.
– kampania dotycząca cyberprzemocy oraz bezpieczeństwa dzieci w serwisach społecznościowych.

• **Pomyśl zanim wyślesz** – 2010 r.
– kampania zwracająca uwagę na konsekwencje nieprzemyślanego umieszczania informacji oraz zdjęć w Internecie.

• **Każdy ruch w Internecie zostawia ślad** – 2010 r.
– kampania ukazująca problem uwodzenia dzieci online, ze szczególnym uwzględnieniem nowych regulacji prawnych w tym zakresie.

• **Internet to nie zabawa. To Twoje życie** – 2011 r.
– kampania ukazująca wpływ aktywności online na realne życie.

• **Promocja bezpieczeństwa w sieci** – 2011 r.
– kampania, której celem było zwrócenie uwagi rodziców na ich rolę w edukacji internetowej dzieci.

• **Nie akceptuję, nie łączę się, nie wchodzę...** – 2011 r.
– kampania poświęcona działalności zespołu Dyżurnet.pl, przyjmującego zgłoszenia o nielegalnych treściach w sieci.

• **W którym świecie żyjesz?** – 2012 r.
– kampania poświęcona problemowi nadmiernego korzystania z komputera i Internetu przez dzieci i młodzież.

7 MATERIAŁY EDUKACYJNE

Fundacja Dzieci Niczyje we współpracy z Fundacją Orange opracowuje ofertę edukacyjną dla dzieci, rodziców oraz profesjonalistów. Obejmuje ona scenariusze zajęć lekcyjnych, kursy e-learning, materiały multimedialne (prezentacje, filmy, kreskówki) oraz wydawnictwa (broszury, plakaty, komiksy, książki). Materiały edukacyjne dystrybuowane są do szkół podstawowych i gimnazjalnych w całej Polsce oraz dostępne są na stronie *www.dzieckowsieci.fdn.pl.* Kursy e-learning znajdują się pod adresem *www.fdn.pl/kursy*.

8 PROJEKT EDUKACYJNY Sieciaki.pl

Sieciaki.pl to projekt edukacyjny Fundacji Dzieci Niczyje adresowany do młodych internautów, którego celem jest edukacja w zakresie bezpiecznego korzystania z Internetu. Głównym elementem projektu jest serwis www.sieciaki.pl, którego użytkownicy biorą udział w grach edukacyjnych, quizach i konkursach. Ważnym elementem projektu jest również, prowadzona wspólnie z Fundacją Orange, akcja Sieciaki na Wakacjach, w ramach której latem organizowane są imprezy

plenerowe, koncerty oraz zajęcia edukacyjne dla dzieci i młodzieży. Od 2012 r. akcja została uzupełniona o wakacyjne pakiety edukacyjne, których elementem jest scenariusz, pozwalający osobom zainteresowanym na zorganizowanie pikniku w swojej miejscowości.

9 PROJEKT Necio.pl

Necio.pl to projekt edukacyjny skierowany do dzieci w wieku 4—5 lat, przeznaczony do nauki bezpiecznego korzystania z Internetu. Na potrzeby projektu powstał serwis internetowy (www.necio.pl) zawierający animacje, gry oraz piosenki tłumaczące najmłodszym zasady bezpiecznego surfowania.

10 PRZEGLĄDARKA „BeSt"

„BeSt" to przeglądarka bezpiecznych stron internetowych dla dzieci w wieku od 3 do 10 lat, dzięki której rodzice mogą wspólnie z dziećmi odkrywać uroki Internetu lub zapewnić im bezpieczne, samodzielne korzystanie z sieci. Program blokuje dostęp do stron spoza katalogu BeSt. Przeglądarka znajduje zastosowanie zarówno w komputerach domowych, jak i szkołach, bibliotekach, domach kultury czy kawiarenkach internetowych. Program można pobrać ze strony: www.best.fdn.pl

11 MAGAZYN „Numa Numa"

„Numa Numa" to magazyn skierowany do młodzieży i poświęcony fenomenom Internetu, mediom elektronicznym i bezpieczeństwu w sieci. Wydawany jest w wersji papierowej oraz elektronicznej (www.numanuma.pl); ukazuje się kilka razy w roku.

12 PROJEKT „ZOSTAŃ ZNAJOMYM SWOJEGO DZIECKA"

Projekt edukacyjny adresowany do rodziców i opiekunów w celu zachęcenia ich do aktywnego uczestniczenia w internetowym życiu dzieci, poznania ich zainteresowań i wirtualnej społeczności, a także zagrożeń, na jakie mogą trafić podczas surfowania po sieci. Na projekt składa się pięć animowanych filmów, które w zabawny sposób pokazują internetowe rodzinne perypetie. Akcja realizowana jest przez NASK.

13 SZKOLENIA I KONFERENCJE DLA PROFESJONALISTÓW

Szkolenia i konferencje poświęcone problematyce bezpieczeństwa dzieci w Internecie kierowane są do przedstawicieli sektora edukacyjnego, wymiaru sprawiedliwości i organów ścigania, organizacji pozarządowych oraz dostawców usług i treści internetowych. Corocznie, pod patronatem unijnej Komisarz ds. Mediów i Społeczeństwa Informacyjnego, organizowana jest Międzynarodowa Konferencja Bezpieczeństwo Dzieci i Młodzieży w Internecie, podczas której prezentowane są m.in. polskie i zagraniczne innowacyjne projekty edukacyjne oraz najnowsza wiedza dotycząca zwalczania nielegalnych treści w sieci (www.www.saferinternet.pl/konferencja).

14 DZIEŃ BEZPIECZNEGO INTERNETU

Międzynarodowy Dzień Bezpiecznego Internetu organizowany jest co roku w lutym i ma na celu nagłośnienie problematyki bezpieczeństwa online oraz promowanie inicjatyw na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych. Organizatorzy DBI w Polsce zachęcają szkoły oraz inne instytucje i organizacje do podejmowania lokalnych działań edukacyjnych związanych z bezpieczeństwem dzieci w sieci. Inicjatywy rejestrowane są w serwisie www.dbi.pl i biorą udział w konkursach z atrakcyjnymi nagrodami.

15 KONSULTACJE Z DZIEĆMI

Regularne konsultacje z dziećmi i młodzieżą pozwalają na projektowanie efektywnych narzędzi edukacyjnych i kampanii medialnych oraz ewaluację prowadzonych działań. Konsultacje takie odbywają się w ramach spotkań Panelu Młodzieżowego, w skład którego wchodzi grupa 13- i 14-letnich uczniów, dzięki kontaktom z użytkownikami portalu Sieciaki.pl oraz w ramach spotkań Kongresu Młodych Internautów.

16 BADANIA, RAPORTY, ANALIZY

Systematyczne badania dotyczące wiedzy, doświadczeń i postaw związanych z zagrożeniami wobec dzieci w Internecie są podstawą do planowania działań medialnych i edukacyjnych oraz wytyczają kierunki rozwoju projektu. Badania obejmują zarówno dzieci i młodzież, jak i rodziców oraz profesjonalistów.

17 Helpline.org.pl

Projekt prowadzony przez Fundację Dzieci Niczyje oraz Fundację Orange. W jego ramach udzielana jest pomoc młodym internautom, rodzicom i profesjonalistom w wypadkach zagrożeń związanych z korzystaniem z Internetu oraz telefonów komórkowych przez dzieci.
Konsultanci Helpline.org.pl udzielają pomocy m.in. w sytuacjach:

- uwodzenia dzieci w sieci (grooming),
- przemocy rówieśniczej z wykorzystaniem Internetu i telefonów komórkowych,
- kontaktu dzieci ze szkodliwymi treściami,
- nadmiernego korzystania z komputera i/lub Internetu przez dzieci.

Adresatami projektu są:

- dzieci i młodzież, gdy:
  - ktoś je ośmiesza, szantażuje, wysyła wulgarne wiadomości,
  - ktoś na czacie zadaje im krępujące pytania, prosi o zdjęcie, namawia na spotkanie,
  - ktoś wysyła lub prezentuje im treści zawierające pornografię lub przemoc.

- rodzice, gdy:
  - nie wiedzą, jak rozmawiać z dzieckiem o bezpieczeństwie w Internecie,
  - są zaniepokojeni tym, czym ich dzieci zajmują się w Internecie,
  - mają podejrzenie, że ich dziecko padło ofiarą cyberprzemocy,
  - ich dzieci miały kontakt ze szkodliwymi treściami (np. pornografia, przemoc, propagowanie narkotyków, faszyzmu, działalności sekt),
  - niepokoją ich znajomości, jakie ich dzieci zawierają w Internecie.

- profesjonaliści, gdy:
  - potrzebują konsultacji w zakresie przypadku krzywdzenia dziecka w sieci.

Możliwe formy kontaktu z konsultantami Helpline.org.pl:

- 800 100 100 (połączenie bezpłatne),
- e-mail: helpline@helpline.org.pl,
- rozmowa online (livechat) na stronie www.helpline.org.pl,
- formularz kontaktowy na stronie www.helpline.org.pl.

18 Dyzurnet.pl

Dyżurnet.pl to punkt kontaktowy prowadzony przez NASK, którego zadaniem jest reagowanie na zgłoszenia nielegalnych treści w Internecie.

W świetle polskiego prawa treści nielegalne to materiały prezentujące:

- treści pornograficzne z udziałem dzieci,
- treści pornograficzne związane z prezentowaniem przemocy lub posługi-

waniem się zwierzęciem,
- treści o charakterze rasistowskim lub ksenofobicznym.

19 Nielegalne treści napotkane w Internecie można zgłaszać do Dyżurnet.pl:
- poprzez formularz na stronie www.dyzurnet.pl,
- mailem na adres: dyzurnet@dyzurnet.pl,
- telefonicznie pod numerem: 801 615 005.

20 Zgłoszenia można dokonać anonimowo. Do zadań zespołu Dyżurnet.pl należy analiza treści nielegalnych i przygotowanie dokumentacji technicznej. Przypadki naruszenia prawa są przekazywane organom ścigania (jeśli serwer znajduje się w Polsce lub kraju, gdzie nie funkcjonuje zespół zrzeszony w INHOPE). Zespół współpracuje również z dostawcami usług i treści internetowych w celu jak najszybszego usuwania niepożądanych treści z sieci.

21 Dyżurnet.pl należy do sieci INHOPE – międzynarodowego stowarzyszenia zrzeszającego hotline'y z całej Europy i świata. Misją INHOPE jest zapewnienie szybkiej i skutecznej reakcji na zgłoszenia dotyczące nielegalnych treści w sieci niezależnie od kraju, w którym zostały zamieszczone, oraz propagowanie dobrych praktyk i wspieranie nowo powstających zespołów reagujących.

22 **PODSUMOWANIE**

Działania Fundacji Dzieci Niczyje należy uznać za niezwykle wszechstronne. Znaczący dorobek Fundacji z pewnością może i powinien stać się inspiracją dla kolejnych inicjatyw w tym zakresie (dop. red.).

PODSTAWOWE
ZAGROŻENIA ZDROWOTNE ZWIĄZANE Z UŻYWANIEM KOMPUTERA I INTERNETU

Wojciech Duranowski

OPIS ZJAWISKA

ROZPOZNANIE OBJAWY

DOBRE PRAKTYKI

ĆWICZENIA 1

WPROWADZENIE

1 W rozdziale tym przedstawione zostaną najważniejsze zagrożenia zdrowia psychicznego oraz fizycznego związane z Internetem, które zostały uznane za jednostki chorobowe lub są na etapie obserwacji związanej z zaliczeniem ich do zaburzeń chorobowych. Ze względu na stosunkowo nową tematykę zagrożeń zdrowotnych Internetu, środowiska lekarskie nie śpieszą się z uznaniem dolegliwości związanych z wykorzystywaniem komputera jako choroby. Dotyczy to szczególnie zagrożeń zdrowia psychicznego, gdzie jak dotychczas nie uznano Zespołu Uzależnienia od Internetu za jednostkę chorobową, mimo to Amerykańskie Towarzystwo Psychiatryczne umieściło rekomendację do dalszego badania, co pozwala mieć nadzieję na uznanie go za chorobę w przyszłości. Kwestie zagrożeń zdrowia psychicznego oraz fizycznego z pewnością wymagają dalszych badań oraz działań edukacyjnych i prewencyjnych redukujących ich negatywny wpływ na życie użytkowników komputera.

DOLEGLIWOŚCI WZROKU
(ang. Computer Vision Syndrome, CVS)

2 DEFINICJA

Tym terminem określamy dolegliwości oczu spowodowane przeciążeniem związanym ze zbyt długą pracą przy komputerze. W obecnych czasach dolegliwości te są najczęściej związane z pracą, jednakże mogą one dotyczyć również nadmiernego wykorzystywania komputera do celów rozrywkowych. Syndrom ten dotyczy nie tylko dorosłych, ale również młodzieży i dzieci, często używających komputerów przystosowanych dla osób dorosłych – chodzi tu przede wszystkim o położenie biurka, wysokość krzesła oraz kąt nachylenia ekranu.

3 ROZPOZNANIE PROBLEMU OBJAWY

Amerykańskie Stowarzyszenie Okulistyczne wskazuje na następujące syndromy występowania CVS:

- przemęczenie wzroku (Astenopia)
- zmęczenie
- ból głowy
- utrata ostrości wzroku
- podwójne widzenie (diplopia)
- senność
- trudności w czytaniu oraz koncentracji
- podrażnione oczy

4 DOBRE PRAKTYKI – przeciwdziałania, rozwiązywanie

W ramach prewencji związanej z CVS należy zapewnić osobie używającej komputera jak najkorzystniejsze warunki do korzystania z niego, począwszy od pomieszczenia, które jest odpowiednio oświetlone i ma odpowiednią temperaturę – sugerowana to 20–24 stopnie Celsjusza. Jak stwierdza inż. Jan Kotowski, bardzo istotne przy organizacji pracy na komputerze jest odpowiednie dobranie oświetlenia, najlepsze pomieszczenia do pracy na komputerze to te, które mają okna skierowane na stronę północną[1].

[1] J. Kotowski, *Praca przy komputerze: Zagrożenia, Zasady bezpiecznej pracy*.

Najkorzystniejsze dla oczu osoby pracującej przy komputerze jest oświetlenie ogólne, bez używania dodatkowego oświetlenia punktowego ze względu na możliwość powstawania olśnienia[2]. Częstym błędem popełnianym przez osoby użytkujące komputer jest ustawianie lamp biurkowych ze światłem skierowanym bezpośrednio na monitor w celu zwiększenia jego jaskrawości, co powoduje odbijanie się światła od monitora i jest szkodliwe dla oczu. Zalecana odległość od monitora przez Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy to 400 do 750 milimetrów, przy czym odległość od innego monitora nie powinna być mniejsza niż 60 cm[3]. Sugerowana jest praca na jasnym tle, przy wykorzystywaniu ciemnej (najlepiej czarnej) czcionki i dużych liter, co najmniej standardowej wielkości 12 pkt. Mniejsze czcionki wymagają większego wytężania wzroku i działają niekorzystnie na użytkownika, także na jego wzrok. Zaleca się wykorzystywanie nowoczesnych monitorów, najlepiej ekranów ciekłokrystalicznych z aktywną matrycą (LCD TFT), ze względu na obraz dużo większej jakości, lepsze barwy, a także brak emisji promieniowania rentgenowskiego szkodliwego dla oczu[4]. Komputer powinien być ustawiony równolegle do okna w pomieszczeniach, należy starać się unikać ustawienia prostopadłego, jako powodującego olśnienia oraz odbicia światła. W przypadku ustawienia monitora równolegle do okna, należy również zaopatrzyć okna w żaluzje, tak aby regulować strumienie światła wpadające do pomieszczenia, w celu zapobiegania szkodliwym odbiciom oraz olśnieniu. Ze względu na osiadanie kurzu na monitorze, należy regularnie przecierać powierzchnię monitora gładkim kawałkiem materiału w celu zapewnienia optymalnej widoczności. Osoba użytkująca komputer powinna mieć odpowiednio dobrane biurko wraz z przestrzenią do wykonywania swoich działań.

W wypadku dzieci wykorzystujących komputer do grania lub do prac domowych wielkość biurka, odległość oraz krzesło powinny być dostosowane do ich wieku. Istotną kwestią przy doborze stanowiska pracy jest również zakup odpowiedniego krzesła, które powinno być wygodne, dawać możliwość obrotu (krzesła obracane), posiadać podłokietniki oraz możliwość regulacji oparcia zgodnie z życzeniem użytkownika.

5 Dobrą praktyką, szczególnie w wypadku długotrwałej pracy przy komputerze, jest zapewnienie użytkownikowi podnóżków do pracy przy komputerze, które umożliwiają wyprostowanie nóg oraz zmianę pozycji, zapobiegając usztywnieniom. Przy aranżowaniu stacji komputerowej należy również zwrócić uwagę na otoczenie, takie jak meble, obrazy, tło, które nie powinny być w krzykliwych kolorach, ani nie powinny być źródłami światła jaśniejszymi niż ekran, dotyczy to również blatu, na którym ustawiony jest komputer. Sugerowane kolory otoczenia to jasne matowe oraz nieodblaskowe powierzchnie, które nie powodują znużenia oka. To właśnie niewłaściwe skomponowanie otoczenia tła oraz monitora komputerowego, jest jedną z najczęstszych przyczyn występowania CVS, gdyż oko ludzkie musi dostosować wzrok do kontrastujących źródeł światła (np.: jasny jaskrawy monitor w ciemnym pokoju). Pracujący na komputerze powinni również zwrócić uwagę na to, że osoba intensywnie wykorzystująca komputer bez odpowiednich przerw, mruga o wiele mniej niż przy zwykłej aktywności dziennej, co może powodować suchość oczu (ang. eye-dry), w tym wypadku zalecane jest robienie sobie przerw, jak również wykorzystywanie specjalnych kropli nawilżających powierzchnie oczu. Istotną kwestią jest ro-

DOBRE PRAKTYKI

[2] Tamże.

[3] Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, http://www.ciop.pl , data dostępu 17.02.2013.

[4] Tamże.

bienie przerw w czasie użytkowania komputera, zalecane są krótkie przerwy co ok.. 15 min pracy przeznaczone na oderwani eoczu, mruganie, wykonanie prostych prac niezwiązanych z komputerem (np.: rozmowa telefoniczna, przemieszczenie się), a także dłuższej co najmniej 5-minutowej przerwy po każdej godzinie pracy. **Nie powinno się pracować więcej niż 8 godzin dziennie przy komputerze**, przy czym, co istotne, w polskim prawodawstwie praca na komputerze jest zaliczana do grupy prac uciążliwych.

Użytkownicy komputera powinni regularnie odwiedzać okulistę w celu sprawdzenia stanu wzroku, badania wpływu pracy na komputerze na wzrok, a także aby otrzymać ewentualne sugestie dotyczące usprawnień swojej pracy w zakresie wzroku. Dobrą praktyką jest odwiedzanie lekarza-okulisty co najmniej raz w roku przy intensywnym wykorzystywaniu komputera zarówno w pracy, jak i do rozrywki.

6 Poniżej podsumowanie działań prewencyjnych, które pozwolą użytkownikom **zminimalizować ryzyko występowania CVS**:

- używanie odpowiednio dobranego monitora komputerowego (istotne jest zapewnienie odpowiedniego monitora komputerowego, przy czym najnowsze monitory, szczególnie LCD TFT, są najkorzystniejsze dla wzroku),
- ergonometria pracy na komputerze (odpowiednio dobrana stacja komputerowa – biurko, krzesło, ewentualnie podnóżek; zachowanie odpowiednich rekomendowanych odległości i przestrzeni),
- zapewnienie odpowiedniego oświetlenia (komputer ustawiony równolegle do okna, oświetlenie ogólne, brak oświetlenia punktowego, jasne matowe tło),
- regularne przerwy w pracy przy komputerze (krótka przerwa co 15 min, dłuższa 5-minutowa co godz.),
- ćwiczenia oczu (mruganie, zamykanie oczu, nawilżanie/przemywanie) oraz zachowywanie wilgotności pomieszczenia,
- regularne badania oczu (zalecana co najmniej jedna wizyta w roku u okulisty),
- używanie okularów zamiast szkieł kontaktowych.

7 Warto również zapoznać się rozporządzeniem Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 roku w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz.U. 1998 nr 148 poz. 973 z dnia 10 grudnia 1998 r.). Poniżej przedstawiony jest ekstrakt najistotniejszych punktów związanych z użytkowaniem monitora i ochroną wzroku z załącznika zatytułowanego „Minimalne wymagania bezpieczeństwa i higieny pracy oraz ergonomii, jakie powinny spełniać stanowiska pracy wyposażone w monitory ekranowe”:

„& 2. 1. Monitor ekranowy powinien spełniać następujące wymagania:

a) znaki na ekranie powinny być wyraźne i czytelne,
b) obraz na ekranie powinien być stabilny, bez tętnienia lub innych form niestabilności,
c) jaskrawość i kontrast znaku na ekranie powinny być łatwe do regulowania w zależności od warunków oświetlenia stanowiska pracy,
d) regulacje ustawienia monitora powinny umożliwiać pochylenie ekranu co najmniej 20° do tyłu i 5° do przodu oraz obrót wokół własnej osi co najmniej o 120° – po 60° w obu kierunkach,
e) ekran monitora powinien być pokryty warstwą antyodbiciową lub wyposażony w odpowiedni filt.,

&8. 2. Stanowisko pracy wyposażone w monitor ekranowy powinno być tak usytuowane w pomieszczeniu, aby za-

pewniało pracownikowi swobodny dostęp do tego stanowiska. Odległości między sąsiednimi monitorami powinny wynosić co najmniej 0,6 m, a między pracownikiem i tyłem sąsiedniego monitora – co najmniej 0,8 m.

§ 8. 3. Odległość oczu pracownika od ekranu monitora powinna wynosić 400 ¸ 750 mm.

§ 9. 1. Oświetlenie powinno zapewniać komfort pracy wzrokowej, a szczególnie:

a) poziom natężenia oświetlenia powinien spełniać wymagania określone w Polskich Normach,

b) należy ograniczyć olśnienie bezpośrednie od opraw, okien, przezroczystych lub półprzezroczystych ścian albo jasnych płaszczyzn pomieszczenia oraz olśnienie odbiciowe od ekranu monitora, w szczególności przez stosowanie odpowiednich opraw oświetleniowych, instalowanie żaluzji lub zasłon w oknach"[5].

[5] Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 1988 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe, Dz.U. 1998 nr 148, poz. 973.

ZESPÓŁ RSI
(ang. Repetitive Strain Injury)

OPIS ZJAWISKA

8 DEFINICJA

Zespół RSI jest zbiorczym terminem dla schorzeń występujących w związku z koniecznością powtarzania ruchów i czynności związanych z pracą lub aktywnością fizyczną, w tym aktywnością na komputerze.

9 PRZYCZYNY RSI

Najważniejsze przyczyny występowania RSI związanego z pracą na komputerze to:

- konieczność powtarzania czynności
- niestosowanie się do zasad ergonomiki pracy
- długotrwała aktywność/ praca na komputerze
- jednostkowe czynniki psychofizyczne

ĆWICZENIA 2

10 SKALA PROBLEMU

Ponieważ RSI jest terminem zbiorczym, do którego zaliczają się różne syndromy/schorzenia związane z powtarzaniem czynności, w tym przede wszystkim **Zespół Cieśni Nadgarstka** (w skrócie ZCN, ang. carpal tunnel syndromme) – jest to schorzenie wywołane poprzez nacisk na nerw pośrodkowy znajdujący się w kanale nadgarstka.

11 Innym przykładem schorzenia zaliczającego się do RSI jest tzw. kciuk Blackberry (ang. Blackberry Thumb) lub kciuk gracza (ang. Gamer's Thumb), czyli schorzenia kciuka związane z nadmiernym

używaniem klawiatury telefonów komórkowych lub sterowników gier komputerowych (np. używanych do gry w konsolach gier) przy szczególnym użyciu kciuka, który nie jest przyzwyczajony ani wystarczająco elastyczny do nadmiernego i szybkiego wykorzystywania przy działaniach manualnych. Występowanie tego schorzenia jest często związane z nieergonomicznym wykorzystywaniem urządzeń, np. smartfonów do wpisywania dużych ilości tekstu (np. przepisywanie długich umów, pisanie bez przerwy sms-ów). Dzieci są szczególnie narażone na schorzenia kciuka związane z nadmiernym wykorzystywaniem konsoli komputerowych.

ROZPOZNANIE OBJAWY

ROZPOZNANIE PROBLEMU/OBJAWY

Wśród symptomów RSI zaliczane są:

- trudności z chwytaniem przedmiotów oraz ból przy uchwycie,
- mrowienie kciuka,
- uszkodzenie nerwu pośrodkowego powodujące bóle dłoni,
- najczęściej bóle występują po obudzeniu się rano, po okresie odprężenia dłoni w czasie snu.

DIAGNOZA

DIAGNOZA – narzędzia, metody

Istnieją testy, które umożliwiają zidentyfikowanie występowania RSI, jednakże w wypadku wystąpienia symptomów konieczna jest wizyta u specjalisty. Testy wykrywające RSI to m.in.:

- test Phalena – polega na zgięciu kciuka na 30 do 60 sekund, jeśli po uwolnieniu uścisku wystąpi promieniujące mrowienie, istnieje możliwość występowania RSI
- test Tinela-Hoffmana polega na opukiwaniu nerwu pośrodkowego przed nadgarstkiem, które wywołuje uczucie przebiegu prądu wzdłuż nerwu
- test Durkana – polegający na ściskaniu kciuka przez lekarza przez ok. 30 sekund

DOBRE PRAKTYKI

12 **DOBRE PRAKTYKI – przeciwdziałania, rozwiązywanie**

Zespół RSI jest najczęstszą przyczyną absencji zawodowej w Wielkiej Brytanii, corocznie ponad milion obywateli rocznie bierze zwolnienie ze względu na RSI[6]. W związku z powszechnością tego schorzenia, a także z powodu poważnych konsekwencji związanych z nieleczeniem, konieczne jest wprowadzenie działań prewencyjnych dla regularnych użytkowników komputerów. Jedną z popularniejszych metod wykorzystywanych przeciw RSI jest instalowanie na komputerze specjalnego oprogramowania (ang. adaptive software), mającego na celu redukcję możliwości występowania syndromu. Możemy podzielić takie oprogramowanie na następujące grupy:

1. **przypominacze o przerwie** (ang. break -reminders) – jest to wszelkiego rodzaju oprogramowanie mające na celu przypominanie o konieczności zrobienia sobie przerwy od monitora w wyznaczonych przedziałach czasowych, najczęściej chodzi o dłuższą przerwę po godzinie pracy. Mogą to być najprostsze wygaszacze, jak również i skomplikowane oprogramowanie połączone z pomiarem innych cech zdrowotnych, zgodnie z nowymi trendami technologicznymi, gdzie komputery służą pomiarowi różnych cech zdrowotnych (np.: liczba przebytych kilometrów, pochłoniętych kalorii, jak również i czas używania komputera), w celu pomiaru zarządzania własnym zdrowiem;
2. **rozwiązania zmniejszające aktywność** – chodzi tutaj między innymi o wykorzystywanie rozpoznawania mowy przy wpisywaniu długich tekstów, wykorzystywanie skanerów OTC, czy też skrótów oraz słowników typu T9 przy wpisywaniu tekstów na telefonach komórkowych. Wszelkie te urządzenia mają na celu zmniejszenie ilości powtarzanych ruchów.

[6] The Health and Safety Executive, http://www.hse.gov.uk/statistics/tables/thorgp02.htm, data dostępu 17.02.2013.

13 Oprócz oprogramowania istotnym elementem wpływającym na ograniczenie występowania RSI jest **zachowanie zasad ergonomiki pracy na komputerze i stworzenie użytkownikowi wygodnego i korzystnego dla zdrowia miejsca pracy oraz użytkowania**. Tak jak w wypadku syndromu związanego ze wzrokiem, w wypadku RSI istotne jest robienie sobie przerw od pracy/użytkowania w ustalonych okresach (np. co godzinę), podczas których ręka oraz kciuk dostaną możliwość odprężenia się, a także odpoczynku. Można również wykorzystywać pewne elementy masażu (w USA dostępne są specjalne masażery ręczne dla osób cierpiących lub zagrożonych RSI), jak również pomoce odstresowujące (np.: miękkie kuleczki do ściskania, które pozwalają mięśniom i nerwom odpocząć po ciągłym użyciu; specjalne urządzenia do ściskania wykorzystywane do wzmocnienia dłoni). Istotne jest również niewykorzystywanie urządzeń mobilnych do regularnej pracy związanej z wprowadzaniem tekstu, ze względu na rozmiar klawiatury, ułożenie klawiszy oraz ergonomikę urządzenia te są przystosowane jedynie do pracy okazjonalnej (np. w czasie podróży, przejazdu do pracy), nie mogą jednak zastępować urządzeń stacjonarnych. W wypadku użytkowania konsoli do gry, korzystne wydaje się rozważenie zakupu takiej, która poruszana jest ruchem użytkownika, w przeciwieństwie do sterowanych joystickami oraz innymi przyrządami, w których występuje konieczność częstych powtórzeń ruchu. Świadomość występowania RSI oraz prewencji jest bardzo istotna, gdyż schorzenie to nie jest mocno zakorzenione w świadomości użytkowników komputerów, a jego wystąpienie może mieć dewastujący wpływ na życie dorosłego czy dziecka. Schorzenia typu RSI nie są łatwe w wyleczeniu, w wypadku zaawansowanych stadiów wymagają wieloletnich kuracji, często z koniecznością operowania. Zachorowanie na RSI wiąże się również z wieloma kosztami społecznymi, takimi jak absencja w pracy czy szkole, utrata biegłości w wykonywaniu zadań pracowniczym, stygmatyzacja

W obecnych czasach zobrazowanie RSI bardzo negatywnie wpływa na aktywność zawodową/edukacyjną. Ze względu na to schorzenie nie można wykorzystywać komputera tak intensywnie, jak przed chorobą, a w obecnym świecie zawodowym wykluczenie z użytkowania komputera prowadzi do wykluczenia cyfrowego, co może spowodować utratę pozycji zawodowej i społecznej. Istnieje wiele świadectw osób z RSI, pokazujących jak wpłynęło ono na ich życie, warto zapoznać się ze znanym brytyjskim blogiem: http://www.ergomatters.co.uk/blog, w którym autor przedstawia swoją 14-letnią walkę z RSI oraz pokazuje wpływ schorzenia na aktywność psychiczną, fizyczną oraz społeczną.

OPIS ZJAWISKA

DOLEGLIWOŚCI UKŁADU KOSTNO-SZKIELETOWEGO (ang. Musculosceletal Disorder, MSD)

14 **DEFINICJA**

Zgodnie z definicją Europejskiej Agencji Bezpieczeństwa i Zdrowia w Pracy z siedzibą w Bilbao, za dolegliwości układu kostno-szkieletowego możemy uznać:

„Choroby układu mięśniowo-szkieletowego związane z pracą to upośledzenie struktur anatomicznych, takich jak: mięśnie, stawy, ścięgna, wiązadła, nerwy, kości i miejscowy układ krążenia krwi, wywoływane lub nasilone przede wszystkim na skutek wykonywania pracy oraz bezpośrednio przez oddziaływanie czynników otoczenia, w którym praca jest wykonywana (…). Choroby układu mięśniowo-szkieletowego mogą być charakteryzowane jako schorzenia o charakterze epizodycznym, ponieważ ból często znika i powraca po kilku miesiącach lub latach. Niektóre MSD jednak mogą mieć charakter chroniczny lub nieuleczalny”[7]

ROZPOZNANIE OBJAWY

15 **ROZPOZNANIE PROBLEMU OBJAWY**

MSD jest szeroką grupą schorzeń, do której należą również schorzenia związane z RSI, tak jak między innymi zespół cieśni nadgarstka. Najczęściej występujące poza RSI schorzenia MSD wśród osób pracujących/użytkujących komputer to bóle pleców oraz okolic szyi. W wypadku innych chorób MSD poza RSI, wskazania prewencyjne są podobne, bardzo istotna jest ergonomika pracy, w tym przestrzeganie zasad BHP związanych z położeniem komputera, kątem nachylenia głowy, oświetleniem oraz wygodnym siedziskiem. Brak dostosowanego siedziska jest częstym przypadkiem, dlatego Ministerstwo Pracy oraz Polityki Socjalnej wskazało następujące wytyczne dotyczące krzesła użytkowanego przy komputerze:

„5.1. Krzesło stanowiące wyposażenie stanowiska pracy powinno posiadać:

a) dostateczną stabilność, przez wyposażenie go w podstawę co najmniej pięciopodporową z kółkami jezdnymi,
b) wymiary oparcia i siedziska, zapewniające wygodną pozycję ciała i swobodę ruchów,
c) regulację wysokości siedziska w zakresie 400-500 mm, licząc od podłogi,
d) regulację wysokości oparcia oraz regulację pochylenia oparcia w zakresie: 5° do przodu i 30° do tyłu,
e) wyprofilowanie płyty siedziska i oparcia odpowiednie do naturalnego wygięcia kręgosłupa i odcinka udowego kończyn dolnych,
f) możliwość obrotu wokół osi pionowej o 360°,
g) podłokietniki”[8].

16 Ze względu na skomplikowanie oraz różnorodność MSD nie sposób przedstawić wszystkich możliwych schorzeń w tym zestawieniu, jednocześnie należy zauważyć, że opisany szczegółowo przypadek RSI jest najczęściej występującym schorzeniem w związku z pracą na komputerze. Unia Europejska uznając istotność problemu MSD wskazała, że choroby MSD są priorytetem we wspólnotowej strategii bezpieczeństwa oraz higieny pracy w UE[9].

ĆWICZENIA 3

[7] *Choroby układu mięśniowo-szkieletowego (MSD) w sektorze Horeca*, Europejska Agencja Bezpieczeństwa i Zdrowia w Pracy, https://osha.europa.eu/pl/publications/e-facts/efact24 data dostępu 17.02.2013.

[8] Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 1988 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe, Dz.U. 1998 nr 148, poz. 973.

[9] Choroby układu mięśniowo-szkieletowego, Europejska Agencja Bezpieczeństwa i Zdrowia w Pracy, https://osha.europa.eu/pl/topics/msds/index_html, data dostępu 19.02.2013.

ZESPÓŁ UZALEŻNIENIA OD INTERNETU (ang. Internet Addiction Disorder, IAD)

17 DEFINICJA

Aktualnie uzależnienie od Internetu (inaczej siecioholizm lub infoholizm) nie jest klasyfikowane jako choroba według klasyfikacji zaburzeń psychicznych DSM IV prowadzonej przez Amerykańskie Towarzystwo Psychiatryczne, dlatego syndrom ten zostanie szczegółowo opisany w rozdziale dotyczącym zagrożeń związanych z uzależnieniami od sieci. Lekarze specjaliści debatują, czy uzależnienie od Internetu może zostać uznane za jednostkę chorobową, czy też nie. Ponieważ jest to stosunkowo nowe zjawisko, lekarze potrzebują więcej czasu na podjęcie decyzji, czy można będzie zaliczyć IAD do chorób. W maju 2013 roku Amerykańskie Towarzystwo Psychiatryczne umieściło IAD w swojej corocznej encyklopedii zdrowia psychicznego „Diagnostic and Statistical Manual of Mental Disorders" z rekomendacją do dalszego badania problemu, co może oznaczać, że w nieodległej przyszłości zostanie ono uznane za zaburzenie psychiczne, tak jak stało się np. z uzależnieniem od hazardu.

18 ROZPOZNANIE PROBLEMU OBJAWY

Symptomy:

- alienacja,
- zaburzenia rytmu dobowego (np.: późne chodzenie spać, spóźnianie się do pracy/szkoły),
- podrażnienie oraz agresja,
- radykalizacja poglądów,
- plany samobójcze,
- konflikty z prawem związane z działalnością w Internecie,
- zaniedbywanie obowiązków zawodowych i rodzinnych,
- odczuwanie podniecenia na myśl o pracy przy komputerze,
- przeglądanie nielegalnych treści w Internecie,
- radykalna zmiana zachowań.

19 DIAGNOZA – narzędzia, metody

Wśród typów IAD można zdiagnozować m.in:

1. **uzależnienie od gier komputerowych** – uzależnienie od gier komputerowych dotyka w szczególności dzieci i młodzież, a polega na kompulsywnym, intensywnym wykorzystywaniu komputera do gier wirtualnych; występuje tu wiele zagrożeń, począwszy od wyłączenia się z życia osobistego, zatarcia granic pomiędzy światem wirtualnym i realnym, niepohamowane napady agresji, aż do wycieńczenia organizmu w przypadku grania kompulsywnego (znany jest przykład tajlandzkiego gracza, który umarł w kafejce internetowej po 40 godzinach gry na komputerze). W Stanach Zjednoczonych na wzór stowarzyszeń Anonimowych Alkoholików istnieją organizacje Anonimowych Graczy (ang. Gamers Anonimous), które zajmują się wychodzeniem z uzależnienia przez graczy komputerowych;
2. **erotomania komputerowa** – w tym wypadku użytkownik przeznacza swój wolny czas na przebywanie na stronach zawierających treści erotyczne/pornograficzne; uzależnienie to może prowadzić do zaburzeń własnego życia osobistego/erotycznego lub w postaci bardziej skrajnej do konfliktów z prawem, np. w wypadku poszukiwania stron pornograficznych z materiałami pedofilskimi; szczególnym przypadkiem erotomanii internetowej jest również poszukiwanie wirtualnych kontaktów seksualnych przez Internet, dotyczy to szczególnie przypadków, gdy może wpływać to na życie rodzinne/osobiste użytkownika;

3. **uzależnienie od informacji** (przeciążenie informacyjne) – jest to kompulsywne wykorzystywanie komputera do zdobywania informacji, zaburzające rytm życia użytkownika. O tym przypadku możemy mówić, gdy dana osoba spędza nieproporcjonalnie dużo czasu na forach internetowych, czatach lub odświeżając i czytając najnowsze wiadomości na portalach informacyjnych; ten rodzaj zagrożenia może wpływać na efektywność życia zawodowego osoby, która nie może skupić się na swoich zadaniach pracowniczych, nieustannie odświeżając nowe, najczęściej bezużyteczne, informacje;
4. **uzależnienie od kontaktów społecznych w sieci** – portale oraz komunikatory społeczne dały ludziom niespotykaną dotychczas w dziejach świata łatwość nawiązywania kontaktów z innymi osobami, często z innych części świata; w przypadku uzależnienia od portalów społecznościowych możemy mówić o szerokiej gamie zagrożeń: począwszy od braku możliwości weryfikacji oraz nieumiejętności oceniania, czy nasz rozmówca ma dobre intencje, co jest szczególnie istotne w przypadku dzieci narażonych na pedofilię w sieci czy też ofiar portali randkowych; często uzależnienie od portali społecznych polega na intensywnym spędzaniu czasu na portalach typu: Facebook czy MySpace, gdzie osoba uzależniona prowadzi bogate życie społeczne, jednocześnie alienując się od życia realnego i posiadając trudności w nawiązywaniu relacji społecznych w rzeczywistości; kontakty przez portale społecznościowe łączą się również z zagrożeniami związanymi z ujawnieniem prywatnych, często intymnych informacji osobom niepowołanym, w tym popularny sexting, czyli wysyłanie intymnych zdjęć za pomocą urządzeń mobilnych lub komputera, które mogą być często wykorzystane przeciw osobie wysyłającej,
5. **cyberchondria** – jest to internetowa odmiana hipochondrii, polegająca na kompulsywnym wykorzystywaniu Internetu, w tym szczególności społeczności zdrowotnych oraz forów internetowych w poszukiwaniu informacji dotyczących chorób; ze względu na brak weryfikacji wiedzy naukowej osób publikujących informacje o chorobach w Internecie, może prowadzić do przyswojenia błędnych informacji, a także do zachowań paranoidalnych oraz wmawiania sobie istnienia chorób; w skrajnych przypadkach cyberchondria może prowadzić również do samobójstw;
6. **samobójstwa w sieci/samookaleczanie** – w rzadkich przypadkach Internet może być platformą wymiany informacji przez osoby mające plany samobójcze lub dokonujące samodestrukcji przez okaleczanie; obecność na takich forach może dawać negatywne wsparcie powodujące, że ktoś może szybciej podjąć decyzję o próbie samobójczej; znane są również jednostkowe przypadki, w których przy użyciu Internetu samobójstwa popełniały grupy osób (tzw. akty samobójcze).

20 W celu zdiagnozowania występowania zespołu uzależnienia od Internetu można wykorzystywać testy kwestionariuszowe, w tym najpopularniejszy test uzależnienia od Internetu (ang. Internet Addiction Test) opracowany przez wybitną ekspertkę w zakresie badania IOD dr Kimberley Young. Ten krótki 20-pytaniowy test składający się z pytań zamkniętych pozwoli ocenić poziom uzależnienia od Internetu.

21 **DOBRE PRAKTYKI – przeciwdziałania, rozwiązywanie**

Ponieważ IOD jak na razie nie jest uznany za jednostkę chorobową, nie istnieją wytyczne co do leczenia tej dolegliwości. Jako potencjalne rozwiązania można wskazać m.in.:

- alternatywne metody spędzania czasu (np. zwiększenie ilości wysiłku fizycznego, spotkania ze znajomymi, dodatkowe zajęcia itp.),
- oprogramowanie ograniczające czas użytkowania komputera,
- wsparcie psychologa,
- terapia behawioralna.

BIBLIOGRAFIA:

Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, http://www.ciop.pl, data dostępu 17.02.2013.

Choroby układu mięśniowo-szkieletowego (MSD) w sektorze Horeca, Europejska Agencja Bezpieczeństwa i Zdrowia w Pracy, https://osha.europa.eu/pl/publications/e-facts/efact24, data dostępu 17.02.2013.

Choroby układu mięśniowo-szkieletowego, Europejska Agencja Bezpieczeństwa i Zdrowia w Pracy, https://osha.europa.eu/pl/topics/msds/index_html, data dostępu 19.02.2013.

Kotowski J., *Praca przy Komputerze: Zagrożenia, Zasady bezpiecznej pracy*.

Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 1988 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe, Dz.U. 1998 nr 148, poz. 973.

The Health and Safety Executive, http://www.hse.gov.uk/statistics/tables/thorgp02.htm, data dostępu 17.02.2013.

DOBRE PRAKTYKI

ZAGROŻENIA ZDROWIA PSYCHICZNEGO I FIZYCZNEGO

CYFROWA DEMENCJA

ORAZ INNE FORMY E-ZAGROŻEŃ JAKO NOWE NASTĘPSTWA NIEPRAWIDŁOWEGO UŻYTKOWANIA NOWYCH MEDIÓW

Łukasz Tomczyk

OPIS ZJAWISKA

ĆWICZENIA 5

1 WPROWADZENIE

Niniejszy tekst jest próbą zmierzenia się z zagadnieniem rzadko do tej pory poruszanym kompleksowo w literaturze pedagogiki medialnej, a odnoszącym się do tematyki następstw trwałych zmian poszczególnych składowych osobowości i mózgu w kontekście nieprawidłowego użytkowania urządzeń cyfrowych. Przygotowanie tekstu możliwe było dzięki książce niemieckiego psychiatry i neurobiologa, profesora Manfreda Spitzera wzbudzającej wśród czytelników zarówno szereg kontrowersji, jak i wielkie uznanie dla trafnej diagnozy psychospołecznego funkcjonowania grupy najmłodszych użytkowników urządzeń cyfrowych.

2 CHARAKTERYSTYKA ZJAWISKA

Warto przedstawić pokrótce sylwetkę autora książki *Cyfrowa demencja*, który dzięki zdobytemu doświadczeniu klinicznemu pokazał szereg odważnych, a zarazem fatalistycznych skutków niekontrolowanego i bezmyślnego implementowania sieciowych urządzeń cyfrowych w codzienne życie dzieci i młodzieży. Manfred Spitzer od początku lat 90. związany jest zawodowo z kierowaniem uniwersyteckimi klinikami psychiatrii w Heidelbergu oraz Ulm. Obecnie zarządza Centrum Wymiany Wiedzy z Dziedziny Neuronauk i Edukacji. Całość rozważań niemieckiego lekarza zawarta w publikacji *Cyfrowa demencja* wywołała na przestrzeni ostatnich kilkunastu lat olbrzymią dyskusję, w którą włączyli się w Polsce zarówno cyfrowi technokraci wspierani przez cyfrowych autochtonów, jak i pedagodzy medialni. Obie grupy zajmują skrajne stanowiska w stosunku do oddziaływania mediów na organikę mózgu i psychospołeczne funkcjonowanie dzieci. Dodatkowo osoby odpowiedzialne, a więc nauczyciele oraz rodzice są najczęściej zdezorientowani i nie posiadają jakiejkolwiek wiedzy w obszarze bezpiecznej obsługi mediów elektronicznych jak i oddziaływania tychże rozwiązań na utrwalanie negatywnych zachowań. Nowe media generują szereg niewystępujących jeszcze kilkanaście lat temu problemów, takich jak: uzależnienie od mediów i generowanie niekorzystnych nawyków obsługi urządzeń cyfrowych[2], pobieranie nielegalnego oprogramowania oraz brak prawidłowego rozumienia prawa autorskiego[3], cyberprzemoc[4], niekontrolowany kontakt dzieci z nieznajomymi w sieci[5], pornografia i pedofilia[6], niskie kompetencje osób znaczących w zakresie kontroli dzieci w przestrzeni nowych mediów[7]. **M. Spitzer analizując e-zagrożenia sięga głębiej, dosadnie argumentując przy użyciu badań naukowych w obszarze neuronauk, iż media elektroniczne przede wszystkim zmieniają nasz mózg**. Ponadto przeobrażenia te w perspektywie dorastającego pokolenia mogą okazać się w dalszej perspektywie niezwykle niekorzystne dla całego społeczeństwa.

3 Tytułem wstępu warto zaznaczyć, że od czasu upowszechnienia się komputerów w Polsce minęły już ponad dwie de-

[1] Większość artykułu została oparta na książce M. Spitzera oraz wybranych dyskusjach toczących się w portalach branżowych w momencie opublikowania pracy.

[2] J. Holtkamp, *Co ogłupia nasze dzieci?*, Wydawnictwo Salwator, Kraków 2010.

[3] Por. E. Bendyk, *Bunt sieci*, Biblioteka Polityki, Warszawa 2012.

[4] Por. R. Kowalski, S. Limber, P. Agatston, *Cyberprzemoc wśród dzieci i młodzieży*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2011, J. Pyżalski, *Agresja elektroniczna wśród dzieci i młodzieży*, Gdańskie Wydawnictwo Psychologiczne, Sopot 2011.

[5] Por. A. Słysz, B. Arcimowicz, *Przyjaciele w Internecie*, Gdańskie Wydawnictwo Psychologiczne, Sopot 2009.

[6] B. Danowski, A. Krupińska, *Dziecko w sieci*, Wydawnictwo Helion, Gliwice 2007.

[7] F. Huber, C. Neuschäffer, *Rodzice offline? Jak nawiązać kontakt ze skomputeryzowanym dzieckiem*, Wydawnictwo Lekarskie PZWL, Warszawa 2003.

kady. Internet na stale zagościł w większości domostw. Polska według najnowszych badań np. Diagnozy Społecznej (2013), coraz mniej odstaje w zakresie posiadania sprzętów elektronicznych od innych krajów europejskich. Dodatkowo powszechnie wprowadzane rozwiązania informatyczne wspomagające codzienne funkcjonowanie ludzi w instytucjach oraz życiu prywatnym są stanem normalnym następującym za sprawą logicznego toku rozwoju społeczno-technicznego. Bez rozwiązań informatycznych trudno wyobrazić sobie w dzisiejszych czasach funkcjonowanie banków, szkół, urzędów państwowych. Urządzenia cyfrowe stały się również nieodłącznym elementem życia cyfrowych autochtonów. Komputery, konsole, telewizja cyfrowa, tablety, smartfony, odtwarzacze mp3, nawigacje to oprzyrządowanie, które bez wątpienia usprawnia i uprzyjemnia nasze życie, jednakże z drugiej strony jest przyczyną wielu niekorzystnych zjawisk, które pokrótce zostaną scharakteryzowane w dalszej części tekstu.

4 MEDIA ELEKTRONICZNE W OBSZARZE UCZENIA

Systematycznie od końca lat 90-tych XX wieku do czasów obecnych zauważalny jest wzrost wykorzystania mediów elektronicznych przez dzieci i młodzież. Przeciętne europejskie dziecko w wieku szkolnym spędza o wiele więcej wolnego czasu, będąc w kontakcie z nowymi mediami niż przeznacza na realne relacje w domu rodzinnym czy też w środowisku rówieśniczym. Czas ten jednak jest głównie związany z funkcjami komunikacyjnymi oraz rozrywkowymi, jakie oferują tego typu urządzenia. Paradoksalnie patrząc z perspektywy rodziców można zauważyć, że większość osób, wyposażając swoje pociechy w urządzenia elektroniczne zakłada, że media elektroniczne mają za zadanie przede wszystkim wspomaganie ich rozwoju, procesu uczenia się, spostrzegawczości. Jednakże, jak podkreśla M. Spitzer oraz liczne badania naukowe, na które się powołuje, czas wypełniany przez urządzenia sieciowe jawi się jako stracona szansa na pełny i realny rozwój młodych użytkowników technologii cyfrowej.

5 Zasadnicze pytanie stawiane na I roku studiów pedagogicznych brzmi – na czym polega właściwy proces uczenia się? Otóż kandydat na stanowisko nauczyciela po dwóch semestrach jest już w stanie udzielić poprawnej i rzetelnej odpowiedzi. Zatem **uczenie się związane jest z procesami neurobiologicznymi, występującymi tylko w sytuacji, gdy realny wysiłek intelektualny powoduje trwałe zmiany w mózgu**. Najbardziej skomplikowany i niezbadany do końca organ naszego ciała, jakim jest mózg funkcjonuje prawidłowo w wymiarze neuronalnym wyłącznie wtedy, gdy zachodzą w nim zmiany pod wpływem włączania nowych neuronów w system pozostałych podstawowych struktur. Z aktywizacją neuronów jest podobnie jak z treningiem mięśni. W sytuacji gdy człowiek zostaje poddawany stymulacji w postaci wysiłku intelektualnego, nowo powstające neurony w hipokampie włączane są w pozostałą siatkę połączeń, natomiast pojawiające się informacje w postaci impulsów elektrycznych przekazywane za pomocą synaps uaktywniają wybrane części mózgu. **Zachowanie odpowiedniej sprawności umysłowej jest możliwe zatem tylko i wyłącznie w sytuacji stawiania nowych, nieodtwórczych zadań dla mózgu**. Pytanie, na ile powierzchowna komunikacja i przeglądanie stron internetowych oraz korzystanie z aplikacji rozrywkowych stymuluje mózg do realnego działania, staje się zasadniczą kwestią służącą wyjaśnieniu fenomenu tytułowej cyfrowej demencji.

6 Od kilkudziesięciu lat wiadomo, że proces uczenia się jest możliwy również w okresie starości, gdyż wtedy także pomimo utraty sporej liczby neuronów produkowane są nowe „szare komórki" w hipokampie. Neurony odpo-

ĆWICZENIA 6

OPIS ZJAWISKA

wiednio zaaktywizowane przez proces uczenia się, a więc wysiłek intelektualny, wzbogacają potencjał sprawnego działania i wiedzy. W tym kontekście dostrzegalny jest coraz widoczniej dylemat, na ile wspomaganie nowymi mediami, m.in. przez platformy do kształcenia na odległość, prezentacje multimedialne stymuluje do prawdziwego uczenia się, a na ile jest tylko jego marnym substytutem. Głębokość przetwarzania informacji ma tutaj olbrzymie znaczenie. Wertowanie dużej liczby stron, szybkie czytanie, przesuwanie ikonek na pulpicie oraz nagminne wklejanie przez uczniów i studentów treści na zasadzie „ctrl + c" oraz „ctrl + v" nie tylko skutkuje brakiem osiągnięcia założonych celów kształcenia, lecz przede wszystkim nie powoduje trwałych zmian w systemie neuronalnym, uniemożliwiając zdobycie prawdziwej wiedzy.

7 NAJNOWSZE DONIESIENIA

Patrząc z innej perspektywy na poruszone zagadnienie, od początku lat 90-tych XX wieku można zauważyć ogólną fascynację nowymi rozwiązaniami informatycznymi, które wielokrotnie na siłę implementowane są w system edukacji. Owa niezbadana merytorycznie pod względem efektywności działań dydaktycznych fascynacja trwa do dzisiaj. Trudno obecnie spotkać w Polsce szkołę nieposiadającą w swoim wyposażeniu tablicy interaktywnej czy też projektorów multimedialnych. W ramach zakładanego unowocześniania edukacji coraz częściej wprowadzane są obowiązkowe e-podręczniki, natomiast ćwiczenia rozwiązywane są nie w tradycyjnych zeszytach, lecz na tabletach, czy też netbookach. Spitzer analizując fenomen wszechobecnej informatyzacji podkreśla, że komputery i sieć dostarczają nam informacji podobnie jak nauczyciele. Na tej podstawie wielokrotnie bywa wyciągany błędny wniosek, iż urządzenia cyfrowe stanowią doskonałe, a na dodatek multimedialne (polisensoryczne) źródło informacji jednocześnie nieograniczonej pod względem zasobów i terytorium. **Jednakże pomimo masowej implementacji rozwiązań cyfrowych brak jest do tej pory rzetelnych wyników badań sugerujących, że nowoczesne technologie** ICT takie jak tablety, tablice interaktywne (na marginesie: z których nie wszyscy nauczyciele potrafią korzystać) **warunkują skuteczniejszą efektywność uczenia się i nauczania niż tradycyjne metody**. Po fali zachwytu szybkością dostępu do informacji pojawia się od kilkunastu miesięcy coraz ostrzejsza dyskusja nad problemem związanym ze zjawiskiem powierzchowności uczenia się za pomocą urządzeń elektronicznych. W ramach prowadzonych analiz można spotkać się również z opiniami, że urządzenia zamiast wspierać rozwój dzieci obniżają zakres ich elementarnych umiejętności i wiedzy.

8 Niemiecki neurobiolog stawia przewrotne, ale zasadne pytanie „co jest lepsze – odkładanie pamięci w mózgu czy w chmurze", udzielając jednocześnie odpowiedzi w tekście swojej publikacji. **Odciążanie ludzkiej pamięci prowadzi nie tylko do mniej intensywnego działania mózgu, lecz jednocześnie obniża skuteczność zapamiętywania**. Przechowywanie informacji na twardych dyskach, pendrivach, serwerach, w poczcie elektronicznej daje specyficzne poczucie dostępu do każdej informacji w dowolnym miejscu i czasie. Odzwyczajenie się od zapamiętywania informacji jest o tyle niebezpieczne (abstrahując od wyłączenia zasilania czy awarii sieci), iż skutkuje nie tylko zmianami fizykalnymi mózgu, lecz generuje szereg niekorzystnych zjawisk, takich jak: zanikanie samodzielnej potrzeby dochodzenia do prawdy, brak fachowej wiedzy łączonej z jej powierzchownością.

9 Najbardziej wartościowym etapem rozwojowym człowieka jest okres dzieciństwa. Wtedy to zdobywamy szereg umiejętności, kompetencji, postaw pozwalających na efektywne

funkcjonowanie w dorosłości. W okresie tym wszystkie organy ludzkie wykazują olbrzymią tendencję rozwojową, w tym szczególnie mózg. Kształtowanie odpowiednich nawyków związanych z ruchem, samokontrolą, samooceną warunkuje nabycie prawidłowych mechanizmów umożliwiających sukces życiowy. Należy wobec tego faktu podkreślić znaczenie telewizji, która jest specyficznym przedstawicielem mediów elektronicznych. Brak wyznaczania granic w zakresie oglądania bajek telewizyjnych staje się pierwszym krokiem sprzyjającym kolejnym negatywnym nawykom związanym z niekontrolowanym i bezmyślnym użytkowaniem mediów sieciowych w okresie adolescencji.

10 NAJMŁODSI W ŚWIECIE MEDIÓW

Dziecko uczy się poprzez swój specyficzny okres rozwojowy o wiele szybciej niż dorosły. Fakt ten powinien być szczególnie ważny dla pedagogów medialnych, którzy bazując jedynie na idei nieograniczonego dostępu do olbrzymiej ilości informacji w sieci zapominają, iż ważna jest również dokładność w zakresie segregacji i wartościowania informacji. Wspieranie edukacji na etapie szkolnym oraz przedszkolnym jest o tyle istotne, że nie ilość zdobytych przez ucznia informacji jest istotna, co kształcenie elementarnych kompetencji związanych z pisaniem, liczeniem, pamięcią krótkotrwałą i długotrwałą; kompetencje społeczne oraz holistyczne pojmowanie świata możliwe dzięki koncepcji nauczania zintegrowanego. Część tych zdolności realizowana jest za sprawą aktywności rozwijających zdolności motoryczne poprzez zabawy, gry, interakcje rówieśnicze. Wobec tychże faktów bezzasadne wydaje się wdrażanie na etapie wczesnej edukacji laptopów, tabletów, gdyż są to urządzenia, które nieodpowiednio wdrożone nawet jako wspomagające środki dydaktyczne mogą bardziej zakłócić proces edukacyjny niż przyczynić się do jego poprawy. Odnosząc się do zastąpienia tradycyjnych zeszytów ćwiczeń oraz podręczników ich cyfrowymi substytutami, część pedagogów i rodziców zastanawia się, w jakim celu prowadzone są tego typu działania. Czy jest to konieczne tylko i wyłącznie dlatego, że skoro są zabezpieczone fundusze (np. z projektów unijnych) i mamy łatwy dostęp do zakupu urządzeń cyfrowych oraz e-podręczników, należy koniecznie wykazując się postępem zmienić tradycyjną i do tej pory skuteczną metodykę kształcenia? Warto zastanowić się nad tym i podobnymi dylematami nieco szerzej w kontekście rzetelnych badań oraz przewidywań, a także dotychczasowej wiedzy związanej z biopsychospołecznym rozwojem człowieka.

11 M. Spitzer zaznacza, że główną odpowiedzialność za ogłupianie dzieci i niedbanie o ich prawidłowy rozwój ponoszą rodzice. Wynika to przede wszystkim z faktu pozornego dbania o dobre samopoczucie oraz rozwój dzieci poprzez wyposażenie gospodarstw domowych w konsole do gry oraz komputery mające jako główny cel wyrównanie bądź też podnoszenie szans edukacyjnych. Rodzice przed zakupem urządzeń cyfrowych rzadko kiedy dokonują namysłu nad realnym wpływem tego typu techniki na proces uczenia się, relacje społeczne, kształtowanie systemu wartości oraz zachowań związanych z prozdrowotnym spędzaniem czasu wolnego. **Z prowadzonych eksperymentów jasno wynika, że dzieci intensywnie grające w różnego rodzaju aplikacje rozrywkowe osiągają gorsze wyniki w nauce, niż rówieśnicy nieposiadający konsoli lub korzystający z aplikacji rozrywkowych w ograniczonym zakresie**. Ponadto inną kwestią jest rodzaj gier, z których korzystają dzieci. Wielu opiekunów nie potrafi podjąć chociażby małej próby zastanowienia się nad następstwami nadmiernego i niekontrolowanego użytkowania mediów sieciowych. Trudne do osiągnięcia na tym etapie roz-

ROZPOZNANIE OBJAWY

woju społeczeństwa zinformatyzowanego są również inne cele pedagogiki medialnej związane z doborem gier adekwatnych do wieku. Oczywiście istnieją systemy oznaczania gier komputerowych np. PEGI, jednakże spore grono rodziców i opiekunów wyznaje zasady, że skoro dziecko przebywa w bezpiecznej przestrzeni domowej, nic nie jest w stanie mu zagrozić, a zabawa z grą sprawia przecież wiele radości i nie angażuje dorosłego w interakcję z dzieckiem. W obliczu dynamicznego rozwoju branży gier komputerowych oraz ich niesłabnącej „konsumpcji" przez najmłodszych użytkowników zasadne staje się wyznaczenie nowych trendów w edukacji medialnej związanych z kształceniem w osobach dorosłych wiedzy i umiejętności pozwalających na bezpieczne wychowanie w społeczeństwie mimowolnie zinformatyzowanym. Osoby dorosłe, a więc z założenia bardziej świadome i odpowiedzialne za swoje dzieci, powinny szczególnie uwrażliwić się na czas korzystania z mediów elektronicznych, treści występujące w grach, które zostawiają ślady pamięciowe, kształtując tym samym nawyki i rodzącą się osobowość dziecka.

M. Prensky[8], którego typologią podziału społeczeństwa na cyfrowych autochtonów i imigrantów posiłkują się pedagodzy medialni opisujący zależności międzypokoleniowe, zauważa, iż osoby, które wyrosły w czasach analogowych posiadają zupełnie inny odbiór rzeczywistości niż współczesna młodzież. Fakt ten nie wynika z tradycyjnych różnic pomiędzy pokoleniami, lecz jego dynamikę wyznacza wszechobecna informatyka oraz co za tym idzie zmiana stylu życia młodszego pokolenia. Aby zrozumieć fenomen cyfrowych autochtonów, należy podkreślić, że **przeciętny młody człowiek przed ukończeniem dwudziestego pierwszego roku życia**[9]:

- wysłał lub otrzymał dwieście pięćdziesiąt tysięcy e-maili i esemesów,
- poświęcił na obsługę telefonu komórkowego dziesięć tysięcy godzin,
- grał przez pięć tysięcy godzin w gry komputerowe,
- spędził ponad trzy tysiące godzin na portalach społecznościowych (współczynnik ten będzie się dynamicznie podnosił w ciągu kolejnych lat, o czym świadczą tendencje związane z popularnością wybranych stron internetowych np. Facebooka).

12 ROZPOZNANIE OBJAWY

Typowy cyfrowy tubylec jest online przez większość dnia, utrzymuje stały kontakt mailowy oraz komunikację w portalach społecznościowych i komunikatorach czy też w sposób esemesowy. Cyfrowy autochton działa wielozadaniowo, słuchając muzyki serfuje w sieci przez wiele godzin, ma swoje ulubione gry komputerowe, którym poświęca również dużą ilość wolnego od obowiązków szkolnych czasu. Grając na konsoli (zazwyczaj w gry sieciowe, często wykraczając poza dozwolony zakres wiekowy) lub oglądając wieczorny program telewizyjny, ma zapewniony stały kontakt z wirtualnym światem poprzez smartfon podpięty pod domowy hotspot, czy też komputer osobisty. Zamiast budzika programuje komórkę, pozostaje przez cały dzień osiągalny, przed snem odczytuje najnowsze wiadomości w telefonie i Internecie. Zasypia po 23.00, słuchając ulubionej muzyki online lub pobranej z sieci plików mp3.

Spitzer analizując opisany tryb życia nie demonizuje, lecz stawia otwarte pytania: jakie mogą być długofalowe następstwa takiego codziennego trybu życia? Czy szybkie zmiany techniczne nazywane cyfrową rewolucją, za którą większość cyfrowych imigrantów nie nadąża, są dobrodziejstwem czy też przekleństwem? Jednocześnie lekarz udziela odpowiedzi, że na podstawie

8 M. Prensky, *Digital Natives, Digital Imigrants,* On the Horizon 2001, MCB University Press, Vol. 9. No 5, www.marcprensky.com, data dostępu 12.2013

9 M. Spitzer, *Cyfrowa demencja. W jaki sposób pozbawiamy rozumu siebie i swoje dzieci*, Wyd. Dobra Literatura, Słupsk 2013, s. 179.

dotychczasowych wyników badań kognitywnych można z całą pewnością stwierdzić, że nie jest to zjawisko obojętne dla umysłu i ciała.

13 **Grupy osób urodzone w połowie lat 90-tych XX wieku określane również mianem „pokolenia Google" nie są zdolne wyobrazić sobie funkcjonowania świata bez sieciowych urządzeń mobilnych**[10]. Osoby z tej kategorii wiekowej wyrosły w zupełnie innych uwarunkowaniach społeczno-technicznych, które zdeterminowały ich neuroplastykę mózgu. Nie jest to jednak pokolenie, jakby się wydawało z pozoru, cyfrowych geniuszy, niesamowitych programistów, wizjonerów, pasjonatów, korzystających z istotnych informacji umieszczonych w odległych zakątkach globu. Spora grupa cyfrowych tubylców ma wręcz problemy z wykonywaniem kluczowych zadań związanych z podstawą programową w zakresie technologii informacyjnej. Korzystanie z mediów w celach rozrywkowych nie przekłada się w prostej linii na umiejętności informatyczne, które są odrębną kategorią wymagającą myślenia algorytmicznego opartego na zdolnościach matematycznych. Typowy cyfrowy autochton być może uruchamia nieskończoną ilość stron i innych „łatwych" w odbiorze materiałów audiowizualnych, jednakże głęboka systematyczna praca umysłowa, będąca podstawą uczenia się jest mu obca. Właściwe uczenie się bez kontroli osób znaczących zastąpione jest „ślizganiem się" po treściach, co nie jest realnym procesem uczenia się.

14 WIELOZADANIOWOŚĆ WE WSPÓŁCZESNYM ŚWIECIE

Innym wymiarem pracy typowej dla współczesnego człowieka jest, jak zaznacza M. Spizter, wielozadaniowość. Według badacza ludzie pracujący w kontakcie z nowymi mediami przerywają wykonywanie właściwych zadań co 11 minut m.in. sprawdzaniem wiadomości w portalu społecznościowym, wybieraniem innej muzyki niż ta, która jest w tle, odpisywaniem na e-maile, wyszukiwaniem informacji w sieci czy też wysyłaniem esemesów lub odbieraniem połączeń telefonicznych. Egzystencja w cyfrowym świecie charakteryzuje się nieustanną realizacją kilku czynności naraz. Jednakże jak dowodzą badania, wykonując wszystkie czynności naraz lub pracując wielowątkowo nad kilkoma zadaniami nie realizujemy ich wszystkich szybciej. Przełączanie się pomiędzy aktywnościami sprzyja nie tylko obniżeniu zdolności do koncentrowania się, lecz prowadzi do wytrenowania większej powierzchowności przetwarzania danych oraz mniejszej efektywności przyswajania danych.

15 PODSUMOWANIE

Zaprezentowane powyżej dylematy nie są próbą stricte naukowego spojrzenia na psychospołeczne funkcjonowanie dzieci i młodzieży w przestrzeni mediów sieciowych, lecz mają przede wszystkim wywołać dyskusję nad przebiegającymi dynamicznie zmianami. Pozbawienie kontroli rodzicielskiej, brak fachowej wiedzy na temat zastosowania nowych mediów w edukacji, czy też iluzoryczna wiara w postęp dzięki nowym technologiom może być i jest w wielu obszarach (np. zmiany w mózgu) niezwykle niebezpieczna dla prawidłowego rozwoju młodego pokolenia. Zatem konieczne w tej sytuacji wydaje się podjęcie dalszej oraz systematycznej głębokiej i merytorycznej debaty nad nowymi zagrożeniami, które pojawiły się za sprawą nowych mediów.

[10] Ł. Tomczyk, A. Wąsiński, *Závislost nových médií u dí a mládeže - polský výhled*, w: K. Kopecký (red.), *Rizika internetové komunikace v teorii a praxi*, Univerzita Palackého, Centrum prevence rizikové virtuální komunikace, Olomouc 2013.

BIBLIOGRAFIA:

Bendyk E., *Bunt sieci*, Biblioteka Polityki, Warszawa 2012.

Holtkamp J., *Co ogłupia nasze dzieci?*, Wydawnictwo Salwator, Kraków 2010.

Huber F., Neuschäffer C., *Rodzice offline? Jak nawiązać kontakt ze skomputeryzowanym dzieckiem*, Wydawnictwo Lekarskie PZWL, Warszawa 2003.

Kowalski R., Limber S., Agatston P., *Cyberprzemoc wśród dzieci i młodzieży*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2011.

Prensky M., *Digital Natives, Digital Immigrants*, On the Horizon 2001, [Online]. [Cit. 2012-10-24]. Dostępne w: MCB University Press, Vol. 9 No. 5, Web site: <http://www.marcprensky.com>.

Pyżalski J., *Agresja elektroniczna wśród dzieci i młodzieży*, Gdańskie Wydawnictwo Psychologiczne, Sopot 2011.

Słysz A., Arcimowicz B., *Przyjaciele w Internecie*, Gdańskie Wydawnictwo Psychologiczne, Sopot 2009.

Spitzer M., *Cyfrowa demencja. W jaki sposób pozbawiamy rozumu siebie i swoje dzieci*, Wyd. Dobra Literatura, Słupsk 2013.

Tomczyk Ł., Wąsiński A., *Závislost nových médií u detí a mládeže – polský výhled*, w: K. Kopecký (red.), *Rizika internetové komunikace v teorii a praxi*, Univerzita Palackého, Centrum prevence rizikové virtuální komunikace, Olomouc 2013.

CYBERPRZEMOC

Velta Lubkina
Gilberto Marzano

OPIS ZJAWISKA

1 WPROWADZENIE

Istnieje wiele zagrożeń związanych z cyberprzestrzenią. Dużą ich część stanowią zagrożenia społeczne, gdyż mają one podłoże kulturalne, takie jak konstruowanie wirtualnej tożsamości czy interakcje w sieciach społecznościowych.

2 Cyberbullying i inne formy cyberprzemocy mogą sprawiać wrażenie, że postęp technologiczny jest czymś złym i najlepiej byłoby, gdyby dzieci nie miały w ogóle dostępu do Internetu, telefonów komórkowych i tym podobnych. Jednak nie powinniśmy tak podchodzić do problemu zagrożeń, jakie niesie ze sobą cyberprzestrzeń – podstępnych i nieustannie narastających. Technologia sama w sobie może być czymś bardzo korzystnym: Internet stanowi źródło informacji i darmowe okno na świat. Nie tylko otwiera pokłady wiedzy (zwłaszcza przed młodzieżą), które w innym przypadku byłyby trudno dostępne, ale pomaga również nawiązywać i utrzymywać kontakty społeczne. Dla wielu osób – patrz sekcja Przydatne technologie – nowe technologie stanowią znakomite rozwiązanie, pozwalają redukować koszty, tworzą nowe miejsca pracy i usługi, jak również alternatywne i efektywne formy uczestnictwa w życiu publicznym/obywatelskim. Internet i związane z nim technologie mają niewątpliwie pozytywny wpływ na nasze życie, natomiast problem może stanowić intencjonalne używanie go w określonych celach przez niektóre osoby. Dlatego istotne jest pogłębianie i szerzenie wiedzy na temat tego, jak zmniejszyć negatywne skutki tych działań.

3 Niniejszy tekst skupia się na cyberbullyingu właśnie ze względu na narastający charakter tego problemu.

4 DEFINICJA

Zanim wyjaśnimy znaczenie terminu **cyberprzemocy** (ang. cyberbullying), należałoby najpierw zastanowić się, czym właściwie jest tradycyjny koncept mobbingu (ang. bullying). **Z mobbingiem mamy do czynienia, jeśli ktoś w sposób zamierzony i powtarzalny prześladuje, grozi, zastrasza inną osobę. Często towarzyszy temu szantaż i inne formy przemocy. Bullying może przejawiać się w następujących formach: agresja słowna, nękanie, znęcanie się fizyczne, obraźliwe listy i wiadomości, nękanie telefonami i e-mailami, szerzenie oszczerstw i plotek oraz wiele temu podobnych.**

4 Zjawisko to może występować na podłożu rasowym, religijnym, płciowym, aparycji, seksualnym, niepełnosprawności lub narodowościowym. Może mieć ono miejsce wszędzie: w szkołach, obiektach sportowych, miejscu pracy etc.

5 W wypadku tego zjawiska mamy do czynienia z przewagą, jaką jedna strona odczuwa nad drugą. Osoby dopuszczające się mobbingu szukają łatwego celu, wybierają jednostki, które mają problem z integracją, wrażliwe i słabe fizycznie. Zatem celem stają się „wykluczeni" przez grupę lub społeczność. Osoby takie zachęca zwłaszcza mowa ciała ich ofiar, jak na przykład postawa czy nieśmiałość przejawiająca się w unikaniu kontaktu wzrokowego.

6 W tradycyjnym ujęciu osoba mobbująca może dopuszczać się przemocy jedynie osobiście, można ją natychmiast rozpoznać i próbować ucieczki, ponieważ osoba taka dąży do fizycznego kontaktu ze swoją ofiarą, by poczuć jej strach i upokorzenie.

7 Mobbing, bez względu na to czy fizyczny, słowny, pośredni, czy względny, został zdefiniowany jako systematyczne nadużywanie siły w sposób ciągły oraz intencjonalny[1].

8 I. Rivers i N. Noret[2] zauważyli, że wiele badań przeprowadzonych nad mobbingiem wskazuje na różnicę wiekową między chłopcami i dziewczynkami, gdy występuje omawiane zjawisko. W wypadku chłopców pojawia się ono wcześniej i przyjmuje postać bezpośredniego znęcania się fizycznego (np. bicie, kopanie), natomiast wśród dziewcząt występuje ono później i ma formę pośredniej lub relacyjnej agresji (szerzenie oszczerstw, wykluczenie społeczne).

9 Jednak najnowsze dane historyczne zebrane przez D. Pepler i in.[3] dowodzą, że z wiekiem różnice płciowe pod względem występowania mobbingu maleją.

10 **Natomiast cyberbullying stanowi szczególną formę mobbingu[4]. Jest to stosunkowo nowe zjawisko definiowane zwykle jako forma mobbingu wyrażająca się poprzez media i urządzenia służące komunikacji, jak telefony komórkowe, e-mail oraz Internet (np. portale społecznościowe, strony internetowe i blogi)**. Osoby stosujące cyberprzemoc szantażują, zastraszają, oczerniają, kompromitują oraz obrażają swoje ofiary. Używają w tym celu zdjęć, filmów, e-maili, wiadomości oraz komentarzy.

11 W przeciwieństwie do innych form mobbingu, co do których istnieje powszechna zgoda badaczy dotycząca powtarzalności zachowań, badania nad cyberprzemocą zdają się być mniej restrykcyjne co do powtarzalności oraz interakcji między ofiarą i napastnikiem, głównie ze względu na anonimowość, którą daje napastnikowi Internet[5].

12 W swojej publikacji N. Willard zidentyfikowała siedem różnych odmian, w jakich przejawia się cyberprzemoc:

Flaming: wysyłanie agresywnych, wulgarnych wiadomości o konkretnej osobie do grupy lub do niej samej przez e-mail lub inną formę komunikacji tekstowej.

Zastraszanie online: powtarzalne wysyłanie obraźliwych wiadomości e-mailowych lub w innej formie tekstowej do osoby zastraszanej.

Cyberstalking: zastraszanie online w formie pogróżek.

Dyskredytacja: wysyłanie nieprawdziwych, oszczerczych, okrutnych informacji o określonej osobie do innych lub zamieszczanie takich informacji online.

Podszywanie się pod kogoś: podszywanie się pod konkretną osobę i wysyłanie lub zamieszczanie informacji w jej imieniu w sieci w celu poniżenia jej.

[1] Por. Nansel i in., 2001; Besag, 2006; Bowie, 2007; Murray-Close i in., 2007; Rivers i in., 2007; Williams i Guerra, 2007).

[2] I. Rivers, N. Noret, N., *'I h 8 u': Findings from a Five-year Study of Text and e-mail Bullying*, "British Educational Research Journal", 36/2010, 4, s. 643–671.

[3] D. Pepler, D. Jiang, W. Craig, J. Connolly, *Developmental Trajectories of Bullying and Associated Factors*, "Child Development", 79/2008, s. 325–338.

[4] R. Kowalski, S. Limber, *Electronic Bullying Among Middle School Students*, "Journal of Adolescent Health", 41/2007, 41, s. 22–30 .

[5] J. Wolak, K. Mitchell, D. Finkelhor, *Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-only Contacts*, "Journal of Adolescent Health", 41/2007, 6 (Supplement), s. 51–58.

Wykluczenie: wykluczenie w okrutny sposób kogoś z grupy online[6].

13 **RÓŻNICE MIĘDZY CYBERBULLINGIEM A MOBBINGIEM**

Norweski naukowiec D. Olweus[7] uważa, że mobbing zasadza się na trzech kluczowych elementach: agresji, powtarzalności oraz sile:

Mobbing charakteryzują trzy następujące kryteria: (a) agresywne zachowanie lub intencjonalne krzywdzenie, (b) powtarza się ono w czasie oraz (c) ma miejsce w ramach relacji interpersonalnych charakteryzujących się asymetrią władzy[8].

14 Zachowanie osoby mobbującej jest z natury agresywne, z intencją zranienia uczuć innej osoby, popsucia jej relacji z innymi lub wręcz jej nastraszenia. Osoba będąca celem mobbingu musi się bronić przed atakami, które często nie są przez nią sprowokowane.

15 **ROZPOZNANIE**

Cyberbullying łączy z tradycyjnym pojęciem mobbingu intencjonalne agresywne zachowanie. Osoby zastraszające w cyberprzestrzeni chcą poniżyć swój cel, rozsyłając kompromitujące zdjęcia lub wymierzone w daną osobę wiadomości. Najczęściej pojawiającą się w tym wypadku wiadomością jest 'I h 8 u' (ang. nienawidzę cię), po której następują obelgi[9]. Przemoc nie odbywa się na poziomie fizycznym, lecz u jej podstaw leży ta sama motywacja, co w przypadku mobbingu.

16 Nawet cyberprzemoc jest zwykle powtarzalna lub ze względu na jej naturę, osoba będąca celem może się z nią zetknąć parokrotnie, natomiast jednorazowy obraźliwy esemes niekoniecznie wpisuje się w definicję mobbingu.

17 Główna różnica pomiędzy tradycyjnym pojęciem mobbingu i cyberbullyingiem polega na tym, że ten pierwszy zasadza się na relacji siły, przejawiającej się przez bezpośredni agresywny kontakt z celem. Z tego względu mobbing może być postrzegany jako forma znęcania się nad innymi, z tym że napastnik znęca się nad rówieśnikami. Cechą odróżnia tę formę przemocy od znęcania się nad dziećmi czy przemocą w domu jest kontekst, w którym się ona odbywa oraz relacje stron. Natomiast najistotniejszym elementem cyberprzemocy jest fakt, że najczęściej tożsamość agresora pozostaje nieznana. Zwykle osoba zastraszana nie jest pewna, kto jest autorem konkretnego komentarza lub kto ukrywa się za fałszywym profilem, co może prowadzić do poczucia bezsilności w przypadku ofiary. Natomiast anonimowość, jaką daje sieć, może prowadzić do braku zahamowań, sprawiając, że w sieci ludzie są skłonni do wypowiedzi i czynów, od których normalnie by się powstrzymali, właśnie dlatego, że czują się niewidoczni.

18 Q. Li uważa, że znajomość takich zmiennych jak płeć, kultura, znajomość strategii bezpieczeństwa oraz częstotliwość korzystania z komputera może dostarczyć cennych informacji w celu oceny stopnia prawdopodobieństwa uczestniczenia w cyberbullyingu. Autor wskazuje na wagę studiów porównawczych nad mobbingiem i cyberprzemocą w celu zrozumienia, jak na cyberbullying wpływają tradycyjne sposoby nękania[10].

6 N. E. Willard, *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*, Research Press, 2007.

7 Dr Dan Olweus jest pionierem w badaniach nad zapobieganiem mobbingowi oraz autorem program Olweus Bullying Prevention Program, obecnie najsłynniejszego programu prewencyjnego w tej dziedzinie.

8 http://www.colorado.edu/cspv/blueprints/modelprograms/BPP.html, data dostępu 3.02.2013.

9 'I h 8 u' – ang. I hate you – nienawidzę cię, to skrót zwykle używany w chat roomach.

10 Q. Li, *Bullying in the New Playground: Research into Cyberbullying and Cyber Victimization*, "Australasian Journal of Educational Technology", 23/2007, 4, s. 435-454.

19 BADANIA NAD CYBERBULLYINGIEM

Tabela przedstawia najważniejsze badania nad cyberbullyingiem przeprowadzone od 2002 roku, rozpoczęte przez Kowalskiego i in.[11] a następnie kontynuowane przez Riversa i Noret[12].

Tab. 1. Zestawienie najważniejszych badań nad cyberbullingiem

Badanie	n	Przedział wiekowy	Metoda	Rodzaj badanego cyberbullyingu
Finkelhor I in. (2000)	1501	10–17	Reprezentatywna ankieta narodowa – Youth Internet Safety Survey – YISS 1 (US)	Zastraszanie online: komunikator, chat room, e-mail
NCH (dziś Action for Children) (2002)	856	11–19	Ankieta (UK)	SMS/wiadomości tekstowe, chat room oraz e-mail
Ybarra i Mitchell (2004)	1501	10–17	Reprezentatytwna ankieta narodowa YISS 1–1999–2000 (US)	patrz YISS 1
NCH 'Putting U in the Picture—Mobile Bullying Survey' (2005)	770	11–19	Ankieta (UK)	SMS/wiadomości tekstowe, Internet, chat room oraz e-mail
Li (2005)	177	12–13	Ankieta (Canada) przeprowadzona wśród uczniów 7 klasy	Niesprecyzowane zachowanie– e-mail, chat room, I telefon komórkowy (niejasne czy odnosi się do SMS/wiadomości tekstowych czy/lub agresji słownej)
Agatston i Carpenter (2006)	257	11–14	Gimnazjalna ankieta szkolna klasy 6–8 (USA)	komunikator i strona internetowa
Fight Crime Pre-teen (2006)	503	6–11	Ankieta telefoniczna (USA)	SMS/ wiadomości tekstowe, e-mail, komunikator, strona internetowa, chat room, zdjęcia
Fight Crime Teen (2006)	512	12–17	Ankieta telefoniczna (USA)	SMS/ wiadomości tekstowe, e-mail, komunikator, strona internetowa, chat room, zdjęcia
Kowalski i Limber (2006)	3767	11–14	Ankieta przeprowadzona wśród uczniów 6-8 klasy – (USA)	Mobbing elektroniczny: e-mail, komunikator, chat room, strona internetowa, SMS/ wiadomości tekstowe.
Kowalski i Witte (2006)	700	> 11	Ankieta przeprowadzona głównie wśród uczniów szkoły średniej (USA)	komunikator, chat room, e-mail
Li (2006)	264	12–15	Ankieta	Mobbing online: blog, komunikator, e-mail
Patchin i Hinduja (2006)	384	< 18	Ankieta online (USA)	SMS/ wiadomości tekstowe, chat room, e-mail, bulletin board, komunikator komputerowy, grupy dyskusyjne

[11] R. Kowalski, S. P. Limber, *Electronic Bullying Among Middle School Students*, "Journal of Adolescent Health", 41/2007.

[12] I. Rivers, N. Noret, *'I h 8 u': Findings from a Five-year Study of Text and e-mail Bullying*, "British Educational Research Journal", 36/2010, s. 4.

Smith i in. (2006)	92	11–16	Ankieta (UK)	Telefon komórkowy, SMS/ wiadomości tekstowe, e-mail, zdjęcia/filmy, komunikator, strona internetowa, chat room
Ybarra i in. (2006)	150	10–17	Reprezentatytwna ankieta narodowa – YISS 2–2005– (US	patrz YISS 1
WiredSafety (2006)	>900	>7	Ankieta online	Mobbing online
Williams i Guerra (2007)	1378	< 18	Ankieta online (USA)	Komunikator komputerowy, e-mail, SMS/ wiadomości tekstowe, chat room, bulletin board, grupa dyskusyjna
Li (2007)	461	12–15	Ankieta	Rola komputera w cyberbullyingu
Smith i in. (2008)	533	11–16	Ankieta szkolna	Telefon komórkowy, SMS/ wiadomości tekstowe, e-mail, zdjęcia/filmy, komunikator, strona internetowa, chat room

Źródo: I. Rivers, N. Noret, *'I h 8 u': Findings from a Five-year Study of Text and e-mail Bullying*, "British Educational Research Journal", 36/2010, p. 4.

20 RÓŻNICE PŁCIOWE

Badania przeprowadzone nad tradycyjnymi formami mobbingu dowodzą, że chłopcy wykazują większą skłonność do tej formy przemocy niż dziewczęta[13], jednak dane są mniej spójne pod względem różnic płciowych w badanych doświadczeniach mobbingu. Niektóre badania dowodzą, że chłopcy częściej zgłaszają akty cyberprzemocy niż dziewczęta, podczas gdy inne nie doszukały się takiej różnicy lub była ona nieistotna[14]. W wypadku chłopców istnieje większe prawdopodobieństwo napaści fizycznej przez rówieśników[15], podczas gdy dziewczęta są częściej nękane poprzez oszczerstwa lub gesty/komentarze na tle seksualnym[16]. Należy również podkreślić, że chłopcy są często nękani przez innych chłopców (rzadziej przez dziewczęta), natomiast dziewczęta bywają nękane przez przedstawicieli obu płci[17]. Chłopcy bywają ofiarami mobbingu fizycznego lub werbalnego, natomiast mobbing w wypadku dziewcząt przyjmuje formę społecznego wykluczenia (np. dziewczyna nie jest włączana w aktywności grupy, w sposób krzywdzący i celowy).

21 Badanie przeprowadzone wśród 264 uczniów trzech szkół średnich dowodzi, że niemalże połowa z nich padła ofiarą mobbingu, natomiast jedna czwarta cyberprzemocy. Ponad połowa uczniów donosi, że znała ofiarę cyberbullyingu. Prawie połowa sprawców cyberprzemocy używała urządzeń elektronicznych więcej niż trzykrotnie do nękania innych. Większość ofiar i świadków tej formy przemocy nie zgłaszała tego faktu dorosłym. Pod względem płci zaobserwowano istotne różnice zarówno w wypadku mobbingu, jak i cyberbullyingu. Chłopcy częściej byli sprawcami mobbingu i cyberbullyingu, natomiast dziewczęta częściej zgłaszały akty cyberbullyingu rodzicom[18].

[13] Por. Currie i in., 2004; Nansel i in., 2001; Olweus, 1993.

[14] Por. Kowalski, R. M., Limber S. P, *Electronic Bullying Among Middle School Students*, "Journal of Adolescent Health", 41/2007.

[15] Por. Finkelhor i in., 2005; Nansel i in., 2001; Olweus, 1993; Rigby, 2002.

[16] Por. Nansel i in., 2001.

[17] Por. Finkelhor i in., 2005; Nansel i in., 2001; Olweus, 1993.

[18] Q. Li Cyberbullying in Schools: *A Research of Gender Differences*, "School Psychology International", 27/2006, s. 157–170.

22 SPRAWCY CYBERBULLINGU

Sprawcy cyberbullyingu używają stron internetowych do rozpowszechniania kłamstw. Podobnie jak w wypadku tradycyjnego mobbingu, istnieje określony powód ich zachowania. Z tego względu wiedza na temat tego, jak działają może pomóc ich wykryć. Zwykle znają oni technologię internetową oraz sposób, w jaki funkcjonują portale społecznościowe. Na cyberbullying wpływ ma rozwój technologii. Wraz z pojawieniem się telefonów z wbudowaną kamerą pojawiła się możliwość zrobienia kompromitującego zdjęcia lub nakręcenia filmiku nieświadomej tego osobie i rozesłania ich wśród rówieśników w celu zawstydzenia ofiary.

Często sprawcy tej formy przemocy podszywają się pod kogoś innego, z nadzieją, że nie zostaną złapani.

D. Roome wylicza motywy kierujące sprawcami cyberbullyingu[19]:

dla wielu z nich poczucie przewagi nad ofiarą jest źródłem satysfakcji. Reakcja ofiary często zachęca ich do kontynuowania i intensyfikowania działań;

dla niektórych cyberbullying jest sposobem na podniesienie popularności i poczucia wartości. Ich samoocena wzrasta poprzez to, że prezentują się w roli eksperta;

jednym z motywów jest zazdrość;

nękanie może być sposobem na zwrócenie na siebie uwagi lub wywołanie w ofierze uczucia strachu;

różnice na tle kulturowym i rasowym mogą przyczynić się do cyberbullyingu w formie krzywdzących i dyskryminujących komentarzy;

osoby pochodzące z rodzin dysfunkcyjnych lub które doświadczyły odrzucenia społecznego częściej mają skłonność do znęcania się nad innymi;

w niektórych wypadkach sprawcy cyberbullyingu sami kiedyś padli ofiarami tej formy przemocy, zatem jest to dla nich sposób na dowartościowanie się;

zaburzenia osobowości mogą uniemożliwić sprawcy mobbingu ocenę jego czynów;

choroby psychiczne również mogą leżeć u podłoża cyberprzemocy;

również niedojrzałość może być istotnym czynnikiem w tego typu relacjach. Sprawca może być nieświadomy bólu i udręki, do jakich się przyczynia. Zdarza się to w wypadku dzieci i nastolatków;

niektórzy dopuszczają się tej formy przemocy w przekonaniu, że nigdy nie zostaną złapani;

Do powyższej listy można dodać wszelkiego rodzaju uczucia zazdrości i urazy, jak również fakt, że cyberbullying nie wymaga kontaktu fizycznego. Sprawcy mogą wyobrażać sobie, że nie krzywdzą prawdziwych osób, lecz ich wirtualne profile.

23 CEL CYBERBULLYINGU

I. Rivers oraz N. Noret przeprowadzili badania nad pogróżkami w formie tekstów i wiadomości e-mail otrzymanych przez uczniów klas 7 i 8 (w wieku 11-13 lat) uczęszczających do 13 szkół w północnej Anglii w latach 2002—2006. Wyniki wskazują, że w ciągu pięciu lat wzrosła liczba osób otrzymujących tego typu wiadomości przynajmniej raz, wzrost ten był większy w grupie badanych dziewcząt. Natomiast liczba stale otrzymywanych tego typu wiadomości była

[19] Por. D. Roome, *Cyberbullying is Never Alright*, Debbie Roome, 2012.

ROZPOZNANIE OBJAWY

porównywalna w powyższym przedziale czasowym. W grupie chłopców otrzymywali je uczniowie doświadczający fizycznej przemocy, w grupie dziewcząt – zwykle skierowane były one do mniej popularnych dziewczynek. Chłopcy zwykle dostawali wiadomości o treści opierającej się na uczuciu nienawiści, natomiast dziewczynki były zwykle ofiarami napaści werbalnej[20].

Istnieją również grupy osób częściej stanowiące cel tego typy ataków niż inni[21].

24 OFIARY CYBERPRZEMOCY

Poniżej zaprezentowano kilka typowych grup ofiar nękania, należy jednak pamiętać, że osoby nienależące do żadnej z wymienionych grup również mogą stać się celem ataków, a zdarza się również, że ofiarami padają osoby przypadkowe:

- dzieci i osoby psychicznie i fizycznie upośledzone;
- osoby wyróżniające się, inne (ze względu na pochodzenie, przekonania kulturowe lub religijne) lub nie należące do społeczności;
- nastolatki i dzieci powszechnie postrzegane jako „lamusy", „palanty", „kujony";
- osoby cechujące się irytującymi nawykami lub nieakceptowalnym zachowaniem;
- osoby pochodzące z nizin społecznych.

25 D. Olweusuważa, że mimo iż nie istnieje jeden profil ofiary, przeprowadzone badania wskazują, że dzieci będące ofiarami mobbingu wykazują jedną lub więcej z następujących cech:

- zwykle są ciche, ostrożne, wrażliwe, skłonne do płaczu;
- mogą one być niepewne siebie, mieć mało wiary we własne możliwości, niskie mniemanie o sobie;
- często mają wąskie grono przyjaciół i są społecznie wyizolowane;
- obawiają się skrzywdzenia;
- mogą być nerwowe lub przygnębione;
- zwykle są fizycznie słabsze od rówieśników (zwłaszcza w przypadku chłopców);
- mogą preferować spędzanie czasu z dorosłymi (rodzicami, nauczycielami, trenerami), niż z rówieśnikami.[22]

26 OZNAKI I REZULTATY CYBERBULLYINGU

Historie cyberprzemocy dowodzą, że niektóre zachowania jej ofiar często się powtarzają, jak przypadki typu samookaleczenia.

27 Istnieją również przeróżne fizyczne oznaki, poczynając od symptomów somatycznych po prawdziwe choroby. Najczęściej spotykane są oznaki związane ze stresem, typu moczenie nocne, koszmary, nudności lub napady złości. Istnieją również bardziej dyskretne symptomy, gdy dzieci mają trudności ze skupieniem się, są zamyślone.

28 OBRONA PRZED CYBERBULLYINGIEM

Mobbing i cyberbullying mogą być zjawiskami ściśle ze sobą związanymi. Możliwość skupienia na sobie uwagi przez napastnika oraz możliwość intensyfiko-

[20] Por. I. Rivers, N. Noret, *'I h 8 u': Findings from a Five-year Study of Text and e-mail Bullying*, "British Educational Research Journal", 36 (2010), s. 4.

[21] Por. K. J. Mitchell, D. Finkelhor, J. Wolak, *Victimization of Youths on the Internet*, "Journal of Aggression", Maltreatment, and Trauma, (2003), 8, 1–39

[22] D. Olweus, *Bullying at School: What We Known and What We Can Do*, Oxford, Blackwell, 1993

wania doznań mobbingu jest istotnym elementem, który należy brać pod uwagę w przeciwdziałaniu przemocy.

29 Najprostszym wyjściem wydaje się wyłączenie Internetu i skasowanie profilu na portalu społecznościowym. Jednak nie jest to takie proste. Wstyd związany z upokorzeniem nie kończy się w takim przypadku. Ponadto osoby należące do społeczności Internetowej mają potrzebę poznać opinie innych.

30 Mimo to obrona przed tego typu atakami jest jak najbardziej możliwa. Istnieje wiele stron internetowych oferujących pomoc w takich przypadkach. Istnieje również komercyjne i darmowe oprogramowanie kontroli rodzicielskiej, dzięki któremu rodzice mogą ograniczyć czas, jaki ich pociechy spędzają online, rodzaje odwiedzanych przez nie stron internetowych poprzez blokowanie tych niepożądanych. Niektóre oprogramowania pozwalają na eliminowanie niepożądanych konwersacji poprzez opcję filtrowania wiadomości e-mailowych lub komunikatorów pod względem używanego wulgarnego języka. Istnieją również narzędzia pzowalające na analizę zdjęć, dzięki czemu można zapobiec oglądaniu niepożądanych obrazów przez dzieci.

31 Naturalnie wszystkie tego typu narzędzia mają ograniczone działanie w przypadky cyberprzemocy. Dlatego nic nie zastąpi zapobiegawczych i czujnych rodziców, gdy ich dziecko jest ofiarą przemocy, bez względu na to, czy w świecie wirtualnym czy realnym. Dla przykładu, jeśli dziecko wykazuje mniejsze zainteresowanie, spędza mniej czasu grając lub oddając się ulubionym dotychczas aktywnościom online lub przeciwnie, jeśli natychmiast zamyka przeglądarkę, gdy ktoś wchodzi do jego pokoju i unika odpowiedzi na pytanie o to, co robiło – może to stanowić wskazówkę.

32 Najlepszym sposobem ochrony przed zagrożeniem cyberbullyingu jest edukacja dzieci i dorosłych, dostarczanie informacji i prezentowanie przykładów stymulujących ich odpowiednią reakcję.

33 **OD MEGAN MEIER DO AMANDY TODD**

Dwa przypadki można uznać za obrazujące ewolucję tego zjawiska: przypadek Megan Meier oraz Amandy Todd. Przypadek Amandy Todd ukazuje, jak świat wirtualny i realny zaczynają się przenikać, stanowiąc jedną całość. Nowe technologie mają nie tylko wzmacniać efekt ataku, ale również pomagają wzniecić agresję w sieci społeczności, których rola i znaczenie nieustannie wzrastają.
Przypadek Megan Meier został w następujący sposób przedstawiony w Wikipedii:

> Megan Taylor Meier (6 listopada 1992 – 17 października 2006) była amerykańską nastolatką z Dardenne Prairie, w stanie Missouri, która popełniła samobójstwo przez powieszenie na trzy tygodnie przed swoimi czternastymi urodzinami. Rok później jej rodzice rozpoczęli dochodzenie w sprawie samobójstwa, które przypisano cyberbullingowi za pomocą portalu społecznościowego MySpace. Matka koleżanki Meyer, Lori Drew, została oskarżona w tej sprawie w 2008 r., lecz w 2009 została uniewinniona[23].

[23] http://en.wikipedia.org/wiki/Suicide_of_Megan_Meier data dostępu 4.02.2013.

DOBRE PRAKTYKI

34 Według strony internetowej poświęconej jej pamięci[24], w wieku trzynastu lat życie Megan zaczęło zmieniać się na lepsze, po tym gdy straciła dziesięć kilogramów, zmieniła szkołę (z publicznej na prywatną) i chłopiec, rzekomo szesnastoletni Josh Evans skontaktował się z nią przez MySpace, wyrażając swoje zainteresowanie jej osobą. Jednak relacja z rzekomym chłopcem nagle ulega zmianie, gdy zaczął on zamieszczać w Internecie informacje o tym że Megan jest „dziwką" i jest „gruba". W dniu samobójstwa Megan otrzymała wulgarne wiadomości. Po tym gdy matka wyraziła swoją dezaprobatę wobec przypadku, który dotknął jej córkę, Megan rzekomo wpadła w furię, ponieważ rodzice nie byli „po jej stronie". Po samobójstwie Megan jej rodzice dowiedzieli się, że szesnastolatek nigdy nie istniał, lecz został wymyślony przez matkę byłej koleżanki Megan.

35 W smutnej historii Megan należy rozważyć następujące elementy:

1. Fałszywą tożsamość chłopca oraz wiadomości pisane przez różne osoby, które miały dostęp do profilu.
2. Nieujawnieni dorośli zamieszani w sprawę.
3. Brak empatii ze strony matki Megan, która była poirytowana zamiast stanąć „po jej stronie" (jak to ujęła sama Megan w liście pożegnalnym napisanym przed popełnieniem samobójstwa).

36 Historia Amandy Todd w następujący sposób została przedstawiona w Wikipedii:

> 7 września 2012 roku Todd zamieściła 9-cio minutowy film na YouTube zatytułowany *Moja historia: zmagania, mobbing, samookaleczenie i samobójstwo*, w którym za pomocą serii plansz opowiedziała o swoim prześladowaniu. Do października jej film miał 1 600.000 odsłon.

W swoim filmie Todd mówi, że w 7. klasie używała wideo czatu do poznawania nowych ludzi przez Internet, którzy prawili komplementy dotyczące jej aparycji. Nieznajomy przekonał Todd, żeby obnażyła biust przed kamerą. Później groził, że ujawni zdjęcie jej przyjaciołom, jeśli nie pokaże więcej. Todd pisze, że w trakcie przerwy Świąt Bożego Narodzenia policja poinformowała ją o 4:00 rano, że zdjęcie krąży po Internecie. Todd twierdzi, że miała lęki, depresję i napady paniki tym spowodowane. Jej rodzina przeniosła się w nowe miejsce, gdzie Todd zaczęła nadużywać narkotyków i alkoholu. Rok później nieznajomy pojawił się ponownie, tworząc profil na Facebooku, w którym wykorzystał zdjęcie topless Todd jako swoje zdjęcie profilowe i skontaktował się z jej nowymi szkolnymi kolegami. Znów dokuczano Todd, co skończyło się ponowną zmianą szkoły. Amanda pisze, że rozpoczęła czat ze „starym przyjacielem", który się z nią skontaktował. Zaprosił Todd do swojego domu, gdzie uprawiali seks, podczas gdy jego dziewczyna była na wakacjach. Tydzień później Todd została zaatakowana przez zazdrosną dziewczynę i grupę jej przyjaciół, którzy wykrzykiwali przy tym obelgi. Po tym ataku Todd próbowała popełnić samobójstwo, wypijając wybielacz, lecz uratował ją natychmiastowy transport do szpitala i płukanie żołądka.

Po powrocie do domu Todd odkryła obelżywe wiadomości o jej nieudanym samobójstwie na Facebooku. Rodzina znów się przeniosła w nowe miejsce, by zacząć wszystko od nowa, lecz przeszłość wciąż podążała za Todd. Sześć miesięcy później kolejne wiadomości i obelgi były zamieszczane na portalach społecznościowych. Jej stan psychiczny uległ

[24] http://www.meganmeierfoundation.org/megansStory.php, data dostępu 4.02.2013.

pogorszeniu, czego wyrazem było samookaleczanie. Pomimo przyjmowanych antydepresantów i pomocy psychologa przedawkowała leki i spędziła dwa dni w szpitalu.

Dokuczano jej z powodu niskich ocen, wynikających z trudności w przyswajaniu wiedzy i licznych pobytów w szpitalu, w czasie których leczyła depresję.

10 października 2012 roku około godziny 18:00 wieczorem znaleziono Todd powieszoną w domu.

37 Historia Amandy Tood zaczyna się podobnie do historii Megan od nieznajomego, prezentującego się jako przyjaciel, który pochlebstwami zyskał jej zaufanie i w przypadku Amandy zdjęcie topless. Jednak druga część historii Amandy jest zupełnie inna. Amanda zostaje zaatakowana przez osoby, które zna i jest prześladowana przez koleżanki i kolegów z klasy. Informacje o jej nieudanej próbie samobójstwa zostają rozprzestrzenione na Facebooku i obraźliwe wiadomości pod jej adresem są zamieszczane na portalach społecznościowych. W przypadku Amandy mamy do czynienia z furią grupową zarówno w sieci, jak i w życiu.

38 DOŚWIADCZENIA I ŚRODKI ZAPOBIEGAWCZE NA ŁOTWIE

Na Łotwie wprowadzono kilka projektów w omawianym zakresie. Jeden z nich, pod nazwą "Safety Online" (ang. bezpieczeństwo w sieci), zapoczątkowany przez Microsoft, został wsparty przez Państwowy Inspektorat do spraw Ochrony Praw dzieci, projekt "Net-Safe Latvia", oraz liczne ogranizacje pozarządowe. Można znaleźć wiarygodne i praktyczne porady dotyczące bezpieczeństwa w sieci na stronie kampanii <http://www.draudzigsinternets.lv/html/etusivu.html> (data dostępu: 4 lutego 2013). Pomogą one nawet najbardziej wrażliwym użytkownikom czuć się bezpiecznie, gdy pracują online.

39 Istnieje również szereg informacji dotyczących środków zapobiegawczych dostępnych dla nauczycieli, rodziców oraz opiekunów. Materiały skierowane do nauczycieli mają na celu wspomóc ich pracę w następujących obszarach:

- dyskusje z uczniami na temat bezpieczeństwa;
- informacja na temat, w jaki sposób dzieci korzystają z internetu;
- informacja na temat, w jakich celach informacje prywatne są używane w Internecie;
- informacja na temat, gdzie szukać dodatkowych wiadomości.

40 Materiały przeznaczone dla rodziców lub opiekunów mają postać przewodnika "Guide to the Safe Use of the Internet Environment" (przewodnik do bezpiecznego korzystania z Internetu) zawierającego dyskusje online, prawa dzieci w Internecie, okazję do zgłoszenia istniejącego problemu oraz opis bezpiecznego korzystania z Internetu w grupach wiekowych: 7–9 lat, 10–12 lat oraz 13–15 lat.

41 Informacja dla rodziców, uczniów i pracowników socjalnych w języku łotewskim, rosyjskim i angielskim jest dostępna pod adresem < http://www.netsafe.lv/page/116 > (data dostępu: 8 lutego 2013).

42 PODSUMOWANIE

Badanie "Modern Technology Usage and Internet Safety" przeprowadzone w okresie od maja do czerwca 2010 roku dostarcza informacji na temat znajomości środków bezpieczeństwa, korzystania z Internetu oraz nawyków dzieci, młodzieży, rodziców i nauczycieli w trakcie

DOBRE PRAKTYKI

korzystania z nowoczesnych technologii. Badanie przeprowadzono, wykorzystując metody ilościowe – pośredni wywiad komputerowy – i oparte jest na odpowiedziach 2017 respondentów. Informacja na temat badania została rozpowszechniona w szkołach po to, by nauczyciele przekazali uczniom wiadomość o tym, że mogą w czasie lekcji informatyki wypełnić ankiety.

43 Najważniejsze wyniki badania są następujące:

- w wieku 13 lat ponad 90% dzieci korzysta z Internetu i posiada telefon komórkowy;
- 35% dzieci w wieku 6–13 oraz 54% w wieku 14–18 lat twierdzi, że ich rodzice nie ograniczają ich czasu korzystania z telefonu komórkowego;
- 42–47% dzieci i nastolatków twierdzi, że Internet nie stanowi dla nich zagrożenia;
- ponad 40% dzieci i nastolatków przyznaje, że spotkało się z nieprzyjemnym materiałem pornograficznym, dostępnym bez żadnych ostrzeżeń. 39% twierdzi, że spotkało się z materiałem zawierającym przemoc. 22–31% twierdzi, że były ofiarami mobbingu online. 10% w wieku 6–13 lat oraz 19% w wieku 14–18 lat twierdzi, że otrzymało propozycje seksualne od osób dorosłych;
- 19% twierdzi, że odbierało niepokojące telefony i esemesy na telefon komórkowy, 9% twierdzi, że otrzymało groźby w postaci esemesów lub za pośrednictwem telefonów komórkowych i 5% twierdzi, że otrzymało nieprzyjemne materiały seksualne lub esemes na telefon komórkowy;

44 Generalnie dzieci i młodzież potrafią dobrze ocenić, co jest i co nie jest odpowiednie w sieci, 10–13% dzieci i nastolatków twierdzi, że nękało innych, używając telefonu komórkowego lub Internetu[25].

[25] Por. http://www.netsafe.lv/page/116, data dostępu: 8.02.2013).

BIBLIOGRAFIA:

Besag, V. E., *Understanding Girls' Friendships, Fights and Feuds: a Practical Approach to Girls' Bullying*, Maidenhead, Open University Press, 2006.

Bowie, B. H., *Relational Aggression, Gender and the Developmental Process*, "Journal of Child and Adolescent Psychiatric Nursing", 20/2007, s. 2.

Kowalski, R. M., Limber S. P, *Electronic Bullying Among Middle School Students*, "Journal of Adolescent Health", 41/2007.

Li Q., Cyberbullying in Schools: *A Research of Gender Differences*, "School Psychology International", 5/2006), s. 27.

Li Q., *Bullying in the New Playground: Research into Cyberbullying and Cyber Victimization*, "Australasian Journal of Educational Technology", 23 (2007), 4,

Mitchell K. J., Finkelhor D., Wolak J., *Victimization of Youths on the Internet*, "Journal ofAggression", Maltreatment, and Trauma, 8/2003.

Murray-Close D., Ostrov J., Crick N., *A Short-term Longitudinal Study of Growth of Relational Aggression During Middle Childhood: Associations with Gender, Friendship Intimacy, and Internalizing Problems*, "Developmental Psychopathology", 19/2007, s. 1.

Willard N. E., *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*, Research Press, 2007.

Olweus, D., *Bullying at School: What We Know and What We Can Do*, Oxford, Blackwell, 1993.

Pepler, D., Jiang, D. Craig, W., Connolly, J., *Developmental Trajectories of Bullying and Associated Factors*, "Child Development", 79/2008.

Rivers, I., Duncan, N., Besag, V. E., *Bullying: a Handbook for Educators and Parents*, Westport, Greenwood Press, 2007
Rivers, I., Noret, N., *'I h 8 u': Findings from a Five-year Study of Text and e-mail Bullying*, "British Educational Research Journal", 36/2010, s. 4.

Roome D., *Cyberbullying is Never Alright*, Debbie Roome, 2012.

Underwood M. K., Rosen L. H., *Gender and Bullying: Moving Beyond Mean Differences to Consider Conceptions of Bullying*, w: Espelage D. L., Swearer S. M. (Eds.), *Bullying in North American Schools* 2nd Edition, London, Routledge, 2010.

Williams, K. R. & Guerra, N. G, *Prevalence and Predictors of Internet Bullying*, "Journal of Adolescent Health", 41/2007, s. 6.

Wolak J., Mitchell K. J., Finkelhor D., *Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-only Contacts*, "Journal of Adolescent Health", 41/2007, s. 6 (Supplement).

ZAGROŻENIA ZDROWIA PSYCHICZNEGO I FIZYCZNEGO

ZAPOBIEGANIE
CYBERPRZEMOCY

Velta Lubkina
Gilberto Marzano

OPIS ZJAWISKA

1 WPROWADZENIE

Niniejszy artykuł został zainspirowany przez dziesięć wskazówek autorstwa S. Hinduji i J. W. Patchina mających na celu zapobieganie cyberprzemocy[1].

Pierwszy prewencyjny krok to znajomość samego zjawiska – wiedza na temat cyberbullyingu i jak się on przejawia w poszczególnych kontekstach. To nie takie proste, gdyż cyberprzemoc jest skomplikowanym i stosunkowo nowym zjawiskiem, w związku z czym badacze wciąż się spierają co do jego definicji i zasięgu. Mimo to cyberbullying stanowi realne zagrożenie, zwłaszcza dla pokolenia online, które często ma trudności z odróżnieniem rzeczywistości od świata wirtualnego. Ponadto Internet jest przepastnym, intrygującym światem, trudnym do zgłębienia, pełnym przydatnych informacji, ale i niebezpieczeństw, który ulega nieustannym przemianom.

2 Literatura przedmiotu podkreśla podstawową rolę edukacji w walce z cyberprzemocą. Istnieje ogólny konsensus co do odpowiedzialności szkół w tej nierównej walce. Jednak tworzenie skutecznych programów nie jest wcale takie proste, gdy weźmie się pod uwagę liczbę implikacji oraz konieczność integrowania wiedzy z różnych dziedzin.
Niniejszy artykuł analizuje wpływ zdobywanej wiedzy kontekstualnej, aktywności edukacyjnych oraz technicznego wsparcia na zapobieganie i walkę z zagrożeniem cyberbullyingiem wśród młodzieży.

Słowa kluczowe: zapobieganie cyberbullyingowi, rady dla pedagogów

3 PODSTAWOWE INFORMACJE

Kilka lat temu S.Hinduja oraz J.W. Patchin wymienili dziesięć wskazówek dla pedagogów pomagających zapobiegać cyberprzemocy[2]. Można je podzielić na trzy grupy:

- Przyswajanie wiedzy kontekstualnej (wskazówka: *ocena formalna*);
- Aktywności edukacyjne (wskazówki: *uświadamiaj uczniów, że wszelkie formy mobbingu są nieakceptowalne; wyznacz jasne reguły dotyczące korzystania z Internetu i urządzeń elektronicznych; dbaj o pozytywną atmosferę w szkole, edukuj twoją społeczność*);
- Wsparcie techniczne (wskazówki: *konsultuj się ze szkolnym prawnikiem, zanim dojdzie do incydentu; stwórz wszechstronny kontakt formalny; zainstaluj oprogramowanie blokujące/filtrujące; wyznacz „Eksperta do spraw cyberprzemocy”*).

4 Zajęcia z aktywności edukacyjnych opierają się na pięciu z wymienionych dziesięciu rad, co podkreśla wagę edukacji w promowaniu odpowiednich strategii rozwiązywania problemu. W kolejnych sekcjach wskazówki S.Hinduji i J. W.Patchinga są dokładnie analizowane i komentowane, jednak zanim przejdziemy do części dotyczącej przeciwdziałania cyberprzemocy, najpierw należałoby zdefiniować sam termin.

5 PRZYPOMNIENIE

Czym jest cyberprzemoc

T. Beran i Q. Li określili to zjawisko słowami „stare wino w nowych butelkach”[3].

[1] S. Hinduja, J. W. Patchin, (2009). *Preventing Cyberbullying: Top Ten Tips for Educators*. http://www.nyasp.biz/conf_2013_files/Kelly_Top_Ten_Tips_Educators_Cyberbullying_Prevention.pdf. Data dostępu 28.12.2013.

[2] S. Hinduja, J. W. Patchin, (2009). *Preventing Cyberbullying: Top Ten Tips for Educators*. http://www.nyasp.biz/conf_2013_files/Kelly_Top_Ten_Tips_Educators_Cyberbullying_Prevention.pdf, Data dostępu 28.12.2013.

[3] T. Beran, Q. Li, *The Relationship Between Cyberbullying and School Bullying*. “The Journal of Student Wellbeing”, 1(2)/2008, s. 16–33.

Hipoteza o bliskoznaczności terminu mobbing i cyberbullying zdaje się być potwierdzona przez dane przedstawione przez niektórych naukowców[4]. Wskazują oni, że istotnie 44% osób pada ofiarą zarówno agresji online, jak również realnej. Natomiast zarówno T. Beran i Q.Li, jak również R. M. Kowalski i S.P. Limber dowiedli, że nawet 60% osób było ofiarami w życiu realnym i wirtualnym – zatem pozostaje 40% osób, które nie miały styczności z tego typu atakami w rzeczywistości. Niemieckie badanie zdaje się potwierdzać informację, że ponad 80% cyberprzestępców dopuszcza się mobbingu na swoich kolegach szkolnych również w rzeczywistości, mimo iż w większości przypadków wydaje się, że cyberbullying stanowi jedynie część technik wykorzystywanych przez osoby dopuszczające się tradycyjnej formy mobbingu[5]. Również najnowsze badania wskazują istotny związek pomiędzy tymi dwoma zjawiskami[6].

6 DEFINICJA

Literatura przedmiotu zawiera liczne definicje cyberprzemocy[7]. Jednak według R. M. Kowalskiego i S. P. Limbera wiele osób zajmujących się tą tematyką **postrzega cyberbullying jako szczególną formę mobbingu, odbywającą się za pomocą mediów i urządzeń służących komunikacji, jak telefony komórkowe, e-mail, Internet (np. portale społecznościowe, strony internetowe, chat roomy i blogi)**. Cyberprzestępcy grożą, zastraszają, oczerniają, upokarzają i obrażają swoje ofiary na odległość. Używają przy tym zdjęć, filmów, e-maili, wiadomości i komentarzy.[8]
Do najczęściej cytowanych definicji cyberprzemocy należą[9]:

> Agresywny, zamierzony akt dokonany przez grupę lub jednostkę przy użyciu elektronicznych form komunikacji, w sposób powtarzalny, przed którym ofiara nie może się łatwo bronić[10]

> Cyberbullying ma miejsce, jeśli ktoś powtarzalnie naśmiewa się z innej osoby w sieci lub nęka ją poprzez e-maile lub wiadomości tekstowe lub gdy zamieszcza coś w Internecie o osobie, której nie lubi[11]

> Cyberbullying polega na użyciu technologii informacyjnych i komunikacyjnych w celu wsparcia celowego, powtarzalnego i wrogiego zachowania wobec osoby lub grupy w celu ich skrzywdzenia[12]

7 SZCZEGÓLNE CECHY CYBERBULLINGU ZNACZENIE DLA ZAPOBIEGANIA

Mimo iż mobbing i cyberbullying w dużej mierze pokrywają się w sensie empirycznym i konceptualnym, wyodrębniono

[4] Por. Ybarra & Mitchell, 2004; Beran & Li, 2005; Kowalski & Limber, 2008; Del Rey i in., 2012.

[5] Por. J. Riebel, R. S. Jaeger, & U. C. Fischer, *Cyberbullying in Germany–an Exploration of Prevalence, Overlapping with Real Life Bullying and Coping Strategies*, „Psychology Science Quarterly", 51(3)/2009, s. 298–314.

[6] Por. Perren i in., 2010; Sourander i in., 2010.

[7] Por. artykuł *Cyberprzemoc* i przce: Smith i in. 2002; Hinduja & Patchin 2006, 2007, 2008; Ybarra i in. 2006; Ybarra & Mitchell, 2007; Dooley i in., 2009; Steffgen i in. 2009; Lenhart, 2010; Ortega-Ruiz & Nunez, 2012; Heirman & Walrave, 2012; Wachs i in., 2012; Palladino i in., 2012; Paul i in., 2012; Vandebosch i in. 2012; Franco i in. 2012.

[8] R. M., Kowalski, S. P. Limber, *Electronic Bullying Among Middle School Students*, „Journal of Adolescent Health", 41/2007, s. 22–30.

[9] Por. Robert S. Tokunaga, *Konceptualne definicje cyberbullyingu w literaturze*, 2010, s. 278.

[10] P. K. Smith, J. Mahdavi, M. Carvalho, S. Fisher, s.Russell, N. Tippett., *Cyberbullying: its nature and impact in secondary school pupils*, „J Child Psychol Psychiatry", 49 (4)/2008, s. 376.

[11] Por. S. Hinduja, J. W. Patchin, *Cyberbullying: Neither an epidemic nor a rarity*. „European Journal of Developmental Psychology", 9, 539–543, doi:10.1080/17405629.(2012).706448. s. 540.

[12] Por. Besley, 2013.

OPIS ZJAWISKA

swoisty zestaw cech właściwych jedynie cyberprzemocy[13]. Sprawcy tej formy przemocy są w stanie dotrzeć do szczególnie szerokiej rzeszy odbiorców w tej samej grupie wiekowej, w przeciwieństwie do tradycyjnej formy mobbingu, w której publiczność jest zwykle ograniczona. W porównaniu z większością tradycyjnych form nękania, osoba dopuszczająca się cyberbullyingu może być mniej świadoma lub zupełnie nieświadoma konsekwencji swoich czynów.

8 Naszym zdaniem **dwie cechy tej formy przemocy są przyczynami wielu teoretycznych i praktycznych problemów. Pierwszą z nich jest brak całkowitej kontroli, co wiąże się z rodzajem stosowanych technologii**. Dla przykładu, gdy krzywdząca cyfrowa treść (sms, tekst, zdjęcie lub film) zostanie wysłana lub zamieszczona w Internecie, może być pobierana, przesyłana i rozpowszechniana przez każdego, w rezultacie trudno zatrzymać obieg informacji. Ponadto ofiara może doznać tego samego aktu agresji wielokrotnie poprzez wielokrotny kontakt z tą samą toksyczną cyfrową treścią. Pamięć Internetu jest poza zasięgiem zarówno sprawcy, jak i ofiary, a cyberprzestępcy wykorzystują specyficzne właściwości komunikacji w sieci (anonimowość, asynchroniczność oraz dostępność) w celu dręczenia ofiary[14].

9 **Druga cecha wiąże się z pojęciem asymetrii władzy, które może się odnosić do różnych sfer dominacji i uległości**[15]. Właściwie można założyć, że cyberprzestępcy posiadają szeroką wiedzę na temat technologii, dlatego czerpią korzyści z anonimowości. Jednak może być również odwrotnie, możliwa jest sytuacja, w której stalker jest gorzej obeznany z technologią niż jego ofiara, ale używa jej jedynie jako uzupełnienie agresji mającej miejsce w świecie rzeczywistym lub w celu dokumentowania jej. Jednocześnie dowiedziono, że dzięki swej naturze komunikacja elektroniczna może stanowić dla ofiary tradycyjnego mobbingu okazję do odwetu w sieci lub zaatakowania swojego oprawcy ze świata rzeczywistego[16]. Ankieta internetowa przeprowadzona wśród 473 uczniów badała rolę zemsty i odwetu jako motywu skłaniającego do stosowania cyberprzemocy. Zgromadzone dane dowodzą, że 149 respondentów zostało zidentyfikowanych jako ofiary tradycyjnego mobbingu, które faktycznie mszczą się na swoich oprawcach, czyniąc z nich swoje cyberofiary[17].

10 W naszej opinii cyberprzemoc jest niezwykle skomplikowanym problemem. Zwykle przybiera dwie różne formy w zależności od zastosowanej technologii komunikacji. Nękanie online może stanowić prosty, lecz naprawdę poważny rodzaj uzupełnienia mobbingu: stary problem wyrażony na nowo. Ofiary znają swoich prześladowców, natomiast dynamika występująca pomiędzy obiema stronami jest dokładnie taka sama, jak w świecie rzeczywistym. Jednak istnieje inny aspekt, dalece trudniejszy do zbadania ze względu na naturę wirtualnej relacji oraz rolę percepcji w wypadku relacji tego typu. Ten rodzaj mobbingu jest podstępny i niebezpieczny, gdyż zasadza się na sferze intymności oraz tego, jak młodzi ludzie postrzegają siebie samych. Ponadto

[13] Por. Dooley i in., 2009; Smith i in., 2008.

[14] P. M. Valkenburg, J. Peter, *Online Communication among Adolescents: An Integrated Model of its Attraction, Opportunities and Risks*. „Journal of Adolescent Health", 48(2)/2011, s.121–127.

[15] D. M. Law, J. D. Shapka, S. Hymel, B. F. Olson, T. Waterhouse, *The Changing Face of Bullying: An Empirical Comparison between Traditional and Internet Bullying and Victimization*. „Computers in Human Behavior", 28(1)/2012, s. 226–232.

[16] R. M. Kowalski, S. P. Limber, P. W. Agatston, *Cyber Bullying*, Malden 2008, MA: Blackwell.

[17] A. König, M.Gollwitzer, M., G. Steffgen, G., *Cyberbullying as an act of revenge?*, „Australian Journal of Guidance and Counselling", 20(02)/2010, s. 210–224.

11 młodzi ludzie od najmłodszych lat obcują z technologią, dlatego używają technologii cyfrowej jako głównego środka komunikacji między sobą. Jednak pomiędzy tymi różnymi rodzajami cyberbullyingu istnieje wiele form zależnych od kontekstu i osobowości uczestniczących w nim osób (sprawcy, ofiary, osoby postronne, pedagodzy, rodzice), jak również od czynników kulturowych i historycznego dziedzictwa, które również mogą wpływać na cyberprzemoc lub jej postrzeganie:

Co istotne, podczas porównywania badań należy pamiętać o kulturowych podobieństwach i różnicach zarówno w przypadku upowszechnienia tematu cyberprzemocy oraz samego zjawiska w konkretnej kulturze[18].

Żaden z powyższych aspektów omawianego problemu nie może zostać pominięty w procesie rozwijania skutecznego programu edukacyjnego wymierzonego w cyberprzestępczość.

12 **PRZECIWDZIAŁANIE**

Zdobywanie wiedzy w określonym kontekście

Pierwszą wskazówką wymienianą przez S. Hinduję i J. W. Patchina jest zdobywanie wiedzy o zakresie problemu w ramach zajęć szkolnych. Radzą zebranie danych za pomocą ankiet i/lub wywiadów przeprowadzanych z uczniami w celu zorientowania się, jak przedstawia się sytuacja w szkole. Zdobywanie wiedzy jest niezbędnym warunkiem wstępnym do wprowadzenia środków zapobiegawczych. Głównym celem ankiet powinny być informacje, na podstawie których można edukować uczniów i nauczycieli na temat bezpieczeństwa w sieci oraz możliwości korzystania z Internetu w sposób kreatywny i efektywny.

13 Co więcej, naszym zdaniem, zrozumienie kontekstu szkolnego nie powinno się ograniczać do zbierania danych na temat mobbingu w życiu i w Internecie, ale powinno również dotyczyć zbierania danych na temat świadomości grona pedagogicznego w kwestii istnienia tego typu zdarzeń w ich szkole oraz ich kompetencji w rozwiązywaniu omawianych problemów. Świadomość nauczycieli i pedagogów przyczyn mobbingu/cyberprzemocy może się różnić[19] i wymaga posiadania rozległej podstawowej wiedzy na temat agresji, tego, że wiele jej przejawów jest subtelnych, ukrytych i niewykrywalnych, ale jednocześnie mających przytłaczające konsekwencje. Łatwo zauważyć główny czynnik, ewidentną przemoc, ale istnieją również inne formy agresji relacyjnej mające charakter ukryty, jak wykluczenie i wyśmiewanie się[20] . Brak wiedzy na ten temat może sprawić, że nauczyciele nie będą w stanie właściwie ocenić agresji relacyjnej i nie będą interweniować, jeśli wystąpią tego typu problemy. Z tego względu ocena zdolności szkolnego grona pedagogicznego do rozpoznania oznak mobbingu jest jednym z zasadniczych elementów w walce z tego typu problemami[21].

14 **ZBIERANIE INFORMACJI**

Istotne są również strategie i techniki zbierania danych o zachowaniach uczniów oraz świadomości i umiejętności nauczycieli ra-

[18] Por. R. M.. Kowalski, S.Limber, P. W. Agston, *Cyberbullying: Bullying in the Digital Age*, 2th edition, Malden 2012, MA, Wiley—Blackwell.

[19] B. Kochenderfer-Ladd, M. E. Pelletier, Teachers' Views and Beliefs about Bullying: Influences on Classroom Management Strategies and Students' Coping with Peer Victimization. "Journal of School Psychology", 46(4)/2008, s. 431–453.

[20] T. Ryan, M. Kariuki, H. Yilmaz, Z. A. Gazi, E. Ongun, D. Atlas, J. A. Burston, *Comparative Analysis of Cyberbullying Perceptions of Preservice Educators: Canada and Turkey*, „TOJET" 10(3)/2011.

[21] W. M. Craig, K. Henderson, J. G. Murphy, *Prospective Teachers' Attitudes toward Bullying and Victimization*, „School Psychology International", 21(1)/2000, s. 5–21.

dzenia sobie z wirtualną i rzeczywistą formą przemocy.

15 Najbardziej odpowiednią i najczęściej stosowaną formą zbierania danych jest ankieta. W przypadku tego typu przemocy ankieta musi być starannie przygotowana i musi dostarczać wstępnych zadań. Istotne jest, aby grono pedagogiczne brało udział w przygotowaniu i dystrybucji kwestionariuszy wraz z dokładnymi instrukcjami oraz wskazówkami. Należy poinformować uczniów, że wypełnienie ankiety jest dobrowolne, ale szkoła doceni jej wypełnienie. Ponadto należy ich zapewnić, że wszystko co napiszą będzie w najwyższym stopniu poufne, a odpowiedzi nie zostaną ujawnione przed nauczycielami, dyrektorem, ani innymi uczniami. Sprawą najwyższej wagi jest zaznaczenie, że odpowiedzi powinny być prawdziwe, z uzasadnieniem tego dobrem samych uczniów i chęcią ich ochrony. Uczniowie powinni być zachęcani do wypełnienia ankiety, dzielenia się swoimi uwagami oraz zaangażowania.

16 Istnieje wiele rzetelnych wzorów do zbierania tego typu informacji w szkole oraz oceny świadomości i umiejętności radzenia sobie z nią nauczycieli.

17 Zwykle ankiety skupiają się na życiu uczniów w szkole i poza nią w ciągu ostatnich 2–3 miesięcy. Zachęca się ich do odpowiedzi na pytania z perspektywy ostatnich paru miesięcy, a nie na podstawie obecnego stanu. Często dla celów naukowych tego typu kwestionariusze zawierają definicję lub wyjaśnienie mobbingu:

Mówimy o mobbingu, jeśli jeden uczeń wobec innego ucznia lub innych uczniów:
- mówi podłe i krzywdzące rzeczy, wyśmiewa lub obraża go;
- zupełnie ignoruje i wyklucza go/ją z grupy ich przyjaciół;
- bije, kopie, popycha lub zamyka go/ją w klasie;
- kłamie lub rozpowiada plotki na jej/jego temat lub rozsyła krzywdzące informacje i stara się poróżnić jego/ją z innymi;
- i inne przykre tego typu rzeczy[22].

Taka definicja mobbingu jest ogólnie przyjęta przez naukowców i jest zgodna z definicją D. Olweusa[23].

18 Dlatego właściwe ankiety zawierają definicję cyberprzemocy. Ale przecież definicje cyberbullyingu mogą się różnić między sobą, tak jak naukowcy mają różne opinie na temat tego zjawiska. Poniżej znajduje się przykład takiej definicji zaczerpniętej z popularnego badania, którego celem było poznanie form, świadomości, efektów oraz zależności między wiekiem i płcią w przypadku cyberprzemocy.

Dziś chcielibyśmy przyjrzeć się bliżej szczególnej formie mobbingu: cyberprzemocy, która opiera się na stosowaniu przemocy poprzez:
- wiadomości SMS,
- zdjęcia, filmy,
- telefony (pogróżki, milczące etc.),
- e-maile,
- chat roomy,
- komunikatory,
- strony internetowe[24].

19 Nawet we wstępie do kwestionariusza zachęca się uczniów do pamiętania o tym, że mówimy o mobbingu, jeśli wyżej wymienione elementy powta-

[22] P. K. Smith, J. Mahdavi, M. Carvalho, N. Tippett, *An Investigation into Cyberbullying, its Forms, Awareness and Impact, and the Relationship between Age and Gender in Cyberbullying*, „Research Brief" No. RBX03-06/2006, London: DfES

[23] D. Olweus, *Bullying at School: What we Know and What We Can Do*, 1993, Wiley-Blackwell.

[24] P. K. Smith, J. Mahdavi, M. Carvalho, N. Tippett, *An Investigation into Cyberbullying, its Forms, Awareness and Impact, and the Relationship between Age and Gender in Cyberbullying*, „Research Brief" No. RBX03-06/2006, London: DfES.

rzają się, a ofierze trudno jest się przed nimi bronić. Istotne jest, aby uczniowie zrozumieli, że mówimy o mobbingu, jeśli jednemu uczniowi inny ciągle dokucza, chcąc go zranić, ale nie jeśli ktoś się z nim drażni w żartobliwy i niewinny sposób, czy też gdy dwóch uczniów o podobnej sile pokłóci się lub pobije.

20 Pragniemy zaznaczyć, że definicja mobbingu i cyberprzemocy jest warunkiem wstępnym analizy naukowej. Mimo to nie jest niezbędnym rozpoczęcie dyskusji naukowej na ten temat, gdy istnieje potrzeba zdobycia informacji przed wprowadzeniem planowanego programu przeciwko cyberprzemocy. Niezbędne są bardziej ogólne dane na temat nawyków uczniów oraz kontekstu rodzinnego, tj. na temat korzystania z Internetu i telefonów komórkowych, czasu spędzanego na serfowaniu w Internecie, występowaniu przemocy w rodzinie, wrogości w klasie, umiejętności korzystania z nowych technologii, świadomości cyberzagrożeń, wagi posiadania profilu na portalu społecznościowym, wagi wirtualnych relacji etc.

21 Zwalczanie tego zjawiska jest niemożliwe bez znajomości kontekstu, w którym odbywa się cyberprzemoc. Internet stanowi przepastny świat, niezbadany, pełen dobra i zła, podlegający nieustannym przemianom. Można zauważyć, że nawet jeśli młodzi ludzie spędzają czas razem, w relacjach osobistych, jednocześnie korzystają z telefonów komórkowych i smartfonów, prowadzą dialog zarówno w rzeczywistości, jak i w wirtualnym świecie, z rzeczywistymi przyjaciółmi i jednocześnie z przyjaciółmi, których znają jedynie z Internetu. Należy starać się zrozumieć świat młodych ludzi oraz obecność wirtualnej rzeczywistości[25] w ich życiu, ich obawy oraz wagę reputacji w sieci. Ponadto należy zauważyć, że agresja może brać swój początek w szkole, a dopiero później może się rozszerzyć na dom i społeczność za pomocą technologii, ale oczywiście możliwa jest odwrotna sytuacja, w której przemoc oparta na komputerze i telefonie komórkowym przeradza się w przemoc fizyczną. Najbardziej zagubione są osoby będące jednocześnie napastnikami i ofiarami, co oznacza, że potrzebne są nowe strategie prewencyjne i interwencyjne. Naukowcy z dziedziny psychologii i psychiatrii argumentują, że cyberprzemoc oraz cyberkrzywda wiążą się z problemami psychiatrycznymi i psychosomatycznymi, a osoby cierpiące najbardziej zaliczają się jednocześnie do obydwu grup[26].
Grono pedagogiczne, chcąc nie chcąc, powinno brać to pod uwagę.

22 Alarmujący śmiertelny przypadek, który wydarzył się we Włoszech 26 grudnia 2013 roku dowodzi, że bliskie powiązanie między światem rzeczywistym i wirtualnym jest nie tylko domeną ludzi młodych. Zakładając profil na Facebooku, 42-letnia kobieta sprowokowała wybuch zazdrości swojego partnera, który w efekcie brutalnie ją zamordował.[27].

23 **ZAJĘCIA EDUKACYJNE**

S. Hinduja i J. W.Patchin zalecają przede wszystkim uświadamianie uczniów, że wszelkie formy mobbingu są nieakcepto-

[25] W 2013 roku we Włoszech 67-letni mężczyzna zamordował dwie 15-letnie dziewczynki, o czym opowiedział nieznajomemu chłopcu przypadkowo napotkanemu w pociągu: „To było jak w grze GTA. Czuliśmy się jak bohater gry".

http://www.repubblica.it/cronaca/2013/04/10/news/delitto_udine_sequestrate_pagine_fb_delle_ragazze-56337211/; data dostępu 1.1.2014.

[26] A. Sourander, A. Brunstein Klomek, M. Ikonen, J. Lindroos, T. Luntamo, M. Koskelainen, H. Helenius, *Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study*, "Archives of General Psychiatry", 67(7)/2010, s. 720.

[27] http://bari.repubblica.it/cronaca/2013/12/28/news/cadavere_di_donna_nelle_campagne_l_amante_confessa_sono_stato_io=74647487-/?ref-HREC1-8. data dostępu 28.12.2013.

DOBRE PRAKTYKI

walne, oraz że cyberprzemoc jest karana. Zachęcają pedagogów do rozmawiania z uczniami na temat podstawowych sposobów zapobiegania jej. Uczniowie muszą mieć świadomość, że nawet jeśli jakieś zachowanie ma miejsce daleko od szkoły może być poddane karze, jeśli ma wpływ na atmosferę w szkole. Wskazówka ta łączy się z kolejną, którą włączyliśmy do grupy zajęć ze wsparcia technicznego. Autorzy sugerują stworzenie „formalnej umowy" w zależności od definicji cyberprzemocy przyjętej przez szkołę lub organizację zajęć z etyki, które identyfikują tego typu zachowanie jako nieodpowiednie. Pod wpływem tych zaleceń wiele szkół w Stanach Zjednoczonych przyjęło postawę *zero tolerancji* dla cyberprzemocy.

Zgadzamy się z podejściem, że uświadamianie uczniów na temat cyberbullyingu stanowi podstawę w jego zwalczaniu. Szkoła musi otwarcie przyznać, że tego typu zachowanie nie będzie tolerowane i spotka się z określonymi konsekwencjami. Sugerujemy wyznaczenie reguł postępowania w takich przypadkach, które powinny być systematycznie uaktualniane przez grono pedagogiczne w porozumieniu z reprezentantami rodziców i uczniów. Określenie zasad „zero cyberprzemocy" i ich aktualizacja jest okazją do zilustrowania konsekwencji związanych z tego typu zachowaniem, także tych prawnych.

24 Mimo wszystko nauczyciele i pedagodzy powinni pamiętać o tym, że aktualne regulacje prawne mają mały wpływ na zwalczanie i karanie cyberprzemocy. Regulaminy portali społecznościowych takich jak MySpace czy Facebook zezwalają każdemu powyżej czternastego roku życia na przyłączanie się do nich. W trakcie rejestracji nowi członkowie muszą podać informacje osobiste, wybrać hasło oraz zapoznać się z regulaminem i polityką prywatności, po czym wyrazić na nie zgodę poprzez wybranie odpowiedniego pola lub w inny sposób. Właśnie do polityki prywatności odnosi się przypadek Lori Drew[28]. Sprawa Drew była szeroko komentowana w międzynarodowych mediach, w wyniku czego Drew stała się swoistą ikoną cyberprzemocy. Lori Drew pomogła swojej córce stworzyć profil na portalu MySpace.com w celu dotarcia do jej szkolnej koleżanki i sąsiadki, trzynastoletniej Megan Meyer. Profil rzekomo należał do atrakcyjnego szesnastolatka Josha Evansa.

25 L. Drew twierdzi, że fałszywy profil miał na celu uzyskanie poufnych informacji na temat tego, co Megan Meier mówi o jej córce. Miesiąc później Meier otrzymała wiadomość na komunikatorze od rzekomego Evansa, w której twierdził on, że już jej nie lubi i że świat byłby lepszy bez niej. Tego samego dnia Meier popełniła samobójstwo. Lori Drew została oskarżona o złamanie prawa federalnego, ponieważ zorganizowała nagonkę w MySpace i tym samym doprowadziła do samobójstwa dziecko sąsiadów. Zdaniem władz Drew tworząc profil „Josha Evansa" pogwałciła politykę prywatności portalu MySpace.com. Pierwszy werdykt skazujący został oddalony przez sędziego federalnego rozstrzygającego w tej sprawie, który zgodził się z argumentami obrony. Na podstawie statutu polityka prywatności nie zarządza autoryzacją: portal MySpace dał dostęp do swoich komputerów poprzez stworzenie profilu Josha Evansa i pozwalając grupie na wysyłanie i otrzymywanie wiadomości [29]. W trakcie procesu wiceprezes obsługi klienta w MySpace przyznał, że sama liczba 400 milionów kont na MySpace sprawia, iż niemożliwe jest zidentyfiko-

[28] http://bari.repubblica.it/cronaca/2013/12/28/news/cadavere_di_donna_nelle_campagne_l_amante_confessa_sono_stato_io=74647487-/?ref-HREC1-8. data dostępu 28.12.2013.

[29] O. S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*. „Minn. L. Rev.", 94/2009, s. 15–61.

wanie tych, które pogwałciły regulamin prywatności.

26 Jak zauważyła J. P. Meredith:

> Właściwie kary za pogwałcenie polityki prywatności MySpace należą do rzadkości. Bardziej prawdopodobne, że portal po prostu ostrzeże użytkowników, iż kontynuowanie przez nich działań może spowodować powiadomienie organów lub usunięcie kwestionowanego profilu z portalu[30]

27 Inne wskazówki S. Hinduji i J. W. Patchina dotyczące programów edukacyjnych w celu zapobiegania cyberprzemocy odnoszą się do innego istotnego aspektu: udziału wszystkich zaangażowanych stron w rozwijaniu takiego programu. Radzą oni stosowanie grup wsparcia rówieśników do promowania pozytywnych interakcji w sieci np. organizowanie lekcji, podczas których starsi uczniowie uczą i dzielą się doświadczeniem z młodszymi. Kolejna wskazówka odnosi się do kultywowania pozytywnej atmosfery. Argumentują, iż niezbędne jest, aby tworzyć i podtrzymywać pozytywną atmosferę polegającą na szacunku i uczciwości, której pogwałcenie spotka się z nieformalnymi lub formalnymi sankcjami. Radzą również wprowadzenie specjalnych zajęć lub sesji informacyjnych na temat tego zjawiska typu kółka i panele dyskusyjne w celu podniesienia stopnia świadomości wśród młodych ludzi.

28 Na sam koniec podkreślają również wagę dyskusji ze specjalistami, rozsyłania informacji do rodziców oraz organizacji wydarzeń edukacyjnych z udziałem rodziców, krewnych i innych osób dorosłych. Specjaliści i edukatorzy powinni podkreślać korzyści płynące ze stosowania nowych technologii, które nie tylko mogą wspomagać proces uczenia, ale również pozytywnie wpływać na relacje społeczne. Co więcej, portale społecznościowe oraz wirtualne relacje są istotne z punktu widzenia osób mających trudności z ich nawiązywaniem w rzeczywistości, ponieważ anonimowość w sieci może obniżyć zahamowania występujące podczas nawiązywania kontaktów. Za pomocą portali społecznościowych łatwiej dotrzeć do większej liczby odbiorców i opowiedzieć, co dzieje się w naszym życiu i jak się czujemy[31]. Mogą one również ułatwić nawiązywanie kontaktów z osobami, które mają szczególne zainteresowania lub dzielą aspekty tożsamości rzadko spotykane w świecie rzeczywistym.

29 REGULACJE PRAWNE

Należałoby do powyższych wskazówek dodać za J. P. Meredith sugestię dotyczącą kryminalizacji cyberbullyingu. Zgadzamy się z jej zastrzeżeniami, że należy w ten sposób jedynie kwalifikować czyny niewątpliwie kryminalne. Jak zauważa J. P. Meredith pod tym względem nie rozróżnia się cyberprzestępczych aktów dokonywanych przez osoby dorosłe i nieletnie oraz zwraca ona uwagę na trudność znalezienia granicy między nieprzyjemną wypowiedzią a groźbą. Przytacza przypadki, gdy wymiar sprawiedliwości określał cyberprzestępstwa mianem wykroczeń młodocianych i wymagał od szkół, żeby wprowadziły politykę zapobiegającą takim występkom. Jest to swego rodzaju przeniesienie odpowiedzialności i obciążanie szkół dodatkowymi obowiązkami[32].

---

[30] J. P. Meredith, *Combating Cyberbullying: Emphasizing Education over Criminalization*, Fed. Comm. LJ, 63/2010, s. 311.

[31] W. Heirman, M. Walrave, *Assessing Concerns and Issues about the Mediation of Technology in Cyberbullying*. „Cyberpsychology: Journal of Psychosocial Research on Cyberspace", 2(2)/2008, article 1. http://cyberpsychology.eu/view.php?cisloclanku=2008111401&article=1.

[32] J. P. Meredith, *Combating Cyberbullying: Emphasizing Education over Criminalization*, Fed. Comm. LJ, 63/2010, s. 328

30 Pod tym względem należy wkładać wysiłek w celu zwiększenia edukacji na temat bezpiecznego korzystania z Internetu. Pedagodzy powinni być wyposażeni w odpowiednie narzędzia w celu instruowania młodzieży i rodziców jak mądrze korzystać z technologii. Istotne jest dostarczanie informacji, która zwiększy świadomość o zagrożeniach związanych z cyberprzestrzenią. Przede wszystkim powinno się uczyć dzieci jak korzystać z pozytywnych aspektów Internetu, nie padając przy tym ofiarą tych negatywnych.

31 Próby zmierzenia się z tym problemem na drodze regulacji prawnych powinny być kontynuowane, zgodnie ze słowami Lindy Sanchez przytoczonymi przez J. P. Meredith[33]:

> Życzyłabym sobie, żeby przepisy prawne odróżniały irytującą komunikację, oburzoną opinię na blogu politycznym, wiadomość napisaną pod wpływem emocji do byłego chłopaka, które są i powinny pozostać zgodne z prawem, od poważnych, powtarzających się i wrogich wiadomości z zamiarem wyrządzenia krzywdy.

32 L. T. Sanchez odnosi się do wysiłków legislacyjnych, ale jej celem stało się również uwzględnienie zapobiegania cyberprzestępczości przy użyciu nowego, lepszego oprogramowania. Producenci oprogramowania powinni dostarczać rozwiązań dla bezpiecznego korzystania z Internetu. Przy tym nie powinno się zapominać o roli mediów.

ROLA MEDIÓW

Czy cyberbullying jest wyolbrzymionym ryzykiem?

33 W Cassidy, C. Faucher i M. Jackson stwierdzają w artykule podsumowującym aktualny stan badań nad cyberprzemocą, że jest ona obok tradycyjnego mobbingu coraz częściej wymieniana jako wybuchowe zjawisko, z którym praktycy i naukowcy muszą się borykać[34]. Wielu z nich przyznaje, że cyberbullying przybiera na sile[35]. Międzynarodowe badania ilościowe wskazują na wzrost skali problemu wśród uczniów, jednak należy przyznać, że poszczególne analizy znacznie się różnią między sobą i w zależności od kultury[36]. Można to częściowo tłumaczyć nieporównywalnością definicji i metod dotychczas stosowanych podczas ich przeprowadzania.

34 Z tego względu trudno porównywać dane dotyczące częstotliwości występowania problemu. W kanadyjskim badaniu Q. Li odkrywa, że 25% uczniów nigdy nie padło ofiarą cyberbullyingu, natomiast 17% dopuszczało się go wobec innych. Wcześniej, w wyniku ankiety przeprowadzonej w USA, M. Ybarra i K. Mitchell (2004) podważyli pogląd o dychotomiczności cyberprzestępców i ofiar, i porównali wyniki w czterech grupach: 4% było celem ataków online, 12% było agresorami online, 3% stało się zarówno agresorami, jak i ofiarami agresji w sieci, podczas gdy 81% nie brało udziału w cyberbullyingu. Niektórzy naukowcy[37] doszukali się wzrostu liczebności tych grup w ciągu ostatnich pięciu lat.

---

[33] W 2009 roku Linda T. Sanchez, członkini Kongresu Kalifornii, wprowadziła 51 Akt Prewencji Cyberprzemocy im. Megan Meier w celu kryminalizacji każdej komunikacji z zamiarem wymuszenia, zastraszenia, nękania za pomocą środków elektronicznych w celu wzmocnienia okrutnego, powtarzalnego zachowania. Akt ten nie został zatwierdzony przez Kongres w 2009 roku i od tego czasu nie padły nowe propozycje regulacji prawnych w tym zakresie. Por. J. P. Meredith, *Combating Cyberbullying: Emphasizing Education over Criminalization*, Fed. Comm. LJ, 63/2010, s.330.

[34] Cassidy i in., 2013

[35] Por. Ybarra & Mitchell, 2004; Campbell, 2005; Cowie & Jennifer, 2008; Smith & Slonje, 2010; Bulut & Gündüz, 2012; Demaray i in., 2012; Hatzichristou i in., 2012; Kowalski i in., 2012a; Kowalski i in., 2012b; Soto i in., 2012; von Mare´es & Petermann, 2012.

[36] Por. D. Ferdon & Feldman, 2007; Smith i in., 2008..

[37] Por. Cassidy i in., 2011; Kowalski i in., 2012; Rivers & Noret, 2010

35 Istnieją również tacy naukowcy, którzy nie zgadzają się z teorią, że mamy do czynienia z lawinowym przyrostem występowania tego zjawiska. D. Olweus[38], Q.Li i in.[39] , oraz S. Hinduja i J. W. Patchin [40] twierdzą, że zjawisko to nie przybrało na sile od czasu, kiedy po raz pierwszy zaistniało, w połowie poprzedniej dekady. Jednak faktem jest, że – zwłaszcza w ciągu ostatnich lat – cyberprzemoc zyskuje coraz więcej uwagi medialnej. To media stymulują świadomość władz oraz publicznej uwagi[41].

36 Ostatnio gazety i programy telewizyjne zaczynają zajmować się tym problemem, zwłaszcza ekstremalnymi przypadkami, np. śmiercią nastoletniej ofiary cyberbullyingu. Zazwyczaj doniesienia medialne skupiają się na rodzicach ofiary, którzy w żalu obarczają winą szkolnych kolegów, władze szkoły oraz rząd, gdyż – w ich opinii – nie zrobili oni nic w celu zwalczania zjawiska i aresztowania sprawców. Z drugiej strony szkolni koledzy oraz władze szkoły zawsze twierdzą, że nie dostrzegli niepokojących sygnałów. Policja natomiast twierdzi, że każdego dnia w mediach społecznościowych zamieszczanych są liczne obraźliwe, niestosowne i obsceniczne komentarze, których nie jest w stanie przeanalizować w takiej ilości. Ponadto wiele z tych komentarzy nie jest na tyle poważnych, żeby uzasadniało ich zaangażowanie.

37 Powyższy akapit dowodzi, że dostawcy portali społecznościowych powinni stosować więcej środków zapobiegawczych, kontrolnych oraz filtrować zawartość stron. Bez wątpienia prasa i media interpretują zaniepokojenie cyberprzemocą, która przedstawiana jest jako alarmująco przybierające na sile zjawisko. Pod tym względem należy pamiętać, że media często wyolbrzymiają fakty, jak w poniższym przykładzie.

38 "Quando i social network uccidono: adolescenti vittime di cyberbullismo [Gdy sieci społecznościowe zabijają: nastoletnie ofiary cyberbullyingu]"[42] jest artykułem internetowym opublikowanym 3 czerwca 2013 przez popularną włoską gazetę „Repubblica". Został on ponownie opublikowany 12 sierpnia tego samego roku, gdy czternastoletni chłopiec podejrzewany o homoseksualizm popełnił samobójstwo. Jednak po paru dniach żarliwych artykułów i wzajemnego oskarżania się o homofobię, policja wykluczyła hipotezę, że samobójstwo miało podłoże cyberbullyingu. Nie powinno nikogo dziwić, że zaraz po incydencie środowiska gejowskie, obrońców praw człowieka i lewicowe żądały zaostrzenia prawa w celu przeciwdziałania homofobii i cyberbullyingowi. Jednak, jak udowodniliśmy, dostosowanie prawa nie jest proste, gdyż nie istnieje uniwersalna definicja cyberprzemocy.

39 Mimo to pytanie o rolę mediów w cyberbullyingu pozostaje otwarte. Czy wzrost zagrożeń związanych z cyberprzestrzenią pokrywa się z rzeczywistością, czy jest to jedynie projekcja ludzkich obaw?

---

[38] Por. D. Olweus, *Cyberbullying: An Overrated Phenomenon?* „European Journal of Developmental Psychology", 9, 520–538, doi:10.1080/17405629.(2012).682358. i D. Olweus,Comments on Cyberbullying Article: A Rejoinder, "European Journal of Developmental Psychology", 9, 559–568, doi:10.1080/17405629.(2012).705086.

[39] Por. Q. Li, D. Cross, & P. Smith, (Eds.), *Cyberbullying in the Global Playground: Research from International Perspectives*. West Sussex 2012, Wiley-Blackwell.

[40] Por. S. Hinduja, J. W. Patchin, *Cyberbullying: Neither an epidemic nor a rarity*. „European Journal of Developmental Psychology", 9, 539–543, doi:10.1080/17405629.(2012).706448.

[41] Por. Dooley, Pyzalski, & Cross, 2009; Patchin & Hinduja, 2011; Li i in., 2012.

[42] http://inchieste.repubblica.it/it/repubblica/rep-it/2013/06/03/news/quando_i_social_network_uccidono_gli_adolescenti_vittima_di_cyberbullismo-60257903/

W tym miejscu należy przyjrzeć się zastrzeżeniom D.Olweusa związanymi z cyberprzemocą.

40 ZASTRZEŻENIA D. OLWEUSA

D. Olweus był pionierem badań nad zapobieganiem mobbingowi oraz twórcą *Olweus Bullying Prevention Program* (ang. program zapobiegania mobbingowi D.Olweusa), zauważył, że cyberprzemoc była badana „w izolacji", to jest poza ogólnym kontekstem tradycyjnego mobbingu, przy czym często bez ogólnej przyjaznej uczniowi definicji tego, co się pod tym pojęciem rozumie. Według D. Olweusa, można mówić o mobbingu ucznia, jeśli inny uczeń lub inni uczniowie:

mówią oczerniające i krzywdzące rzeczy lub naśmiewają się z niego/niej lub przezywają jego/ją;

zupełnie ignorują lub wykluczają jego/ją z grupy przyjaciół lub celowo jego/ją pomijają;

biją, kopią, popychają, poszturchują lub zamykają jego/ją w klasie;

opowiadają kłamstwa lub nieprawdziwe informacje o nim/niej lub wysyłają oczerniające informacje, żeby inni przestali jego/ją lubić;

oraz inne tego typu krzywdzące rzeczy.

Dokładnie takie same cechy cyberbullyingu zostały wyżej wymienione w przeprowadzanej ankiecie przez P. K. Smitha i in[43].

D. Olweus podkreśla, że obraz stworzony przez media – oraz przez naukowców i autorów książek na ten temat – często przedstawia cyberprzemoc jako zjawisko, którego częstotliwość występowania nagle znacznie wzrosła w czasie, oraz że ta nowa forma mobbingu ma wielu nowych sprawców i ofiary. A dokładniej, D. Olweus argumentuje, że informacje w mediach dotyczące cyberprzemocy są często znacznie przesadzone oraz w dużej mierze nie mają naukowego uzasadnienia. Ponadto zaznacza, że tego typu stwierdzenia mogą mieć niekorzystne konsekwencje, dowodząc, że jego argumenty opierają się na analizie empirycznej kilku szeroko zakrojonych badań. Konkluduje, że prawdopodobnie efektywne środki zapobiegania i walki z cyberprzemocą, jakie poszczególne szkoły lub społeczności mogą podjąć, to inwestycja w czas i techniczne kompetencje, w celu wykrycia kilku przypadków przemocy, po czym nagłośnienie anonimowych wyników takiego dochodzenia wśród uczniów.

41 Naszym zdaniem zastrzeżenia jedynie potwierdzają fakt, że jest to zjawisko stosunkowo nowe, różnorodne i wieloaspektowe, a tym samym trudne do zdefiniowania. Jednak istnieją niepokojące dowody: nikt przy zdrowych zmysłach nie dałby broni dziecku, tymczasem nowe technologie mogą być o wiele bardziej zabójcze.

42 CYBERPRZEMOC I TECHNOLOGIA

Zwykle nauczyciele, pedagodzy i rodzice są znacznie mniej biegli w posługiwaniu się nowymi technologiami. Jest to poważny problem prowadzący do niewystarczającej superwizji w szkole i domu, znacznie ograniczający możliwości prewencji cyberbullyingu[44]. Ponadto, mimo iż młodsi pedagodzy wykazują się lepszą znajomością technologii i są zaniepokojeni zjawiskiem, nie są oni w stanie prze-

[43] P. K. Smith, J. Mahdavi, M. Carvalho, N. Tippett, *An Investigation into Cyberbullying, its Forms, Awareness and Impact, and the Relationship between Age and Gender in Cyberbullying*, „Research Brief" No. RBX03-06/2006, London: DfES

[44] C. Popovic, S. Djuric, V. Cvetkovic, *The Prevalence of Cyberbullying among Adolescents: A Case Study of Middle Schools in Serbia*, „School Psychology International", 32/2011, s. 412–424.

łożyć posiadanej wiedzy na politykę lub programy szkolne.

43 Ogólnie należy przyznać, że nauczyciele bardziej skupiają się na zjawisku mobbingu niż na cyberprzemocy. Główny problem stanowi tutaj konieczność zastosowana multidyscyplinarnego podejścia zarówno w tworzeniu polityki, jak i w treningu nauczycieli. W celu zniwelowania technologicznej asymetrii wśród grona pedagogicznego pomocne mogą być warsztaty lub specjalne szkolenia na ten temat[45]. Wiedza nauczycieli powinna być dodatkowo wzbogacona o elementy z dziedziny psychologii, pedagogiki oraz nauk socjalnych istotne w cyberprzemocy, jak np. rewizja tradycyjnych koncepcji samooceny, relacji z rówieśnikami, empatii, komunikacji, asymetrii władzy etc.

44 W ramach zajęć technicznych, należy przybliżyć pojęcie różnych form komunikacji używanych w cyberbullyingu. Niektórzy autorzy dokonują klasyfikacji form tej przemocy w zależności od stosowanych form komunikacji, tj w zależności, czy odbywa się ona za pomocą wiadomości sms, e-mail, komunikatorów etc[46].

45 R. Ortega i in[47]. zalecają podział na podstawie rodzaju aktywności, podobnie jak N. E. Willard (2006), która zdefiniowała osiem podkategorii cyberprzemocy. N. E. Willard sama przyznaje, że niektóre przez nią wymienione zjawiska powinny raczej nosić miano „społecznego okrucieństwa w sieci".

Zatem klasyczne formy cyberbullyingu to:

prześladowanie – może być definiowane jako powtarzające się wysyłanie obraźliwych wiadomości lub pogróżek innym osobom za pośrednictwem wiadomości e-mail, sms, komunikatora, w chat roomach.

oczernianie – to rozsyłanie plotek przy pomocy urządzeń komunikacji elektronicznej. W przeciwieństwie do plotkowania w życiu prawdziwym, informacja w Internecie może zostać rozesłana do tysięcy ludzi w ciągu sekund.

ujawnianie – ma miejsce, gdy ujawnione zostaną informacje prywatne, które ofiara wysłała komuś w zaufaniu – wówczas są one przesyłane dalej w celu skompromitowania ofiary.

wykluczenie jest odpowiednikiem wykluczenia w prawdziwym życiu i oznacza brak możliwości uczestniczenia w życiu społecznym. W kontekście wirtualnego świata może to oznaczać wykluczenie z gier, czatów, platform.

46 Technologia wpływa na tworzenie się nowych związków między ofiarą i prześladowcą:

- napastnik zna ofiarę i ofiara zna napastnika;
- napastnik nie zna ofiary i ofiara nie zna napastnika;
- napastnik zna ofiarę, ale ofiara nie zna napastnika.

47 W cyberprzestrzeni agresor może sobie obrać za cel nieznaną ofiarę o określonym profilu społecznościowym, ale znane są również przypadki, gdy anonimowy post na blogu prowokuje agresję wobec autora. W Internecie przypadki, które z czasem przeradzają się w agresję grupową nie należą do rzadkości: osoby uczestniczące w blogu zaczynają obrażać autora

[45] S. Paul, P. K. Smith, & H. H. Blumberg, *Addressing cyberbullying in school using the quality circle approach*, „Australian Journal of Guidance and Counselling", 20(02)/2010, s. 157–168.

[46] Por. Patchin & Hinduja, 2007; Smith i in., 2008; Limber, 2012.

[47] R. Ortega, J. A. Mora-Merchán, T. Jäger, *Acting Against School Bullying and Violence. The Role of Media, Local Authorities and the Internet*, Verlag Empirische Pädagogik: Landau. Available at: www.bullying-in-school. info/uploads/media/E-Book_English_01. pdf In the Painful lessons report, 2007.

DOBRE PRAKTYKI

postu, po czym poszukują jego/jej na sieci i tam grożą ofierze. Również poziom agresji na niektórych blogach politycznych jest szczególnie wysoki[48].

48 WSPARCIE TECHNICZNE

Wskazówki S. Hinduji i J. W. Patchina obejmują sugestie, które nazwaliśmy mianem wsparcia technicznego. Na przykład radzą zainstalowanie blokującego/filtrującego oprogramowania na sieć komputerów, by chronić przed wchodzeniem na określone strony i oprogramowanie. Te środki zapobiegawcze są niezbędne, jednak nie one decydują o powodzeniu przedsięwzięcia. Istnieje wiele komercyjnych i darmowych rodzajów oprogramowania do kontroli rodzicielskiej. Wiele z nich pozwala na kontrolowanie aktywności dzieci w Internecie, ograniczanie dostępu do niektórych stron oraz czasu spędzanego na serfowaniu po Internecie. Zawsze można jednak obejść tego typu zabezpieczenia, np. można używać innego komputera, gdzie filtry nie zostały skonfigurowane, a rozwój technologii nieustannie daje nowe możliwości dostępu do Internetu.

49 S. Hinduja i J. W. Patchin również podkreślają rolę konsultowania się ze szkolnym prawnikiem jeszcze zanim dojdzie do tego typu incydentów w celu dowiedzenia się, jakie kroki należy podjąć w różnych sytuacjach. Z pewnością znajomość litery prawa pomoże uporać się z przypadkami cyberprzemocy, jest ona szczególnie przydatna dla unikania sytuacji konfliktowych oraz długich i kosztownych procesów sądowych. W chwili obecnej jesteśmy sceptyczni wobec skuteczności prawa w tym zakresie. Debata na ten temat ukazuje różnice zdań między osobami, które się zetknęły z tym problemem i ekspertami. Delikatną kwestią pozostaje również ewentualna cenzura Internetu. Czy przepisy zapobiegające cyberprzemocy są formą cenzury? Doniesienia Edwarda Snowdena na temat globalnej inwigilacji prowadzonej przez Stany Zjednoczone podsyciły debatę na ten temat.

50 Kilka praktycznych pomysłów dotyczących omawianego problemu znalazło się w publikacji C. Zuchora-Walske[49]. Autorka jest zdania, że debata na temat cenzury Internetu powinna toczyć się nadal przy uwzględnieniu następujących pytań:

- Jak najlepiej chronić dzieci w Internecie?
- Czy prawo powinno chronić dzieci przez nieodpowiednimi treściami?
- Czy połączenie edukacji i zaangażowania rodziców jest lepszym sposobem?
- Czy można – czy to wskazane – oczekiwać uprzejmości w Internecie?
- Czy uprzejmość w Internecie pomaga zachować pokojowo nastawione społeczeństwo?
- Czy użytkownicy Internetu powinni kontynuować przywiązanie do tradycji?

51 Wreszcie, w zakresie technicznego wsparcia, zaznaczamy, że skuteczną techniczną pomoc w tym zakresie mogą stanowić *systemy uczące się*. Automatyczna analiza tekstu zawartości sieci społecznych stanowi nowy obszar badań, których wyniki zachęcają do ich kontynuowania[50].

[48] Por. blog Beppe Grillo we Włoszech. Beppe Grillo jest włoskim komikiem i politykiem. Zapoczątkował Ruch Pięciu Gwiazd zdobywając 109 miejsc w niższej izbie parlamentu, jak również 54 miejsca w senacie. Jego blog jest krytykowany ze względu na agresję słowną.

[49] C. Zuchora-Walske, *Internet Censorship: Protecting Citizens Or Trampling Freedom?*, Twenty-First Century Books 2010.

[50] Por. Dinakar i in., 2011; Garaigordobil i in., 2011; Reynolds i in., 2011; Kontostathis i in., 2013.

52 **STRATEGIE ZABEZPIECZAJĄCE**

Wiele wskazówek dotyczących zapobiegania cyberprzemocy dotyczy edukowania dzieci i ich rodziców na temat bezpieczeństwa w Internecie oraz wprowadzania narzędzi w celu ochrony przez tego typu incydentami, jak blokowanie agresywnego zachowania online lub tworzenie przycisków alarmowych dla ofiar na wypadek, gdy poczują się zagrożone. Prewencja poprzez edukację jest strategią, co do której w dużej mierze zgadzają się naukowcy i praktycy. Wszystkie zaangażowane strony podkreślają jednogłośnie, że kryminalizacja nie pomoże zwalczać tego zjawiska, gdyż jej negatywne następstwa znacznie przewyższają ewentualne pozytywne efekty. Edukacja na temat bezpieczeństwa w Internecie okazuje się skuteczna, zatem wyposażenie nauczycieli w teoretyczne i praktyczne narzędzia ma ogromną wagę. Programy wzajemnej edukacji oraz grupy wsparcia również uważa się za skuteczne. Opierają się one na założeniu, że uczniowie uczą się od siebie, przy czym mają na siebie duży wpływ. Sposób zachowania może się zmienić, gdy lubiani i poważani członkowie grupy będą liderami tej zmiany[51].

53 Istnieje kilka programów dostępnych dla nauczycieli, którzy chcieliby przyczynić się do zapobiegania cyberprzemocy[52]. Przykłady programów zwalczania tego zjawiska są dostępne również w Internecie, podczas gdy programy prewencyjne skupiające się na poziomie szkoły wydają się być bardziej skuteczne[53].

54 Wreszcie, należy przyznać że programy antymobbingowe mające na celu systematyczną walkę z cyberprzemocą, włączając udział uczniów i ich rodziców, mogą przynieść zadowalające efekty w zapobieganiu i zwalczaniu cyberbullyingu[54].

55 Mimo to może się okazać, że nieodzowne będą programy opracowane specjalnie pod kątem cyberprzemocy. Pod tym względem J. Riebel i in.[55] zidentyfikowali **cztery główne strategie zwalczania**:

- społeczna: pomoc rodziny, przyjaciół, nauczycieli, wsparcie grupy;
- agresywna: odwet, ataki fizyczne, ataki werbalne;
- bezsilna: poczucie beznadziei, reakcja pasywna, jak unikanie okazywania emocji;
- kognitywna: asertywna odpowiedź, podejście zdroworozsądkowe, analiza wydarzenia i zachowania agresora.

56 **PODSUMOWANIE WNIOSKI**

Ankieta przeprowadzona na grupie 23 420 dzieci i młodzieży europejskiej wykazała, że 5% respondentów było ofiarami cyberprzemocy częściej niż raz na tydzień, 4% raz do dwóch razy w miesiącu i 10% rzadziej; przy czym znaczna większość nie padła ofiarą cyberbullyingu[56]. Inne wyniki dała metaanaliza wskazująca na częste występowanie tego problemu we wszystkich krajach: około 40% i 55% uczniów miało styczność z tym zjawiskiem (w roli ofiar, agresorów, postron-

DOBRE PRAKTYKI

[51] Por. Naylor & Cowie 1999; Turner & Shepherd, 1999; Maticka-Tyndale & Barnett 2010.

[52] J. A. Snakenborg *Cyberbullying: Prevention and Intervention to Protect our Children and Youth*, „Preventing School Failure", 55(2)/2011, s. 88–95.

[53] M. A. Couvillon, V. Ilieva, *Recommended Practices: a Review of Schoolwide Preventative Programs and Strategies on Cyberbullying*, Preventing School Failure: Alternative Education for Children and Youth" 55(2)/2011, s. 96–101.

[54] Por. Perren i in., 2012; Mc Guckin i in. 2014

[55] J. Riebel, R. S. Jaeger, U. C. Fischer, Cyberbullying in Germany–an Exploration of Prevalence, Overlapping with Real Life Bullying and Coping Strategies, „Psychology Science Quarterly", 51(3)/2009, s. 298–314.

[56] S. Livingstone, L. Haddon, A. Görzig, K. Ólafsson, Risks and Safety on the Internet: the Perspective of European Children. Full Findings, LSE, London: EU Kids Online.

nych świadków)[57]. Te rozbieżności są po części wynikiem nowego zjawiska cyberprzemocy, po części wynikają z różnego podejścia badaczy:

Różne badania znacznie różnią się zakresem wieku badanych (10–18 lat), techniką lub oceną zastosowanych narzędzi, typami badanych rodzajów zachowania oraz przedziałem czasowym[58].

57 Mimo to istnieją dowody, które wymagają rozważenia: obecnie, ponad 65% osób w wieku 11–16 lat posiada profil na portalach społecznościowych, zaś ujawnianie informacji jest coraz bardziej powszechne wśród młodzieży. Ujawnianie informacji może wydawać się osobliwym zjawiskiem, w którym osoby w sposób nieograniczony i celowy rozsyłają poufne lub krzywdzące informacje (włączając informacje obciążające) do jak najszerszej grupy osób, najwyraźniej nie bacząc na konsekwencje. Powszechnie wiadomo, że młodzież ma skłonność do odnoszenia wrażenia, że jest nieustannie obserwowana lub że jest „na scenie" („wyimaginowana publiczność"), jednak ujawnianie informacji nie dotyczy jedynie nastolatków. Dodatkowo należy zauważyć znaczny wzrost stron plotkarskich, na których ocena plotek odbywa się na podstawie liczby kliknięć w daną plotkę (która przypuszczalnie została przeczytana).

58 Wymienione elementy skłaniają do stawiania nowych pytań odnośnie najlepszych strategii walki z cyberprzemocą. Działania zapobiegawcze powinny następować po dokładnej analizie zarówno ewolucji technologii, jak również pojawiających się nowych aspektów oraz negatywnych efektów cyberprzemocy. Badania empiryczne powinny być przeprowadzane częściej, podobnie jak inicjatywy wprowadzania środków zapobiegawczych, testowania ich skuteczności. Ale, nade wszystko, należy podkreślić rolę, jaką odgrywa w tym procesie szkoła, inaczej będziemy mądrzy po szkodzie.

59 Microsoft ostatnio zlecił badanie w celu zrozumienia powszechności zjawiska mobbingu online[59]. To, co jest formalnie określane mianem cyberbullyingu może się różnić od tego, jak jest on postrzegany w zależności od kultury, a nawet pomiędzy różnymi osobami. 40% (w porównaniu ze średnią 25 krajów rzędu 37%) dzieci w wieku 8–17 lat, które wypełniły ankietę, przyznało że było obiektem różnych zachowań, z których część można postrzegać jako mobbing:

- 31% wrogie lub nieprzyjemne traktowanie,
- 17% wyśmiewanie lub drażnienie się,
- 17% agresja słowna.

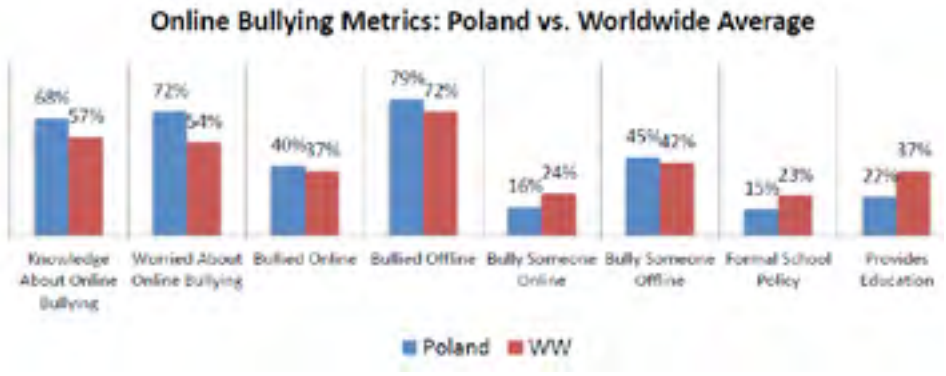
60 Polska jest na siódmym miejscu wśród najczęściej obserwowanych zachowań mobbingu na 25 ankietowanych krajów. Mobbing online występuje stosunkowo rzadko, podczas gdy realny mobbing plasuje się na poziomie średnim. Siedmioro na dziesięcioro dzieci wie dużo lub coś na ten temat oraz podobny odsetek jest bardzo lub względnie zaniepokojony tym zjawiskiem. Rodzice podejmują średnią liczbę kroków w celu ochrony swoich dzieci (3,8 wobec 3,3). W polskich szkołach jest średnio mniej formalnych regulaminów szkolnych odnoszących się do tego zjawiska, jak również mniej zaznajomionych z tym tematem nauczycieli, rodziców oraz uczniów.

[57] M. Garaigordobil, *Prevalencia y consecuencias del cyberbullying: una revisión*, „International Journal of Psychology and Psychological Therapy", 11(2)/2011, s. 233–254.

[58] M. Garaigordobil, *Prevalencia y consecuencias del cyberbullying: una revisión*. „International Journal of Psychology and Psychological Therapy", 11(2)/2011, s. 243

[59] http://www.microsoft.com/en-us/download/details.aspx?id=30148>; data dostępu 2013.12.18.

Wykres 1. Cyberprzemoc: Polska w porównaniu ze średnią światową



Legenda:

- wiedza na temat cyberprzemocy (Knowledge About Online Bullying),
- zaniepokojenie zjawiskiem (Worried About Online Bullying),
- odsetek osób, które doświadczyły cyberprzemocy (Bullied Online),
- odsetek osób, które doświadczyły mobbingu (Bullied Offline),
- odsetek osób, które dopuściły się cyberprzemocy (Bully Someone Online),
- odsetek osób, które dopuściły się mobbingu (Bully Smeone Offline),
- szkolna polityka (Formal School Policy),
- edukacja (provides Education).

Źródło: http:www.microsoft.comen-usdownloadderails.aspx&id. Data dostępu 18.12.2013

BIBLIOGRAFIA:

Beran, T., & Li, Q., *The Relationship Between Cyberbullying and School Bullying*. ‘‘The Journal of Student Wellbeing”, 1(2)/2008.

Bulut S., & Gündüz S., *Exploring Violence in the Context of Turkish Culture and Schools* w: Jimerson S. R., Nickerson A. B., Mayer M. J., & Furlong M. J. (Eds.), *Handbook of School Violence and School Safety: International Research and Practice* (2nd ed.) (pp. 165–174). New York 2012, NY: Routledge.

Campbell, M. A.,*Cyber Bullying: An old Problem in a New Guise? ”*Australian Journal of Guidance and Counselling”, 15(1)/2005,

Cassidy W., Brown K. & Jackson M., *Moving from Cyber-Bullying to Cyber-Kindness: What do Students, Educators and Parents say?* In Dunkels E., Franberg G. M., & Hallgren C. (Eds.), Youth Culture and Net Culture: Online social practices (pp. 256–277). Hershey, NY: Information Science Reference 2011

Cassidy W., Faucher C. & Jackson M., *Cyberbullying among Youth: A Comprehensive Review of Current International Research and its Implications and Application to Policy and Practice*. ,,School Psychology International” 2013.

Couvillon M. A. & Ilieva V., *Recommended Practices: a Review of Schoolwide Preventative Programs and Strategies on Cyberbullying*, „Preventing School Failure: Alternative Education for Children and Youth” 55(2)/2011.

Cowie H., Hutson N., Jennifer D. & Myers C. A., *Taking Stock of Violence in UK Schools Risk, Regulation, and Responsibility*, ,,Education and Urban Society”, 40(4)/2008, Craig W. M., Henderson K. & Murphy J. G., *Prospective Teachers' Attitudes Toward Bullying and Victimization*, ,,School Psychology International”, 21(1)/2000.

David-Ferdon C. & Hertz M. F., *Electronic Media, Violence and Adolescents: An Emerging Public Health Problem*, ,,Journal of Adolescent Health”, 41(6)/2007.

Demaray M. K., Malecki C. K., Jenkins L. D. & Westermann L. D., *Social Support in the Lives of Students Involved in Aggressive and Bullying Behaviours*, „Handbook of School Violence and School Safety: International Research and Practice”, 2012, Del Rey R., Elipe P. & Ortega-Ruiz R., *Bullying and cyberbullying: Overlapping and Predictive Value of the Co-occurrence*. „Psicothema”, 24(4)/2012.

Dinakar K., Reichart, R. & Lieberma, H., *Modeling the Detection of Textual Cyberbullying*, „The Social Mobile Web”, 7/2011.

Dooley J. J., Pyżalski J. & Cross D., *Cyberbullying versus Face-to-face Bullying*, „Zeitschrift für Psychologie/Journal of Psychology”, 217(4)/2009,

Franco, L.R., Bellerín, M., Borrego, J., Díaz, F. & Molleda, C., *Tolerance Towards Dating Violence in Adolescents*. „Psicothema”, 24(2)/2012.

Garaigordobil, M., *Prevalencia y consecuencias del cyberbullying: una revisión*. „International Journal of Psychology and Psychological Therapy”, 11(2)/2011.

Garaigordobil, M., & Berrueco, L., *Effects of a Play Program on Creative Thinking of Preschool Children*. „Spanish Journal of Psychology”, 14(2)/2011.

Hatzchristou, C., Polychroni, F., Issari, P., & Yfanti, T., *A synthetic approach for the study of aggression and violence in Greek schools* w: Jimerson S. R., Nickerson A.

B., Mayer M. J., & Furlong M. J. (Eds.), *Handbook of School Violence and School Safety: International Research and Practice* (2nd ed.) (s. 141–152). New York 2012, NY: Routledge.

Heirman, W., & Walrave, M., *Assessing Concerns and Issues about the Mediation of Technology in Cyberbullying*. „Cyberpsychology: Journal of Psychosocial Research on Cyberspace", 2(2)/2008, article 1. http://cyberpsychology.eu/view.php?cisloclanku=2008111401&article=1 Heirman, W. & Walrave, M., *Predicting Adolescent Perpetration in Cyberbullying: an Application of the Theory of Planned Behavior.* „Psicothema", 24(4)/2012.

Hinduja, S. & Patchin, J.,*Bullies Move Beyond the Schoolyard: a Preliminary Look at Cyberbullying*. „Youth Violence and Juvenile Justice", 4(2)/2006.

Hinduja, S. & Patchin, J.,*Offline Consequences of Online Victimization: School Violence and Delinquency*. „Journal of School Violence", 6(3)/2007.

Hinduja, S. & Patchin, J.,*Cyberbullying: an Exploratory Analysis of Factors Related to Offending and Victimization*. "Deviant Behavior", 29(2)/2008.

Hinduja, S., & Patchin, J. W. (2009). *Preventing Cyberbullying: Top Ten Tips for Educators*. < http://www.nyasp.biz/conf_2013_files/Kelly_Top_Ten_Tips_Educators_Cyberbullying_Prevention.pdf >. data dostępu 28.12.2013.

Hinduja, S., & Patchin, J. W. (2012). *Cyberbullying: Neither an epidemic nor a rarity*. „European Journal of Developmental Psychology", 9, 539–543, doi:10.1080/17405629.(2012).706448.

Kerr, O. S.,*Vagueness Challenges to the Computer Fraud and Abuse Act*. „Minn. L. Rev.", 94/2009, 1561.

Kochenderfer-Ladd, B., & Pelletier, M. E., *Teachers' Views andBbeliefs about Bullying: Influences on Classroom Management Strategies and Students' Coping with Peer Victimization*. "Journal of School Psychology", 46(4)/2008,

König, A., Gollwitzer, M., & Steffgen, G., *Cyberbullying as an act of revenge?*, „Australian Journal of Guidance and Counselling", 20(02)/2010,

Kontostathis, A., Reynolds, K., Garron, A., & Edwards, L., *Detecting Cyberbullying: Query Terms and Techniques*, „Proceedings of the 5th Annual ACM Web Science Conference" 5/2013 (pp. 195–204). ACM.

Kowalski, R. M., & Limber, S. P., *Electronic Bullying Among Middle School Students*, „Journal of Adolescent Health", 41/2007, Kowalski, R. M., Limber, S. P., & Agatston, P. W., *Cyber Bullying*, Malden 2008, MA: Blackwell.

Kowalski, R. M., Limber, S. Agston, P. W., *Cyberbullying: Bullying in the Digital Age*, 2th edition, Malden 2012a, MA, Wiley–Blackwell.

Kowalski, R. M., Morgan, C. A., & Limber, S. P., *Traditional Bullying as a Potential Warning Sign of Cyberbullying*. "School Psychology International", 33/2012b doi:10.1177/0143034312445244.

Law, D. M., Shapka, J. D., Hymel, S., Olson, B. F., & Waterhouse, T.,, *The Changing Face of Bullying: An Empirical Comparison between Traditional and Internet Bullying and Victimization*. „Computers in Human Behavior", 28(1)/2012,

Li, Q., Cross, D., & Smith, P. (Eds.), *Cyberbullying in the Global Playground: Research from International Perspectives*. West Sussex 2012a, Wiley-Blackwell.

Li, Q., Smith, P. K., & Cross, D.,, *Research into Cyberbullying: Context*, W: Q. Li, D. Cross, & P. K. Smith (Eds.), *Cyberbullying in the Global Playground: Research from International Perspectives* (s. 3–12), West Sussex,2012b, Wiley-Blackwell.

Lenhart, A. (2010), *Cyberbullying 2010: What the Research Tells Us. Resource Document. Youth Online Safety Working Group*. <http://www.pewinternet.org/Presentations/2010/May/Cyberbullying-2010.aspxZ; data dostępu 01.03.2014.

Limber, S. P. (2012), *Cyberbullying: Bullying in the Digital Age*, Wiley. com.

Livingstone, S., Haddon, L., Görzig, A. & Ólafsson, K. (2011), *Risks and Safety on the Internet: the Perspective of European Children. Full Findings*, LSE, London: EU Kids Online.

Maticka-Tyndale, E., & Barnett, J. P., *Peer-led Interventions to Reduce HIV Risk of Youth: a Review*, „Evaluation and Program Planning", 33(2)/2010,

Mc Guckin, C., Perren, S., Corcoran, L., Cowie, H., Dehue, F., Ševíková, A., ... & Völlink, T. (2014), *Coping with Cyberbullying: How Can we Prevent Cyberbullying and How Victims Can Cope with it*.; doc document retrieved: 1.01.2014.

McKenna K. Y., & Green A. S., *Virtual Group Dynamics*, „Group Dynamics: Theory, Research, and Practice", 6(1)/2002, 116.

Meredith J. P., *Combating Cyberbullying: Emphasizing Education over Criminalization*, Fed. Comm. LJ, 63/2010, 311.

Moore M. J., Nakano T., Suda T., & Enomoto, A.,*Tools in Cyberbullying*, „Social Network Engineering for Secure Web Data and Services", 67/2013.

Naylor P., & Cowie H., *The Effectiveness of Peer Support Systems in Challenging School Bullying: the Perspectives and Experiences of Teachers and Pupils*, „Journal of Adolescence", 22(4)/1999.

Ortega, R., Mora-Merchán, J. A., & Jäger, T. (2007), *Acting Against School Bullying and Violence. The Role of Media, Local Authorities and the Internet*, Verlag Empirische Pädagogik: Landau. Available at: www. bullying-in-school. info/uploads/media/E-Book_English_01. pdf In the Painful lessons report.

Ortega-Ruiz, R. & Nunez, J.C., *Bullying and cyberbullying: research and intervention at school and social contexts*, „Psicothema", 24(4)/2012.

Olweus, D. (1993), *Bullying at School: What we Know and What We Can Do*, Wiley-Blackwell.

Olweus, D. (2012a), *Cyberbullying: An Overrated Phenomenon?* „European Journal of Developmental Psychology", 9, 520–538, doi:10.1080/17405629.(2012).682358.

Olweus, D. (2012b). Comments on Cyberbullying Article: A Rejoinder, "European Journal of Developmental Psychology", 9, 559–568, doi:10.1080/17405629.(2012).705086.

Perren, S., Corcoran, L., Cowie, H., Dehue, F., Garcia, D. J., Mc Guckin, C., ... & Völlink, T., *Tackling Cyberbullying: Review of Empirical Evidence Regarding Successful Responses by Students, Parents, and Schools*, "International Journal of Conflict and Violence", 6(2)/2012,

Palladino, B.E., Nocentini, A. & Menesini E., *Online and Offline Peer Led Models Against Bullying and Cyberbullying*, "Psicothema", 24(4)/2012,

Patchin, J.W., Hinduja, S. (2007*), Cyberbullying: an Exploratory Analysis of Factors Related to Offending and Victimization. Deviant Behavior.*

Paul, S., Smith, P. K., & Blumberg, H. H., *Addressing Cyberbullying in School Using the Quality Circle Approach*, „Australian Journal of Guidance and Counselling", 20(02)/2010, s. 157-168.

Paul, S., Smith, P.K. & Blumberg, H.H. , *Investigating legal aspects of cyberbullying*,„Psicothema", 24(4)/2012.

Perren, S., Dooley, J., Shaw, T., & Cross, D., *Bullying in school and cyberspace: Associations with depressive symptoms in Swiss and Australian adolescents*, „Child and Adolescent Psychiatry and Mental Health", 4(28)/2010.

Perren, S., Corcoran, L., Cowie, H., Dehue, F., Garcia, D. J., Mc Guckin, C., ... & Völlink, T.,, *Tackling Cyberbullying: Review of Empirical Evidence Regarding Successful Responses by Students, Parents and Schools*, "International Journal of Conflict and Violence", 6(2)/2012.

Popovic B., Djuric, S., & Cvetkovic, V. (2011), *The Prevalence of Cyberbullying among Adolescents: A Case Study of Middle Schools in Serbia*, „School Psychology International", 32, 412–424, doi:10.1177/0143034311401700.

Reynolds, K., Kontostathis, A., & Edwards, L., *Using Machine Learning to Detect Cyberbullying*, Machine Learning and Applications and Workshops (ICMLA), 2011 10th International Conference" 12/2011 (Vol. 2, pp. 241–244). IEEE.

Riebel, J., Jaeger, R. S., & Fischer, U. C., *Cyberbullying in Germany–an Exploration of Prevalence, Overlapping with Real Life Bullying and Coping Strategies*, „Psychology Science Quarterly", 51(3)/2009, 298–314.

Rivers, I., & Noret, N., *'I h8 u': Findings from a Five-year Study of Text and email Bullying*, „British Educational Research Journal", 36/2010, 643–671, doi:10.1080/01411920903071918.

Ryan, T., Kariuki, M., Yilmaz, H., Gazi, Z. A., Ongun, E., Atlas, D. & Burston, J., *A Comparative Analysis of Cyberbullying Perceptions of Preservice Educators: Canada and Turkey,* „TOJET" 10(3)/2011.

Sahin, M., *Teachers' Perceptions of Bullying in High Schools: A Turkish Study*, „Social Behavior and Personality: an International Journal", 38(1)/2010,

Smith P. K., Cowie H., Olafsson R. & Liefooghe A., *Definitions of Bullying: a Comparison of Terms Used and Age and Gender Differences, in a Fourteen-country International Comparison*, „Child Development", 73/2002,.

Smith, P. K., Mahdavi, J., Carvalho, M., & Tippett, N., *An Investigation into Cyberbullying, its Forms, Awareness and Impact, and the Relationship between Age and Gender in Cyberbullying*, „Research Brief" No. RBX03-06/2006, London: DfES.
Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., Tippett , N., *Cyberbullying: its nature and impact in secondary school pupils*, „J Child Psychol Psychiatry", 49 (4)/2008.

Smith, P. K., Slonje, R. (2010), *Cyberbullying: The nature and extent of a new kind of bullying, in and out of school*, w: S. R. Jimerson, S. M. Swearer, & D. L. Espelage (Eds.),

Handbook of Bullying in Schools: An International Perspective (pp. 249–262). New York, NY: Routledge.

Snakenborg, J. A.,, *Cyberbullying: Prevention and intervention to protect our children and youth*, „Preventing School Failure", 55(2)/2011.

Sourander, A., Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M., ... & Helenius, H.,, *Psychosocial Risk Factors Associated with Cyberbullying among Adolescents: A Population-based Study*, "Archives of General Psychiatry", 67(7)/2010, 720.

Turner, G., & Shepherd, J. ,,*A Method in Search of a Theory: Peer Education and Health Promotion,* „Health Education Research", 14(2)/1999.

Vandebosch, H., Beirens, L., D'Haese, W., Wegge, D. & Pabian, S., *Police actions with regard to cyberbullying: the belgian case*, „Psicothema", 24(4)/2012.

Valkenburg, P. M., & Peter, J., *Online Communication among Adolescents: An Integrated Model of its Attraction, Opportunities and Risks*. „Journal of Adolescent Health", 48(2)/2011.

von Mare´ es, N., & Petermann, F., *Cyberbullying: An increasing challenge for schools.* „School Psychology International", 33/2012, 467–476, doi:10.1177/0143034312445241.

Wachs, S., Wolf, K.D. & Pan, Ch.-Ch., *Cybergrooming: Risk Factors, Coping Strategies and Associations with Cyberbullying*, „Psicothema", 24(4)/2012,

Willard, N. E. (2006), *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Cruelty, Threat, and Distress*. Center for Safe and Responsible Internet Use.

Ybarra, M.L., & Mitchell, K.J., *Online Aggressor/targets, Aggressors and Targets: A Comparison of Associated Youth Characteristics*, „Journal of Child Psychology and Psychiatry", 45/2004, 1308–1316.

Ybarra, M., Mitchell, K., Wolak, J. & Finkelhor, D., *Examining Characteristics and Associated Distress Related to Internet Harassment: Findings from the Second Youth Internet Safety Survey, „*Pediatrics", 118(4)/2006.

Ybarra, M. & Mitchell, K., *Prevalence and frequency of Internet harassment instigation: implications for adolescent health*, „Adolesc Health", 41(2)/2007.

Zuchora-Walske, C. ,,*Internet Censorship: Protecting Citizens Or Trampling Freedom?*,Twenty-First Century Books 2010.

SAMOBÓJSTWA
Z INSPIRACJI SIECI

Anna Andrzejewska

OPIS ZJAWISKA

1 **WPROWADZENIE**

Terminologia związana z samobójstwem jest bardzo zawiła. Dla naukowców badających to zjawisko pojęcia z nim związane mają różne znaczenie, interpretacje.

W celu uporządkowania wiedzy związanej ze zjawiskiem samobójstwa podano poniżej propozycje terminów.

2 **DEFINICJA**

Według *Popularnej Encyklopedii Powszechnej* **samobójstwo to świadome pozbawienie się życia, które najczęściej jest skutkiem poważnych zaburzeń psychicznych (depresja) lub chwilowych kryzysów emocjonalnych**[1].

Jest to jednak niekompletna definicja oddająca istotę tego zjawiska. Zjawisko to ma wiele złożonych przyczyn często połączonych ze sobą. Najodpowiedniejsza zatem wydaje się tu definicja stworzona przez E. Durkheima. Według francuskiego socjologa **samobójstwem nazywamy każdy przypadek śmierci, który bezpośrednio lub pośrednio wynika z pozytywnego lub negatywnego działania ofiary, która wiedziała, że da ono taki rezultat. Próba samobójcza to określone wcześniej działanie, z tą różnicą, iż nie wynikła z niego śmierć**[2].

3 Światowa Organizacja Zdrowia określa samobójstwo jako proces długotrwały i wieloetapowy. Rozpoczyna się już w dzieciństwie i stanowi wypadkową psychospołecznej sytuacji jednostki, jej pozycji i ról pełnionych w poszczególnych kręgach środowiskowych, a także wewnętrznej, subiektywnej percepcji rzeczywistości i własnej wartości[3].

4 Z kolei B. Hołyst analizując Durkheima i innych naukowców tworzy własną definicję samobójstwa. **Samobójstwo jest przez niego interpretowane jako końcowe ogniwo procesu autodestrukcji.** Zachowanie autodestrukcyjne nazywane jest tu świadomym destrukcyjnym zachowaniem jednostki, która na takie zachowanie się godzi[4].

5 Zdaniem I. Pospiszyl najważniejsze koncepcje dewiacji to:

„• teoria anomii – dewiacja jako efekt niedostatecznej kontroli społecznej;
• teoria stygmatyzacji, teoria neutralizacji – dewiacja, jako konsekwencja nadużycia kontroli społecznej;
• teoria zróżnicowanych powiązań – dewiacja jako zachowanie wyuczone;
• teoria Hirscha – dewiacja jako konsekwencja więzi społecznych;
• koncepcja ponownego przemyślenia Ferscha – dewiacja jako wybór jednostki”[5].

6 Według I. Pospiszyl samobójstwem „jest świadome zachowanie, którego przynajmniej jednym z bezpośrednich celów jest pozbawienie siebie życia”[6]. I. Pospiszyl uważa, iż należy do „charakterystycznych cech agresji zaliczyć:

[1] M. Szulc (red.), *Popularna Encyklopedia Powszechna*, Wydawnictwo Pinnex, Kraków 1997, s. 44.

[2] E. Durkheim, *Samobójstwo. Studium z socjologii*, Oficyna Naukowa, Warszawa 2006, s. 51.

[3] B. Mroziak [przekł. z jęz. ang.], *Zapobieganie samobójstwom. Poradnik dla pracowników mediów,* Światowa Organizacja Zdrowia, Genewa- Warszawa 2003, s. 8, http://www.who.int/mental_health/prevention/suicide/en/suicideprev_media_polish.pdf, data dostępu 24.02.2011.

[4] B. Hołyst, *Suicydologia*, Wydawnictwo Prawnicze LexisNexis, Warszawa 2001, s. 42–43.

[5] I. Pospiszyl, *Patologie społeczne. Resocjalizacja*, Wyd. Naukowe PWN, Warszawa 2008, s.27.

[6] Tamże, s. 95.

- wzrost brutalizacji zachowań (…);
- unifikację grupową zachowań agresywnych (…);
- unifikację płciową (…);
- manifestację zachowań agresywnych (…);
- obniżenie się wieku nieletnich sprawców zachowań brutalnych;
- brak więzi grupowej;
- objaw zaburzeń osobowościowych;
- objaw doświadczeń ekstremalnych”[7].

7 Według Bermann I. Jobes osoby młode zagrożone samobójstwem to:

- dorastający w depresji;
- osoby uzależnione od środków odurzających (narkotyki, alkohol);
- jednostki o cechach osobowości pogranicza;
- jednostki antyspołeczne lub zdradzające zaburzenia zachowania;
- osoby izolowane;
- sztywni perfekcjoniści, „gwiazdy” czujące się zagrożone;
- osobnicy psychotyczni, mający halucynacje lub ataki paniki;
- dorastający w czasie kryzysu psychologicznego, u których do sytuacji stresowej doprowadzają impulsywność i irracjonalność[8].

8 Suicydologia jako nauka przyjmuje za pierwsze kryterium klasyfikacyjne w analizie zjawiska skutek zamachu samobójczego. Wyróżnia się zamachy kończące się śmiercią – są to samobójstwa dokonane oraz zamachy, w wyniku których nie dochodzi do śmierci – są to samobójstwa usiłowane[9].

9 Istnieje również pojęcie dość często mylone z próbą samobójczą. Jest to parasamobójstwo. Parasamobójstwo to innymi słowy „pozorowana próba samobójcza, dość popularna wśród młodzieży”[10].

E. Durkheim w swej pracy wskazał cztery rodzaje samobójstwa. Są to:

- samobójstwo egoistyczne,
- samobójstwo altruistyczne,
- samobójstwo anomiczne,
- samobójstwo fatalistyczne[11].

10 **Samobójstwo egoistyczne** charakteryzuje się zbyt niskim przywiązaniem do grupy społecznej. **Samobójstwo altruistyczne** wiąże się z przesadnym przywiązaniem do danej grupy społecznej i przedkładaniem jej interesu nad własny. **Samobójstwo anomiczne** popełniane jest przez zachwianie bezpieczeństwa, punktów odniesienia w życiu człowieka. Ostatni rodzaj samobójstwa to **samobójstwo fatalistyczne**, które wynika z bezsilności, braku wpływu na większą grupę społeczną[12].
Innym pojęciem związanym ze zjawiskiem samobójstwa jest samouszkodzenie. „Jest to zachowanie autodestrukcyjne polegające na celowym uszkodzeniu ciała. Najczęstszym sposobem samouszkodzenia jest cięcie się i trucie”[13].

11 **GRUPA RYZYKA**

Do grupy podwyższonego ryzyka, która jest zagrożona samounicestwieniem należy zaliczyć:

[7] Tamże, s. 110.

[8] Por. K. Zajączkowski, *Profilaktyka zachowań dewiacyjnych dzieci i młodzieży*, Toruń 1998.

[9] B. Hołyst (red.), *Samobójstwo,* Polskie Towarzystwo Higieny Psychicznej, Warszawa, 2002, s. 29.

[10] A. Carr, *Depresja i próby samobójcze wśród młodzieży*, Biblioteka Wychowawcy, Gdańsk, 2008, s. 51.

[11] E. Durkheim, *Samobójstwo. Studium z socjologii*, Oficyna Naukowa, Warszawa, 2006, s. 356–62.

[12] W. Surówka, *Samobójstwo*, http://www.superja.pl/node/1835, data dostępu 17.02.2011.

[13] C. Fox, K. Hawton, *Zachowania autodestrukcyjne młodzieży—szkoła bezradna?*, Fraszka Edukacyjna, Warszawa, 2009, s. 11.

OPIS ZJAWISKA

1) ludzi młodych borykających się z problemami w kontaktach z rodzicami, sympatiami, nauką;
2) ludzi starych, ze szczególnym wskazaniem na ludzi osamotnionych, izolujących się od społeczeństwa;
3) osoby chore na przewlekłe choroby somatyczne i psychiczne, zaniedbujące leczenie;
4) ludzi przeżywających długotrwałe problemy w ramach związku (kryzysy małżeńskie, miłosne);
5) osoby znajdujące się w trudnej sytuacji socjalnej, mające kłopoty finansowe, borykające się z trudnymi warunkami mieszkaniowymi;
6) osoby, któe już w przeszłości podejmowały nieudane lub symulowane próby samobójcze;
7) osoby uzależnione od alkoholu i innych środków psychoaktywnych;
8) członkowie rodzin alkoholików, a w szczególności kobiety;
9) osoby, które są ofiarami zachowań agresywnych (np. znęcania się w rodzinie, szkole, wojsku, zakładzie karnym, pracy, itp.)[14].

12 W polskim prawie nie istnieje kara za popełnienie lub chociażby usiłowanie popełnienia samobójstwa. Przepisy wiążące się z samobójstwem znajdują się w Kodeksie Karnym. Karze podlega w tym wypadku tylko: osoba, która doprowadziła przez znęcanie się do sytuacji, w której ofiara targa się na własne życie (art. 207, § 3 KK[15]), osoba, która nakłaniała do samobójstwa lub pomogła w nim innej osobie (art. 151 KK[16]). W pierwszym przypadku za przestępstwo grozi od dwóch do dwunastu lat, w drugim natomiast od trzech miesięcy do pięciu lat pozbawienia wolności.

13 Od 2010 roku do przestępstw karalnych w Kodeksie Karnym dołączył stalking, czyli prześladowanie osoby poprzez nagminne esemesy, niechciane prezenty oraz uporczywe telefonowanie. Nowelizacja w wypadku popełnienia przestępstwa przewiduje karę pozbawienia wolności do trzech lat. Jeżeli w wyniku przestępstwa osoba poszkodowana targnie się na swoje życie, kara ta wzrasta do dziesięciu lat pozbawienia wolności[17].

14 CHARAKTERYSTYKA MŁODZIEŻY W OKRESIE ADOLESCENCJI

Nastolatkowie przechodzą jeden z najtrudniejszych okresów swojego życia, jakim jest dojrzewanie. Młodzi ludzie w tym okresie charakteryzują się niezrównoważeniem emocjonalnym (nadmierna pobudliwość) oraz drażliwością. Chłopcy często są nadmiernie agresywni, łatwo doprowadzić ich do wybuchów złości. Dziewczęta są za to płaczliwe, nadąsane, mają często zły humor. W okresie pełnej adolescencji, jaka następuje między 12 a 17 rokiem życia, młodzież uniezależnia się od rodziców, stawiając nad nich rówieśników, jest arogancka, buntownicza, nie posiada autorytetów. Pojawiają się u niej pierwsze intensywne emocje[18].

15 Dojrzewanie jest nie tylko procesem prowadzącym do dojrzałości fizycznej i zdolności reprodukcji, ale również procesem, w którym dochodzi do rozwoju sfery emocjonalnej i psychicznej młodego człowieka. Jest przejściem od młodości

[14] B. Hołyst, *Wiktymologia*, Warszawa 2003, s. 204—205.

[15] http://www.polskieustawy.com/norms.php?head=0&actid=474&adate=20061220&norm=207&lang=48#vor, data dostępu 24.02.2011.

[16] http://www.polskieustawy.com/norms.php?actid=474&norm=151&lang=48&adate=20061220&head=0, data dostępu 24.02.2011.

[17] http://www.tvn24.pl/-1,1693976,0,1,trzy-lata-za-uporczywe-i-zlosliwe-nekanie,wiadomosc.html, data dostępu 28.02.2011.

[18] A. Wróblewska, *Charakterystyka młodzieży w wieku gimnazjalnym*, s. 1—2, http://sod.ids.czest.pl/publikacje2/l1117/l1117.pdf, data dostępu 05.03.2011.

do dojrzałej dorosłości[19]. Dynamika okresu młodości wpływa na tryb życia i motywacje postępowania młodzieży[20].

16 Młodzież w okresie dojrzewania intelektualnie rozwija w sobie:

- „refleksyjność i krytycyzm – młodzi ludzie zaczynają postrzegać sprzeczności teorii i praktyki w życiu rodzinnym i społecznym. Krytycyzm przejawia się jako agresja werbalna w stosunku do dorosłych osób, a w stosunku do rówolatków w dyskusjach i sporach;
- zdolność do obiektywnego ujmowania działań i właściwości innych ludzi – młodzi ludzie nabywają umiejętność interpretowania intencji, stanów uczuciowych i motywów innych;
- wyobraźnię – młodzież używa marzeń dość często jako ucieczki od trudnych sytuacji, tworzy wyidealizowany obraz siebie i świata;
- pamięć logiczną i dowolną”[21].

17 Rozwój moralny w czasie dorastania jest swoistą próbą sprawdzającą wartość wcześniejszych lat wychowania. Konieczność podejmowania decyzji w tym czasie może wiązać się z ,,załamaniem się” dotychczasowych wartości i norm uznawanych u dziecka[22].

18 Jak twierdzi A. Kubin, młodzież w okresie dorastania jest zagubiona w określeniu siebie. Z jednej strony młody człowiek pragnie nadal być dzieckiem, by być traktowany przez rodziców pobłażliwie, z drugiej zaś strony w gronie rówieśników przyjmuje on pozy dorosłej osoby. Taka postawa jest szukaniem odpowiedzi na pytanie o własną tożsamość. Hormony buzujące w nastolatku powodują pojawianie się kłopotów, które z czasem stają się wielkimi problemami i okazją do sporów z rodzicami i rówieśnikami. Zdolność myślenia formalnego, która pojawia się w czasie dorastania, pozwala na stawianie hipotez i weryfikowanie ich w praktyce, w ten sposób młody człowiek wyrabia własny światopogląd[23].

19 Pobudzenie emocjonalne występujące we wczesnej fazie dorastania (przypadające na wiek gimnazjalny) doprowadza nastolatka do stanów od skrajnej radości do głębokiej rozpaczy. Emocje przeżywane przez młodą osobę są wysoce intensywne. Pobudzenie w tym wypadku dotyczy przeżyć okazywanych zewnętrznie. Emocje mogą się intensyfikować również wewnętrznie, co trudno zaobserwować. Nastolatek ukrywa swoje przeżycia przed najbliższymi, okazując inne, niezgodne ze stanem faktycznym odczucia, które dla otoczenia są sztuczne i przesadne[24].

20 Dokonując analizy samobójstw, warto jeszcze zwrócić uwagę na inspirację sieci do tego czynu. Istotne znacznie mają w tym procesie gry komputerowe, które modelują określone zachowania[25].

[19] N. Wolański, *Dojrzewanie jako etap w rozwoju osobniczym człowieka*, w: A. Jaczewski, B. Woynarowska (red.), *Dojrzewanie*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa, 1982 s. 12.

[20] Tamże, s. 15.

[21] I. Obuchowska, *Psychologiczne aspekty dojrzewania*, w: A. Jaczewski, B. Woynarowska (red.), *Dojrzewanie*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1982, s. 138–139.

[22] Tamże, s. 145.

[23] A. Kubin, *W trosce o emocjonalną niezależność*, „Edukacja i Dialog”, Warszawa 2007, nr 5, s. 31–32.

[24] I. Obuchowska, *Psychologiczne aspekty dojrzewania*, w: A. Jaczewski, B. Woynarowska (red.), *Dojrzewanie*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1982, s. 152.

[25] Por. M. Jędrzejko, *Śmierć w sieci. Modelowanie zachowań agresywnych w grach komputerowych i sieciowych,* w: S. Bębas, J. Plis, J. Bednarek (red.), *Patologie w cyberprzestrzeni*, Wyd. WSzH w Radomiu, Radom 2012.

ROZPOZNANIE OBJAWY

21 **CECHY MŁODYCH LUDZI W WIEKU DORASTANIA, POPEŁNIAJĄCYCH SAMOBÓJSTWA**

Jest wiele czynników, dzięki którym ryzyko popełnienia przez dojrzewającego nastolatka samobójstwa wzrasta. Najczęściej występującymi są:

- cechy osobowości,
- obciążenia rodzinne,
- wcześniejsze zachowania samobójcze,
- stresujące wydarzenia,
- czynniki społeczne i kulturowe,
- zaburzenia psychiczne,
- kontakt z zamachem samobójczym innej osoby[26].

22 Zamach samobójczy innej osoby pociąga za sobą ryzyko decyzji nastolatka o popełnieniu samobójstwa. Jest to samobójstwo naśladowcze, które występuje w wypadku, gdy młoda osoba dowiaduje się o samobójstwie bliskiej osoby lub kogoś sławnego, np. swojego idola. Naśladowanie może być wynikiem:

- silnego zainteresowania śmiercią,
- większym pozwoleniem na takie zachowania[27],
- wszystkie czynniki suicydogenne mogą współdziałać ze sobą.

23 O decyzji popełnienia samobójstwa w połączeniu z depresją decydują takie cechy osobowości jak:

- wycofanie,
- perfekcjonizm,
- słaba kontrola emocji,
- agresja,
- brak zaufania,
- bezwzględność,
- poczucie beznadziejności[28].

24 Wpływu na podejmowanie decyzji o samobójstwach nie ma sytuacja materialna rodziny, lecz jej dysfunkcyjność. Rodzina, w której młoda osoba podejmuje próbę samobójstwa jest konfliktowa, często rozbita. Występuje w niej często choroba alkoholowa jednego lub obojga rodziców, zaburzenia komunikacji oraz niekonsekwentne oddziaływania wychowawcze[29].

25 Według M. Jarosz, analizując zachowania samobójcze młodych samobójców warto zwrócić uwagę na ich pochodzenie społeczne. Najwyższy wskaźnik prób samobójczych utrzymuje się wśród dzieci z rodzin robotniczych. Najczęściej są to środowiska rodzin robotniczych niewykwalifikowanych. Najniższy wskaźnik występuje wśród dzieci z rodzin rolników[30].

26 **ROZPOZNANIE OBJAWY**

Najbardziej charakterystycznym objawem prowadzącym do przyszłych zachowań samobójczych jest depresja. „Depresja jest zespołem zaburzeń psychicznych, wiążącym się z depresyjnym nastrojem, różnymi zahamowaniami, niepokojem psychicznym oraz długotrwałym lękiem”[31].

Depresja występuje częściej w wieku młodzieńczym niż w okresie dzieciństwa.

[26] M. Tryburcy, *Samobójstwa młodych – czy zawsze nieprzewidywalne?*, http://www.przyjaciele.org/czytelnia.php?id=6, data dostępu 28.02.2011.

[27] A. Młodożeniec, J. Janiak, *Uwarunkowania zachowań samobójczych dzieci i* młodzieży – cz. I, w: *Remedium*, Państwowa Agencja Rozwiązywania Problemów Alkoholowych i Fundacja ETOH, Warszawa, 2009, nr 7/8, s. 3.

[28] M. Tryburcy, *Samobójstwa młodych – czy zawsze nieprzewidywalne?*, http://www.przyjaciele.org/czytelnia.php?id=6, data dostępu 28.02.2011.

[29] J. Komender, *Zapobieganie próbom samobójczym podejmowanym przez dzieci i młodzież,* w: B. Hołyst, M. Staniaszek (red.), *Samobójstwo. Materiały z I Konferencji Suicydologicznej w Łodzi w dniach 24–25.11.1995*, Polskie Towarzystwo Higieny Psychicznej, Warszawa–Łódź 1995, s. 93.

[30] M. Jarosz, *Samobójstwa. Ucieczka przegranych*, Wydawnictwo Naukowe PWN, Warszawa 2004, s. 108.

[31] *Depresja* , http://encyklopedia.pwn.pl/haslo.php?id=3891882, data dostępu 17.02.2011.

W badaniach próby populacji częstotliwość występowania depresji wśród osób w wieku dojrzewania waha się od 2 do 8%. Podatność na depresje zależy do płci. Depresja jest częstszym przypadkiem u dziewcząt niż u chłopców[32].

27 Depresja powoduje u młodych ludzi błędy atrybucyjne takie jak:

- myślenie typu ,,wszystko albo nic"— przyjmowanie kategorycznych kryteriów;
- selektywna ocena – koncentrowanie się na niewielkim elemencie danego zdarzenia i wyciąganie na jego podstawie wniosków;
- uogólnienie – rozpamiętywanie i rozciąganie sytuacji na wszystkie sfery życia;
- wyolbrzymianie – przesadzanie w nadawaniu wybranym sytuacjom znaczenia;
- personalizacja – przypisywanie sobie winy za negatywne odczucia innych;
- rozumowanie emocjonalne – postrzeganie odczuć jako faktów[33].

28 Chociaż najczęściej w wieku dorosłym samobójstwo wybierają mężczyźni, to w wieku młodzieńczym, nastoletnim próby samobójcze popełniają młode dziewczyny. Stosunek zamachów samobójczych u młodych dziewcząt w porównaniu z chłopcami wynosi 3,5:1. Z powodu samobójstwa częściej jednak giną chłopcy, co wyraża się stosunkiem 3,4:1[34].

29 Zgodnie z myślą R. Jabłońskiego[35] wiele badań potwierdza fakt, iż młodzi ludzie nie popełniają samobójstwa z tych samych powodów, co dorośli. Głównymi motywami w ich wypadku są niepowodzenia w szkole, złe relacje z rodzicami, odrzucenie ze strony środowiska lub utrata kogoś bliskiego, nieszczęśliwa miłość.

30 Zachowania ostrzegające przed próbą samobójczą to:

- picie alkoholu, zażywanie narkotyków i innych środków chemicznych;
- pisanie listów samobójczych;
- wybieranie dla siebie sposobu śmierci;
- zmiany w codziennym zachowaniu;
- zachowanie wskazujące na odczuwanie odrzucenia, upokorzenia, beznadziejności i izolacji;
- zachowanie impulsywne;
- inne zaburzenia zachowania, włączając w nie agresywność, złość i wrogość[36].

31 Aby odróżnić, czy nastolatek ma zamiar odebrać sobie życie czy też chce zmanipulować środowisko lub woła o pomoc, trzeba przeanalizować jego zachowanie pod kątem, czy jest to intencja samobójcza czy wyobrażenie samobójstwa. Intencje charakteryzuje:

- staranne planowanie czynu,
- zabezpieczenie się przed ewentualnym odkryciem zamiaru przez innych,
- wybór metody samobójstwa,
- nieprzyjmowanie pomocy,
- dokonanie samobójstwa[37].

[32] A. Carr, *Depresja i próby samobójcze wśród młodzieży*, Biblioteka Wychowawcy, Gdańsk, 2008, s. 11–12.

[33] Tamże, s. 22.

[34] J. Kula-Lic, *Problem samobójstw wśród dzieci i młodzieży*, „ Problemy Opiekuńczo-Wychowawcze," Instytut Rozwoju Służb Społecznych, Warszawa, 2009, nr 6, s. 21.

[35] R. Jabłoński, *Młodzi samobójcy są wśród nas, czy potrafimy ich rozpoznać?,*w: B. Hołyst (red.), *Samobójstwo*, Polskie Towarzystwo Higieny Psychicznej, Warszawa, 2002, s. 191.

[36] M. Tryburcy, *Samobójstwa młodych – czy zawsze nieprzewidywalne?*, http://www.przyjaciele.org/czytelnia.php?id=6, data dostępu 28.02.2011.

[37] A. Carr, *Depresja i próby samobójcze młodzieży. Sposoby przeciwdziałania i reagowania*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk, 2004, s. 52.

32 Wyobrażenie samobójcze jest natomiast opisywane jako nieplanowane samookaleczenia, najczęściej przez podcięcie żył[38]. Jeśli młody człowiek będzie chciał targnąć się na swoje życie, to będzie się kierował intencją samobójczą.

33 Zachowania autodestrukcyjne wśród młodzieży to niepokojąco szybko rosnący trend. Jest to grupa społeczna charakteryzująca się większą nieznajomością środków pozbawiających człowieka życia. Tym samym występuje w niej zwiększona liczba nieudanych prób samobójczych w porównaniu do samobójstw dokonanych[39].

34 Młodzi samobójcy to również grupa nieprzystosowana społecznie. Ich dewiacje łączą się ze sobą przy próbach samobójczych. Nieprzystosowanie objawia się[40] poprzez:

- ucieczki z domu,
- drugoroczność,
- picie alkoholu,
- zażywanie narkotyków,
- wybryki chuligańskie,
- karalność,
- kradzieże,
- pobyt w domach poprawczych.

35 **INTERNET MIEJSCEM INFORMACJI O SAMOBÓJSTWIE**

Internet to źródło wiedzy, ale też tej zakazanej. By dowiedzieć się o sposobach popełniania samobójstw, najlepszych do tego środkach itd. wystarczy wpisać w wyszukiwarkę frazy: „samobójstwo" lub ,,jak się zabić?". Blogów i stron internetowych, które można znaleźć na podstawie takiego szukania jest mnóstwo. Najczęściej są to pamiętniki nastolatków opisujących swoje odczucia związane z tematyką samobójstwa lub też strony poświęcone najlepszym sposobom samobójstwa, popełnianiu samobójstw w grupie, czasami wręcz namawianiu do targnięcia się na własne życie.

36 Najwięcej informacji na temat samobójstw można uzyskać poprzez wpisywanie odpowiednich słów kluczowych np. w wyszukiwarce Google, Yahoo, MSN i Ask. Co ciekawe, w wyszukiwarce MSN można znaleźć przede wszystkim informacje, jak zapobiegać samobójstwu. Zaskakujące, że w czołówce witryn internetowych, w których można znaleźć informacje dotyczące metod i sposobów popełnienia samobójstwa, jest znana wolna encyklopedia internetowa Wikipedia[41].

37 W roku 2007 w Wielkiej Brytanii przeprowadzono badanie Internetu pod kątem dostępności stron, na których można znaleźć informacje odnośnie popełnienia samobójstwa. W wyniku przeprowadzonych badań odnaleziono aż 240 strony, które poświęcone zostały tematyce samobójstwa, 90 portali internetowych mówiło o samobójstwie w sensie ogólnym, 45 stron namawiało wręcz do popełnienia samobójstwa, 62 portale postawiły sobie za cel przekonanie potencjalnego samobójcy, że targnięcie się na swoje życie nie jest najlepszym rozwiązaniem, natomiast 59 serwisów próbowało odstraszać różnymi metodami przed dokonaniem tego czynu[42].

[38] A. Carr, *Depresja i próby samobójcze młodzieży. Sposoby przeciwdziałania i reagowania*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk, 2004, s. 53.

[39] M. Jarosz, *Samobójstwa. Ucieczka przegranych*, Wydawnictwo Naukowe PWN, Warszawa, 2004, s. 106.

[40] Tamże, s.114–116.

[41] http://arstechnica.com/old/content/2008/04/suicide-searches-produce-disturbing-unsurprising-results.ars , data dostępu 04.01.2010.

[42] Ł. Bigo, *Samobójstwa w Internecie-łatwo znaleźć, łatwiej zapobiec*, http://www.idg.pl/news/147397/Samobojstwo.w.Internecie.latwo.znalezc.latwiej.zapobiec.html, data dostępu 02.01.2010.

38 Akty samobójcze na podstawie tych stron internetowych nie popełniają tylko młodzi ludzie dobrze zaznajomieni z najnowszą technologią informacyjną, ale również osoby starsze. W czerwcu 2003 roku amerykańskie media zawrzały po przypadku 52-letniej kobiety, która swoje ostatnie chwile zaaranżowała pod wpływem strony Kościoła Eutanazji. Policjanci, którzy znaleźli ciało kobiety z dwiema butlami helu do wdychania zabezpieczyli na miejscu kartkę z wydrukiem strony: ,,Jak popełnić samobójstwo?" Kościoła Eutanazji.

39 Innym przypadkiem zatracenia się w internetowych stronach o samobójstwie jest przykład z Trzcianki z Wielkopolski. W 2010 roku pewnego poranka 67-letnia Zofia R. została znaleziona w swoim mieszkaniu przez sąsiadkę. Była martwa, popełniła samobójstwo. Metodą, którą wybrała było założenie na głowę kilku toreb foliowych i zaklejenie ich taśmą na szyi w celu odcięcia dopływu powietrza. Jak twierdzą znajomi kobiety była ona fanką Internetu. Policja w czasie szukania motywu postępowania starszej pani znalazła w historii przeglądanych w komputerze stron mnóstwo odsłon na witrynach wskazujących, jak popełnić samobójstwo. Zofia R. szukała również wskazówek, jak spisać testament[43].

40 W Polsce internetowa aktywność ludzi poszukujących informacji o samobójstwie zaczęła się po podaniu do wiadomości informacji o samobójstwie 15-letniej Magdy z Gliwic. Dziewczynka zostawiła po sobie blog mówiący o jej ostatnich dniach życia, gdzie podpisywała się nickiem Kaarel. Ostatnia notka pochodzi z 17 marca 2003 roku. Po wrzawie medialnej na blog weszło tysiące internautów, a dwa miesiące później doszło do kolejnego samobójstwa – była to koleżanka Magdy, Ola. Skoczyła z tego samego wieżowca, co Magda. Po tym wydarzeniu blog został zamknięty. To jednak nie powstrzymało wirtualnej wioski od stworzenia nowych, naśladowczych blogów tego typu[44].

41 W 2009 roku internetową instrukcję dotyczącą samobójstwa znalazła również 19- letnia dziewczyna z Gdańska. Niedoszła samobójczyni zażyła tabletki w ponadnormowej dawce, co doprowadzić miało do śmierci. Lekarze z Pomorskiego Centrum Toksykologii uratowali nastolatkę dosłownie w ostatniej chwili. Dziewczyna przeszła ostrą niewydolność wątroby. Lekarze przestrzegają, iż tak zwani ,,eksperci od samobójstw" to ludzie niemający pojęcia o bezbolesnych sposobach na odejście z tego świata[45].

42 Najbardziej niebezpiecznym sposobem łączenia się ludzi chcących popełnić samobójstwo z inspiracji stron internetowych są tak zwane **kluby samobójców, czyli specjalne fora dyskusyjne, blogi, miejsca w sieci poświęcone tematyce samobójstw, sposobów ich popełniania i dyskusjom na ten temat.** Z takimi stronami spotykała się 17-letnia Carina Stephenson. W 2005 roku, w maju, dziewczyna powiesiła się w domu w Branton, w Anglii pod wpływem forów internetowych, których była stałą bywalczynią. Carina zaprzyjaźniła się na niektórych stronach z kilkoma dziewczynami. Razem planowały jak popełnić samobójstwo. Po śmierci Cariny jej mama zaangażowała się w wychwytywanie i usuwanie stron internetowych podpowiadających metody na popełnianie samobójstwa[46].

[43] http://www.se.pl/wydarzenia/kronika-kryminalna/trzcianka-w-internecie-znalazla-przepis-na-smierc_142313.html, data dostępu 18.04.2011.

[44] http://www.newsweek.pl/artykuly/samobojstwa-pl,22650,1, data dostępu 11.04.2011..

[45] http://www.trojmiasto.pl/wiadomosci/Samobojcza-proba-wedlug-instrukcji-z-Internetu-n32041.html, data dostępu 22.04.2011.

[46] http://dziecko.onet.pl/60268,0,11,dzieciece_pokoje_smierci,1,artykul.html, data dostępu 18.04.2011.

43 Na forach internetowych można znaleźć charakterystyczne grupy, z którymi Carina na pewno również miała styczność. Są to tak zwani ,,podszeptywacze śmierci" i ludzie zawierający ,,pakty śmierci". K. Hawton, psychiatra na Uniwersytecie w Oksfordzie uważa, iż **,,podszeptywacze" to osoby, które na forach internetowych o samobójstwach czują się ,,jak ryba w wodzie", ponieważ satysfakcję daje im przyglądanie się cierpieniu innych osób, sprawia im to nawet przyjemność. Jak twierdzi oksfordzki psychiatra, badania pokazują, że ,,podszeptywacze" to ludzie, którzy często nie mają pojęcia, czym są myśli samobójcze.**

44 **DOBRE PRAKTYKI**
zapobieganie

Organizacja Samaritans od lat dąży do tego, by Internet stał się dla ludzi miejscem bezpiecznym, zwłaszcza dla tych ,,na krawędzi". Ich zdaniem ,,podszeptywacze" to osoby, które mogą na początku odciągać ludzi od samobójstw, mając na celu dobro innych. Później jednak sami pod wpływem forów i innych osób dochodzą do wniosku, że samobójstwo jest jedynym rozwiązaniem wszelkich problemów i nakłaniają użytkowników forów do targnięcia się na własne życie. Lista osób, które są niebezpieczne dla osoby będącej przed decyzją o ,,ostatecznym kroku" jest jednak dłuższa. Kolejnym rodzajem są **ludzie zawierający pakty. Są to osoby, które pragną przejść przez akt samobójczy w towarzystwie, z jakąś inną, często obcą osobą. Umawiają się z innymi forumowiczami na popełnienie samobójstwa, piszą ogłoszenia w Internecie, a następnie spotykają się ze swoimi „partnerami" w rzeczywistości, by zakończyć swe życie razem**. We wrześniu 2010 roku taki przypadek miał miejsce w Wielkiej Brytanii, gdzie Joanne Lee napisała ogłoszenie na jednym z forów internetowych o tematyce samobójczej w celu znalezienia osoby, która razem z nią zabiłaby się. Dziewczyna oczekiwała, że ,,partner" będzie posiadaczem auta i pomoże jej dotrwać do końca. Na post odpisał Stephen Lumb. Kilka dni później parę znaleziono w samochodzie otrutą gazem[47].

45 Seria samobójstw związana z serwisami społecznościowymi zaczęła się również w 2007 roku w Bridgend, w Walii. Tylko w 2007 roku powiesiło się tam 13 osób. Byli to ludzie w wieku do 26 roku życia. W 2008 roku 19-letnia Angie Fuller wybrała podobny sposób do trzynastu wcześniej wymienionych samobójców, powiesiła się. Wszystkie osoby, które popełniły akt samobójczy znały się z Internetu, z portali społecznościowych[48].

46 Kluby samobójców swój początek tak naprawdę mają w Japonii, gdzie skala samobójstw to 30 tysięcy rocznie, a sam akt jest czynem honorowym. W 2000 roku zarejestrowano tam pierwszy przypadek samobójstwa z inspiracji Internetu. Do dnia dzisiejszego internetowe samobójstwa i pakty samobójcze stały się dość popularne. W 2005 roku w Kraju Kwitnącej Wiśni przez zmowę internautów paktom poddało się 91 osób[49].

47 Przykładem tego, jak przypadkowo można uratować czyjeś życie, jest historia gimnazjalisty z Katowic z 2007 roku. Nastolatek podczas korzystania z czatu spostrzegł nick jednej z chatowiczek – ,,samobójpopeł". Po krótkiej rozmowie okazało się, że jest to dziewczyna, która od jakiegoś czasu ma myśli samobójcze i zastanawia się nad samobójstwem. Sprawą natychmiast zajęła się policja. Jak ustalono, komputer dziewczyny znajdował się w Siemionie,

[47] http://dziecko.onet.pl/60268,0,11,dzieciece_pokoje_smierci,3,artykul.html, data dostępu 18.04.2011.

[48] http://wiadomosci.wp.pl/kat,1356,title,14-ofiara-internetowego-kultu-samobojcow,wid,9634089,wiadomosc.html, data dostępu 22.04.2011.

[49] http://www.rp.pl/artykul/87210.html, data dostępu 22.04.2011.

a nie Katowicach jak twierdziła internautka. Policjanci, którzy odwiedzili dziewczynę w jej rodzinnym domu dowiedzieli się, że młoda kobieta chce się zabić. Dziewczyna została natychmiast skierowana do szpitala w Czeladzi. I tam otrzymała profesjonalną pomoc[50].

48 Samobójstwa, o których słyszymy, są w wielu wypadkach również nagrywane i transmitowane na żywo w Internecie. Jedną z takich ,,transmisji" (2008 rok) przeżyli użytkownicy serwisu Justin TV, którzy obejrzeli 19-letniego Abrahama K. Biggsa połykającego dużą ilość tabletek. Większość myślała, że jest to przede wszystkim niesmaczny żart, ale po kilku godzinach filmiku i dotarciu na miejsce ekipy medycznej okazało się, że chłopak popełnił samobójstwo, do którego wcześniej namawiali go koledzy[51].

49 Podobnie było w 2010 roku z 24-letnim Japończykiem, mieszkającym w miejscowości Sendai. Młody mężczyzna zaczął umieszczać komentarze dotyczące jego pracy. W pewien poranek na portalu Ustream zamieścił filmik ,,na żywo". Na filmiku chłopak wchodzi na swój balkon i wiesza się. Policja o samobójstwie została poinformowana przez użytkowników serwisu[52].

50 **NOWE ZJAWISKA AUTODESTRUKCYJNE**

Warto w tym miejscu wspomnieć również o zjawisku łączącym się z samobójstwami jakim jest hikikomori. **Hikikomori definiowane jest jako skrajne wycofanie się z życia społecznego. Przejawia się:**

- **niewychodzeniem ze swojego pokoju, domu przez dłuższy okres (zaczynając od miesięcy, kończąc na latach),**
- **porozumiewaniu się z innymi ludźmi tylko za pomocą mediów (telefon, Internet),**
- **unikaniem bezpośredniego kontaktu z innymi ludźmi (twarzą w twarz).**

Zjawisko swoje początki ma w Japonii. Badacze hikikomori datują je na lata 70. XX wieku. Rozwój mediów przekształcił unikanie szkoły w niekontaktowanie się w ogóle z innymi ludźmi. Hikikomori występuje przeważnie wśród młodzieży. Zjawisko jest odpowiedzią młodego człowieka na stawiane mu wymagania głównie dotyczące szkoły, przyszłej kariery zawodowej i pozycji w hierarchii społecznej[53].

51 W Polsce pierwszy przypadek hikikomori datowany jest na rok 2001. Przypadek licealisty z hikikomori odkrył psychiatra M. Krzystanek z Katowic. Do gabinetu lekarza zgłosiła się matka chłopca. Według jej relacji chłopiec przestał wychodzić z domu. Trwało to ponad dwa lata. Kobieta przyznała, że chłopiec był dobrym uczniem. Decyzję o niewychodzeniu z domu licealista powziął przed zakończeniem roku szkolnego w pierwszej klasie.

52 Jak twierdzi T. Saito, choroba ta spowodowana jest przede wszystkim zbytnim przywiązaniem dziecka do matki. Najczęściej ta specyficzna więź wytwarza się między matką a synem. Drugim decydującym czynnikiem jest presja otoczenia, oczekiwania w stosunku do młodej osoby związane z najlepszymi studiami, przyszłym prestiżowym zawodem. Połączenie tych dwóch czynników

[50] http://wiadomosci.gazeta.pl/wiadomosci/1,61085,4670446.html, data dostępu 18.04.2011.

[51] http://pclab.pl/news34462.html, data dostępu 23.04.2011.

[52] http://www.pomorska.pl/apps/pbcs.dll/article?AID=/20101110/KRAJSWIAT/422903430, data dostępu23.04.2011.

[53] http://www.poradnia.pl/choroby/choroby-cywilizacyjne/1636-hikikomori-syndrom-wycofania-spolecznegp, data dostępu 22.04.2011.

OPIS ZJAWISKA

DOBRE PRAKTYKI

powoduje ucieczkę młodego człowieka do świata wirtualnego[54].

53 Osoba, która jest wplątana w zjawisko hikikomori, by wyzdrowieć zostaje poddana terapii podobnej do terapii uzależnień. Skuteczność tej metody to 70 %, ale przypadki które po terapii wracają do zamykania się na świat to aż 30%[55].

54 Na początku 2011 roku w polskich kinach pojawił się film Jana Komasy ,,Sala samobójców" obrazujący zjawisko hikikomori oraz następstwa decyzji zamknięcia się w świecie wirtualnym. Główny bohater to Dominik, licealista, który po ośmieszeniu przez szkolnych kumpli w świecie rzeczywistym i wirtualnym odgradza się od ludzi i korzystając z Internetu natrafia na dziewczynę po próbie samobójczej, która wprowadza go do tak zwanej sali samobójców – wirtualnego miejsca, w którym gromadzą się ludzie zmęczeni życiem. Pod wpływem świata wirtualnego Dominik w końcu popełnia samobójstwo[56].

55 Niepokojąca jest reakcja młodych ludzi na treści zamieszczone w Internecie. Jan Komasa, przygotowując się do napisania scenariusza „Sali samobójców", opisuje w wywiadzie, jak przyglądał się internetowym szykanom nastolatków, którzy nie widzą problemu, pisząc komuś: „idź się zabij". Wspomina wpis dziewczyny, która deklarowała, że popełni samobójstwo i natychmiastowe komentarze: „koniecznie zamieść wideo" albo: „jednego świra mniej"[57].

56 Film porusza jeszcze jedną kwestię związaną z hikikomori i samobójstwami. Jest nią cyberprzemoc.

57 Osoby zastraszające innych w ten sposób czują się bezkarne, ponieważ sieć jest anonimowa. Ich cel, jakim jest obrażenie i zaszczucie innej osoby, jest osiągnięty z większą satysfakcją niż w świecie realnym dzięki ogromnej liczbie ludzi, do których dociera prześmiewczy materiał. Ponadto łatwo jest obrażać inną osobę, nie stając z nią twarzą w twarz[58].

58 **ZAPOBIEGANIE ZACHOWANIOM SAMOBÓJCZYM WŚRÓD MŁODZIEŻY**

Programy prewencyjne powinny respektować pomoc rodzicom w opiece nad dziećmi, podniesienie poziomu edukacji, pomoc w rozwiązywaniu nieporozumień a także działania mające na celu walkę z dyskryminacją, przemocą i uzależnieniami.

59 W realizacji działań profilaktycznych niebagatelne jest zidentyfikowanie osób z predyspozycjami do popełnienia samobójstwa. To znaczy takich, które mają objawy depresyjne, specyficzne cechy osobowości, pochodzą ze środowisk zdezorganizowanych lub patologicznych, w których zaniedbano dobro i istotne potrzeby dziecka[59]. W realizacji tego celu pomocne mogą być narzędzia monitorujące i badania przesiewowe osób z grup ryzyka. Opracowano wiele narzędzi do zbadania ryzyka zachowań samobójczych, na przykład: Skala Poczucia Beznadziejności Becka, Miara Dziecka Zbędnego, Kwestionariusz Orientacji

[54] http://wiadomosci.onet.pl/kiosk/kraj/narkomani-internetu,3,4209612,kiosk-wiadomosc.html, data dostępu 22.04.2011.

[55] http://www.focus.pl/cywilizacja/zobacz/publikacje/hikikomori/, data dostępu 22.04.2011.

[56] http://www.bazafilmowa.pl/pl/bpf/nadeslanenewsy/~14/_20725, data dostępu 22.04.2011.

[57] B. Dobroch, M. Kuźmiński, *Tyrania wizerunku*, „Tygodnik Powszechny", nr 13/2011, s. 38.

[58] http://gospodarka.gazeta.pl/gospodarka/1,58480,3901940.html, data dostępu 22.04.2011.

[59] Por. G. Durka, *Samobójstwa i jego przyczyny*, w: S. Bębas, (red.), *Oblicza patologii społecznych*, Wyd. Wyższej Szkoły Handlowej, Radom 2011, s. 419.

Samobójczej[60]. Wszystkie wymienione narzędzia stosowane są w Stanach Zjednoczonych.

60 Kolejnym istotnym dzianiem jest edukacja odpowiedzialnych za bezpieczeństwo dzieci i młodzieży, czyli rodziców i nauczycieli. Powinni zdobyć wiedzę na temat czynników ryzyka samobójstwa, a także zdać sobie sprawę z pozytywnej roli, jaką mogą pełnić w zapobieganiu samobójstwom[61]. Podstawą takich programów mogą być specjalne szkolenia dla rodziców, psychologów, pedagogów, nauczycieli, ale także pracowników służb społecznych.

61 Ważnym elementem profilaktyki wobec osób zagrożonych popełnieniem samobójstwa jest rozmowa. E. Jakubowicz zwraca uwagę, że podczas rozmowy z dzieckiem, nastolatkiem należy stworzyć atmosferę zaufania, aby czuł, że jego problem jest traktowany poważnie, w ten sposób mógł szczerze wyrazić swoje zamierzenia i uczucia. Nauczyciel powinien zachęcić ucznia do konsultacji z psychologiem i pomóc mu uzyskać odpowiednie wsparcie[62].

62 Innem ważnym działaniem prewencyjnym są programy, warsztaty i zajęcia dla dzieci i młodzieży. Najlepiej, aby ich tematem było zdrowie psychiczne i radzenie sobie w trudnych sytuacjach, ponieważ takie zajęcia mogą pomóc w pozytywnym pokonywaniu kryzysów w wieku dojrzewania i dorosłości[63].

63 Inną propozycją tematu może być radzenie sobie ze stresem, którego codziennie doświadczają nastolatki w szkole i poza nią.

64 Kolejnymi działaniami są ośrodki interwencji kryzysowej, czy specjalne infolinie dla osób przeżywających kryzys i załamanie. Na ich łączach wykwalifikowana kadra oczekuje potrzebujących osób, aby udzielić im psychicznego wsparcia.
Ponadto media, zważywszy na siłę, z jaką oddziałują na dzieci i młodzież, powinny odpowiedzialnie przekazywać treści medialne. Muszą kierować się wskazówkami Światowej Organizacji Zdrowia WHO, opracowanymi dla środków masowego przekazu, dotyczącymi sposobu informowania społeczeństwa o zachowaniach autodestrukcyjnych[64].

65 Udzielenie pomocy osobie po próbach samobójczych powinno zacząć się od:

- oceny, w jakim stopniu próba była przypadkowa, a w jakim miała na celu usiłowanie pozbawienia się życia,
- oceny, jakie jest prawdopodobieństwo powtórzenia się jej,
- ustalenie motywów podjęcia się jej,
- interwencja w środowisku rodzinnym, rówieśniczym oraz szkolnym,
- rozważenie leczenia szpitalnego bądź laboratoryjnego,
- skierowanie osoby do poradni specjalistycznej[65].

[60] Por. C. Fox, K. Howton, *Jak – dlaczego – kiedy rozmawiać z młodymi zagrożonymi samobójstwem*, Wyd. Fraszka Edukacyjna Sp. z o. o., Warszawa 2009, s. 41–45.

[61] A. Młodożeniec, *Uwarunkowania zachowań samobójczych dzieci i młodzieży – cz. II*, Remedium, 9/2009, s. 2.

[62] Por. E. Jakubowicz, *Dlaczego dzieci odbierają sobie życie?,* „Psychologia w Szkole", 1/2011, s. 146.

[63] A. Młodożeniec, *Uwarunkowania zachowań samobójczych dzieci i młodzieży – cz. II*, Remedium 9/2009, s. 3.

[64] Por. E. Jakubowicz, *Dlaczego dzieci odbierają sobie życie?,* „Psychologia w Szkole", 1/2011, s. 83.

[65] J. Kula- Lic, *Problem samobójstw wśród dzieci i młodzieży*, „Problemy Opiekuńczo-Wychowawcze", Instytut Rozwoju Służb Społecznych, Warszawa, 2009, 6, s. 22.

Czynnikami zapobiegającymi i zmniejszającymi ryzyko samobójstwa są:

- towarzyskość ojca i matki,
- akceptacja rodziców,
- wysoka jakość małżeństwa,
- religijność,
- społeczne wsparcie,
- rozległa sieć kontaktów społecznych,
- wysoka siła ego,
- wysoki poziom samooceny,
- stany spokojnego nastroju,
- nastrój szczęścia,
- zaprzeczenie jako mechanizm obronny,
- ,,przemieszczanie" jako styl radzenia sobie,
- ,,przezwyciężanie przeszkód" jako styl radzenia sobie[66].

73 **PODSUMOWANIE**

Podjęcie próby samobójczej przez młodą osobę jest częstsze niż u osoby dorosłej. Mniej więcej 10% młodzieży decyduje się na kolejną próbę samobójstwa w ciągu roku[67].

74 Ryzyko podjęcia kolejnej próby samobójczej po poprzedniej jest ogromne. Ważna jest zatem długa hospitalizacja w oddziale psychiatrycznym z możliwością wrócenia do szkoły, wywiady z rodzicami, ocena dalszego przebiegu zachowania dorastającej osoby, dostosowanie środowiska do zmian poprawiających sytuacje młodego samobójcy[68].

75 Należy pamiętać, że osoba planująca samobójstwo pragnie kontaktu z drugim człowiekiem, uczucia ze strony rodziny i przyjaciół, akceptacji, wysłuchania. Niekiedy może się okazać, że czas i uwaga dla innych jest czymś najcenniejszym, czym możemy obdarować drugiego człowieka.

---

[66] Por. B. Hołyst (red.), *Samobójstwo,* Polskie Towarzystwo Higieny Psychicznej, Warszawa, 2002, s. 141.

[67] A. Młodożeniec, J. Janiak, *Uwarunkowania zachowań samobóczych dzieci i młodzieży – cz. II*, Remedium 9/2009, s. 1.

[68] J. Komender, *Zapobieganie próbom samobójczym podejmowanym przez dzieci i młodzież,* w: B. Hołyst, M. Staniaszek (red.), *Samobójstwo. Materiały z I Konferencji Suicydologicznej w Łodzi w dniach 24—25.11.1995 r.*, Polskie Towarzystwo Higieny Psychicznej, Warszawa- Łódź, 1995, s. 96.

BIBLIOGRAFIA:

Bigo Ł., *Samobójstwa w Internecie – łatwo znaleźć, łatwiej zapobiec*, http://www.idg.pl/news/147397/Samobojstwo.w.Internecie.latwo.znalezc.latwiej.zapobiec.html, data dostępu 02.01.2010.

Carr A., *Depresja i próby samobójcze młodzieży. Sposoby przeciwdziałania i reagowania*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2004.

Carr A., *Depresja i próby samobójcze wśród młodzieży*, Biblioteka Wychowawcy, Gdańsk 2008.

Depresja, http://encyklopedia.pwn.pl/haslo.php?id=3891882, data dostępu 17.02.2011.

Dobroch B., Kuźmiński, *Tyrania wizerunku*, „Tygodnik Powszechny" 13/2011.

Durka G., *Samobójstwa i jego przyczyny*, w: S. Bębas, (red.), *Oblicza patologii społecznych*, Wyd. Wyższej Szkoły Handlowej, Radom 2011.

Durkheim E., *Samobójstwo. Studium z socjologii*, Oficyna Naukowa, Warszawa 2006.

Fox C., Hawton K., *Zachowania autodestrukcyjne młodzieży – szkoła bezradna?*, Fraszka Edukacyjna, Warszawa 2009.

Fox C., Howton K., *Jak – dlaczego – kiedy rozmawiać z młodymi zagrożonymi samobójstwem*, Fraszka Edukacyjna, Warszawa 2009.

Hołyst B. (red.), *Samobójstwo,* Polskie Towarzystwo Higieny Psychicznej, Warszawa 2002.

Hołyst B., *Suicydologia*, Wydawnictwo Prawnicze LexisNexis, Warszawa 2001.

Hołyst B., *Wiktymologia*, Warszawa 2003.

Jabłoński J., *Młodzi samobójcy są wśród nas, czy potrafimy ich rozpoznać?,*w: B. Hołyst (red.), *Samobójstwo*, Polskie Towarzystwo Higieny Psychicznej, Warszawa 2002.

Jakubowicz E., *Dlaczego dzieci odbierają sobie życie?,* „Psychologia w Szkole", 1/2011.

Jarosz M., *Samobójstwa. Ucieczka przegranych*, Wydawnictwo Naukowe PWN, Warszawa 2004.

Jędrzejko M., *Śmierć w sieci. Modelowanie zachowań agresywnych w grach komputerowych i sieciowych,* w: S. Bębas, J. Plis, J. Bednarek (red.), *Patologie w cyberprzestrzeni*, Wyd. WSzH w Radomiu, Radom 2012.

Komender J., *Zapobieganie próbom samobójczym podejmowanym przez dzieci i młodzież,* w: B. Hołyst, M. Staniaszek (red.), *Samobójstwo. Materiały z I Konferencji Suicydologicznej w Łodzi w dniach 24—25.11.1995*, Polskie Towarzystwo Higieny Psychicznej, Warszawa- Łódź 1995.

Kubin A., *W trosce o emocjonalną niezależność*, „Edukacja i Dialog", Warszawa, 5/2007.

Kula-Lic J., *Problem samobójstw wśród dzieci i młodzieży*, „Problemy Opiekuńczo-Wychowawcze", Instytut Rozwoju Służb Społecznych, Warszawa, 6/2009.

Młodożeniec A., *Uwarunkowania zachowań samobójczych dzieci i młodzieży – cz. II*, „Remedium", 9/2009.

Młodożeniec M., Janiak J., *Uwarunkowania zachowań samobójczych dzieci i* młodzieży – cz. I, „Remedium", 7/8/2009, Państwowa Agencja Rozwiązywania Problemów Alkoholowych i Fundacja ETOH.

Mroziak B. [przekł. z jęz. ang.], *Zapobieganie samobójstwom. Poradnik dla pracowników mediów*, Światowa Organizacja Zdrowia, Genewa-Warszawa 2003, http://www.who.int/mental_health/prevention/suicide/en/suicideprev_media_polish.pdf, data dostępu 24.02.2011.

Obuchowska I., *Psychologiczne aspekty dojrzewania*, w: A. Jaczewski, B. Woyna-

rowska (red.), *Dojrzewanie*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1982.

Pospiszyl I., *Patologie społeczne. Resocjalizacja*, Wyd. Naukowe PWN, Warszawa 2008.

Samobójstwo, http://www.superja.pl/node/1835, data dostępu 17.02.2011.

Szulc M. (red.), *Popularna Encyklopedia Powszechna*, Wydawnictwo Pinnex, Kraków 1997.

Tryburcy M., *Samobójstwa młodych – czy zawsze nieprzewidywalne?*, http://www.przyjaciele.org/czytelnia.php?id=6, data dostępu 28.02.2011.

Wolański N., *Dojrzewanie jako etap w rozwoju osobniczym człowieka*, w: Jaczewski A., Woynarowska B. (red.), *Dojrzewanie*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1982.

Wróblewska A., *Charakterystyka młodzieży w wieku gimnazjalnym*, http://sod.ids.czest.pl/publikacje2/l1117/l1117.pdf, data dostępu 05.03.2011.

Zajączkowski K., *Profilaktyka zachowań dewiacyjnych dzieci i młodzieży*, Toruń 1998.

STRONY INTERNETOWE:

http://arstechnica.com/old/content/2008/04/suicide-searches-produce-disturbing-unsurprising-results.ars, data dostępu 04.01.2010.

http://dziecko.onet.pl/60268,0,11,dzieciece_pokoje_smierci,1,artykul.html, data dostępu 18.04.2011.

http://dziecko.onet.pl/60268,0,11,dzieciece_pokoje_smierci,3,artykul.html, data dostępu 18.04.2011.

http://gospodarka.gazeta.pl/gospodarka/1,58480,3901940.html, data dostępu 22.04.2011.

http://pclab.pl/news34462.html, data dostępu 23.04.2011.

http://wiadomosci.gazeta.pl/wiadomosci/1,61085,4670446.html, data dostępu18.04.2011.

http://wiadomosci.onet.pl/kiosk/kraj/narkomani-internetu,3,4209612,kiosk-wiadomosc.html, data dostępu 22.04.2011.

http://wiadomosci.wp.pl/kat,1356,title,-14-ofiara-internetowego-kultu-samobojcow,wid,9634089,wiadomosc.html, data dostępu 22.04.2011.

http://www.bazafilmowa.pl/pl/bpf/nadeslanenewsy/~14/_20725, data dostępu 22.04.2011.

http://www.focus.pl/cywilizacja/zobacz/publikacje/hikikomori/, data dostępu 22.04.2011.

http://www.newsweek.pl/artykuly/samobojstwa-pl,22650,1, data dostępu 11.04.2011.

http://www.polskieustawy.com/norms.php?actid=474&norm=151&lang=48&adate=20061220&head=0 data dostępu 24.02.2011.

http://www.polskieustawy.com/norms.php?head=0&actid=474&adate=20061220&norm=207&lang=48#vor data dostępu 24.02.2011.

http://www.pomorska.pl/apps/pbcs.dll/article?AID=/20101110/KRAJSWIAT/422903430, data dostępu 23.04.2011.

http://www.poradnia.pl/choroby/choroby-cywilizacyjne/1636-hikikomori-syndrom-wycofania-spolecznegp, data dostępu 22.04.2011.

http://www.rp.pl/artykul/87210.html, data dostępu 22.04.2011.

http://www.se.pl/wydarzenia/kronika-kryminalna/trzcianka-w-internecie-znalazla-przepis-na-smierc_142313.html, data dostępu 18.04.2011.

http://www.trojmiasto.pl/wiadomosci/Samobojcza-proba-wedlug-instrukcji-z-Internetu-n32041.html, data dostępu 22.04.2011.

http://www.tvn24.pl/-1,1693976,0,1,trzy-lata-za-uporczywe-i-zlosliwe-nekanie,wiadomosc.html, data dostępu 28.02.2011.

SZCZEGÓŁOWY
PROGRAM SZKOLENIA

Anna Andrzejewska

PROGRAM KSZTAŁCENIA - ZAGROŻENIA ZDROWIA PSYCHICZNEGO I FIZYCZNEGO	
Sposób realizacji	Warsztat
Materiały	**Materiały dydaktyczne dla uczestników szkolenia składają się z:** materiały szkoleniowe dotyczące zagrożeń zdrowia psychicznego i fizycznego oraz cyberprzemocy;
Treści merytoryczne	**blok tematyczny: (8h dydaktycznych)** Dolegliwości wzroku, Zespół RSI, Dolegliwości układu kostno-szkieletowego, Zespół Uzależnienia od Internetu Definicje Skala zjawisk związanych z zagrożeniami dla mózgu Rozpoznanie i objawy Dobre praktyki Cyberprzemoc Istota i charakterystyka cyberprzemocy Identyfikacja cyberprzemocy Skala i zasięg zjawiska Objawy świadczące o występowaniu cyberprzemocy Charakterystyka ofiary i sprawcy cyberprzemocy Zagrożenie samobójstwem wśród młodzieży Charakterystyka zjawiska hikikomori
Obszary	**Efekty kształcenia**
Wiedza zdobyta w czasie zajęć	W wyniku przeprowadzonych zajęć, Uczestnik powinien być w stanie: • wymienić ogólne podstawy teoretyczne dotyczące zagrożeń zdrowia psychicznego i fizycznego oraz cyberprzemocy; • rozumieć uwarunkowania, prawidłowości oraz mechanizmy dotyczące zagrożeń zdrowia psychicznego i fizycznego oraz cyberprzemocy; • orientację stanu i zasięgu zagrożeń zdrowia psychicznego i fizycznego oraz cyberprzemocy;
Umiejętności zdobyte w czasie zajęć	zdobyć umiejętności w zakresie: • diagnozowania przyczyn, przebiegu, objawów, skutków zagrożeń zdrowia psychicznego i fizycznego oraz cyberprzemocy; • przeciwdziałania i realizowanie profilaktyki w zakresie dotyczącym zagrożeń zdrowia psychicznego i fizycznego oraz cyberprzemocy; • doskonalienia niezbędnych kompetencji społeczno-wychowawcze w zakresie zagrożeń zdrowia psychicznego i fizycznego oraz cyberprzemocy.

Forma zajęć	Zajęcia grupowe, analiza realizowanych zadań w zespołach, studia indywidualnych przypadków dotyczące zagrożeń zdrowia psychicznego i fizycznego.
Metody prowadzenia zajęć	Metody warsztatowe. Wykład, ćwiczenia aktywizujące, grupowe, inscenizacja uzależnień i zagrożeń, burza mózgów, dyskusja, wymiana poglądów.
Zalecane ćwiczenia	Ćwiczenia 1-8 znajdujące się w module *Kształcenie*
Sprawdzenie efektów szkolenia	Ankiety, testy kompetencyjne, aktywny udział w dyskusji, odpowiedzi na pytania.

ZAGROŻENIA SPOŁECZNO-WYCHOWAWCZE

PEDOFILIA W SIECI

Anna Andrzejewska
Józef Bednarek

OPIS ZJAWISKA

ROZPOZNANIE OBJAWY

1 WPROWADZENIE

Sieć stała się wprost wymarzonym narzędziem dla przestępców oraz różnego rodzaju dewiantów. Dzieci nie przestrzegają podstawowych zasad bezpieczeństwa – bardzo często udostępniają obcym dane personalne i poprzez kontakt internetowy spotykają się z nieznajomymi w rzeczywistym świecie. Niechciane rozmowy na tematy związane z seksem i niechciana ekspozycja zdjęć pornograficznych są coraz powszechniejszym doświadczeniem młodych ludzi. Problem pedofilii i wykorzystywanie Internetu przez pedofilów poszukujących ofiar coraz wyraźniej jest dostrzegany w świadomości społecznej.

2 DEFINICJA

Pedofilia to stan, w którym jedynym lub preferowanym sposobem osiągania satysfakcji seksualnej jest kontakt z osobami nieposiadającymi trzeciorzędowych cech płciowych (z dziećmi).

3

Pedofilia należy do jednej z najczęściej spotykanych dewiacji seksualnych. Polega na skłonnościach do kontaktów seksualnych z dziećmi. Zakres tych kontaktów bywa zróżnicowany: dotykanie narządów płciowych, obnażanie ich, nakłanianie dziecka do pobudzania seksualnego sprawcy lub pobudzania samego siebie, stosunki seksualne, oralne, analne[1].

„Często zapominamy, że nie każdy pedofil to gruby, obleśny facet, przechadzający się w okolicach szkół czy placów zabaw, szukając swojej ofiary. Takie stereotypy krążą jeszcze w podświadomości rodziców, przez co usypiają ich czujność. Nie ma kryteriów co do wyglądu pedofila, jego koloru skóry, wieku, wykształcenia, poziomu zarobków, miejsca zamieszkania czy nawet płci”[2]. W Internecie pedofile mogą udawać, kogo chcą. Statystycznie pedofilia występuje wielokrotnie częściej u mężczyzn niż u kobiet (ok. 90% przypadków stanowią heteroseksualni mężczyźni).

4 ROPOZNANIE

Działalność tego typu przestępców w sieci może przejawiać się w:

- Tworzeniu, ściąganiu i rozpowszechnianiu pornografii dziecięcej.
- Tworzeniu stron internetowych skłaniających do zalegalizowania kontaktów seksualnych z dziećmi.
- Wyszukiwaniu potencjalnych ofiar za pomocą komunikatorów, poczty elektronicznej, chatroomów (program do pogawędek) itp.
- Pozyskiwaniu i wymienianiu się danymi osobowymi dzieci.
- Nawiązywaniu znajomości internetowej z zamiarem spotkania w realnym świecie.
- Wciąganiu dzieci w rozmowy o charakterze seksualnym.
- „Oswajaniu” dzieci z pornografią dziecięcą.
- Handlu dziećmi.

5

Naukowcy Uniwersytetu w New Hampshire ustalili, że ponad połowa ze złapanych przez wymiar sprawiedliwości posiadaczy pornografii dziecięcej, molestowała dzieci lub podejmowała takie próby[3].

[1] Por. Z. Lew-Starowicz, *Seks nietypowy*, Instytut Wydawniczy Związków Zawodowych, Warszawa 1988, s.141.

[2] J. Śpiewak, *Internetowe stereotypy*, „Niebieska Linia”, 1/2006, s. 7.

[3] *Possessing Internet Child Pornography is a Serious Crime with Serious Consequences, Study Finds*, http://www.unh.edu/news/news_releases/2005/june/em_050607study.html, data dostępu: 20.02.2013..

6 Przestępców przyciągają przede wszystkim dzieci zagubione, osamotnione, mające problemy w domu. Podsycając pretensje do rodziców i domowego życia, tworzą atmosferę „my przeciwko nim". Powstaje wtedy dystans pomiędzy dzieckiem a rodzicami, jednocześnie tworzy się przymierze dziecka z pedofilem[4].

7 Wielu rodziców wie o istnieniu takiego zagrożenia, natomiast wychodzi z założenia, że nie dotyczy to ich dzieci. Bardzo często nie dostrzegają niebezpieczeństwa, a tymczasem pedofil wchodzi wprost do pokoju dziecka, przez jego komputer. Źródłem informacji o dzieciach mogą być prowadzone przez nie blogi lub prywatne strony.

8 „Wzrost skali zjawiska oglądania, kolekcjonowania i posiadania pornografii dziecięcej prowadzi do wzrostu liczby dzieci wykorzystywanych seksualnie, ponieważ:

1. pewna część populacji tych, którzy oglądają, kolekcjonują i posiadają pornografię dziecięcą, po pewnym czasie zaczyna wykorzystywać seksualnie dzieci w świecie rzeczywistym,
2. związany z tym zjawiskiem wzrost popytu na nowe zdjęcia i filmy pornograficzne z udziałem dzieci prowadzi do werbowania większej liczby nowych dzieci, które padają ofiarą wykorzystywania seksualnego w procesie produkcji takich materiałów"[5].

9 Jednym z przejawów działalności pedofili jest tworzenie stron internetowych w celu upowszechniania nieprawdziwych informacji o ich działalności. Witryny te zazwyczaj nie zawierają jawnych treści pornograficznych, dlatego nie ma podstaw prawnych do ich usunięcia. Na stronach prezentowane są badania, z których między innymi wynika, „iż utrzymywanie stosunków seksualnych z dziećmi nie zawsze wywołuje u nich negatywne konsekwencje. Pojawiają się także zestawienia danych, które mają świadczyć o następującej współcześnie akceleracji rozwoju seksualnego młodych osób, co miałoby stanowić silny argument na rzecz obniżenia wieku dzieci, od którego podejmowanie z nimi aktywności seksualnej jest karalne"[6]. Osoby molestujące dzieci często przekonane są, że akty seksualne mają dla dziecka wartość edukacyjną[7].

10 Sieć umożliwia tym przestępcom szybsze, bezpieczniejsze i bardziej przystępne, niż w realnym świecie, nawiązywanie kontaktów z innymi pedofilami oraz wymianę posiadanych doświadczeń. „W trakcie pierwszych rozmów z dzieckiem pedofil często stara się ustalić dokładną lokalizację komputera w domu ofiary. Próbuje się dowiedzieć, z jakim prawdopodobieństwem któryś z domowników mógłby przypadkowo zobaczyć lub usłyszeć jego rozmowy z potencjalną ofiarą. Często stara się nakłonić dziecko, żeby usuwało z komputera wszelkie ślady ich kontaktów, ponieważ (...) zapis takich rozmów mógłby dostarczyć policji użytecznego materiału dowodowego"[8].

11 Internet stał się narzędziem ułatwiającym sprawcom poszukiwanie nowych ofiar, zbieranie o nich informacji, a także wymienianie się uzyskanymi danymi. Sieć umożliwia wirtualny kontakt

---

[4] P. Aftab, *Internet a dzieci. Uzależnienia i inne niebezpieczeństwa*, Wyd. Prószyński i S-ka, Warszawa 2003, s. 150.

[5] J. Carr, *Internet a wykorzystywanie seksualne dzieci i pornografia dziecięca*, http://www.dzieckokrzywdzone.pl /UserFiles/File/kwartalnik13/13_carr.pdf, data dostępu: 15.01.2013.

[6] A. Izdebska, *Aktywność pedofilów w Internecie*, http://www.stoppedofilom.pl/index.php?s=artykuly&id=18, data dostępu: 10.02.2013.

[7] A. Zwoliński, *Obraz w relacjach społecznych*, Wydawnictwo WAM, Kraków 2004, s. 335.

[8] J. Carr, *Internet a wykorzystywanie seksualne dzieci i pornografia dziecięca*, http://www.dzieckokrz ywdzone.pl/UserFiles/File/kwartalnik13/13_carr.pdf, data dostępu: 04.01.2013.

z wieloma osobami naraz. Pedofile do kontaktów z dziećmi wykorzystują między innymi: serwisy BBS (*Bulletin Boards System*), grupy dyskusyjne – Usenet, e-maile, rozmowy online na IRC (*Internet Really Chat*), programy typu IM (*Instant Messanger*) – komunikatory czy sieć P2P (*Peer to Peer*), internetowe programy do wymiany plików.

12 Wyszukiwanie dzieci może odbywać się np. za pomocą różnych komunikatorów, gdzie do katalogu publicznego można dodać swoje dane. Doskonałym źródłem informacji są także wirtualne pamiętniki (blogi) publicznie dostępne w Internecie, jak również prywatne strony internetowe, prowadzone przez dzieci. Innym sposobem są serwisy ogłoszeniowe i randkowe, gdzie pedofile szukają ogłoszeń zamieszczanych przez małoletnich oraz umieszczają swoje anonse[9].

13 Pedofile, realnie zrzeszając się w wirtualnym świecie, często dokładają starań, by uniknąć możliwości bycia zidentyfikowanym. Ich witryny są zazwyczaj opatrzone hasłami, mają niewskazujące na zawartą treść adresy, a nade wszystko mają charakter efemeryczny. Adresy oraz serwery, na których są one umieszczane, ulegają częstym zmianom[10].

14 „Gdy pedofilowi uda się już nawiązać z dzieckiem więź, w treść rozmów stopniowo wprowadzany jest temat seksu. W tym celu nierzadko wykorzystywane są materiały z pornografią dziecięcą. Pokazując je dziecku, pedofil kształtuje w nim przekonanie, iż tego typu aktywność nie jest niczym złym i inne dzieci także się jej poddają”[11]. Pedofil ma na celu zapoznanie dziecka z praktykami seksualnymi przy jednoczesnym osłabieniu u niego wstydu i oporu. Doprowadzić to może z czasem do znieczulenia dziecka i w rezultacie spotkania z pedofilem.

15 Współczesnych rodziców trzeba uwrażliwić na sygnały wysyłane przez dziecko, na rozmowy prowadzone z małoletnimi o Internecie, wskazywać zalety i wady sieci, wtedy istnieje większa szansa, że dziecko dostrzeże szkodliwe intencje osób poruszających się w sieci oraz zrozumie zagrożenia wynikające z potencjalnej anonimowości użytkowników Internetu[12].

16 **BADANIA**

Pierwszymi badaniami dotyczącymi ryzyka kontaktów o charakterze seksualnym doświadczanych przez dzieci w Internecie były badania sondażowe przeprowadzone przez J. Mitchell, D. Filkenchor, J. Wolak w Stanach Zjednoczonych na przełomie 1999 i 2000 roku na ogólnokrajowej grupie N=1501 dzieci i młodzieży w wieku 10–17 lat. Pytania związane z wykorzystywaniem seksualnym dzieci poprzez Internet pogrupowano w trzech obszarach:

- **niechciana prezentacja materiałów pornograficznych** podczas przeszukiwania zasobów Internetu czy korzystania z poczty elektronicznej,
- **propozycje seksualne** – rozmowa dorosłego z dzieckiem online na tematy seksualne, czy też proponowanie kontaktu seksualnego,
- **agresywne propozycje seksualne** – propozycje o charakterze seksualnym online, za pośrednictwem regularnej poczty, telefonu komórkowego,

[9] K. Pospiszyl, *Geneza pedofilii*, http://www.stoppedofilom.pl/index.php?s=artykuly&id=9, data dostępu: 23.01.2013.

[10] A. Izdebska, *Aktywność pedofilów w Internecie*, http://www.stoppedofilom.pl/index.php?s=artykuly&id=18, data dostępu: 10.02.2013.

[11] Tamże.

[12] P. Olejnik, *Internet-niebezpieczeństwo dezintegracji osobowości dziecka?*, w: J. Izdebska, T. Sosnowski (red.), *Dziecko i media elektroniczne – nowy wymiar dzieciństwa*, t.2, Trans Humana, Białystok 2005, s. 130.

które mają na celu doprowadzenie do spotkania w świecie rzeczywistym.

17 Wyniki badań okazały się bardzo niepokojące i odbiły się szerokim echem w społeczeństwie oraz zainicjowały działania – nie tylko w Stanach Zjednoczonych, ale także w wielu innych krajach, na rzecz dzieci wykorzystywanych seksualnie.

18 Okazało się, że:

- 20% dzieci otrzymało w ciągu roku poprzedzającego badanie propozycję seksualną od nieznajomej osoby z sieci,
- 3% otrzymało agresywne propozycje seksualne,
- 25% wbrew woli dziecka zaprezentowano mu materiały pornograficzne,
- 25% dzieci przeżyło stres związany z ww. zgłaszanymi zdarzeniami.

19 W Polsce w ramach kampanii społecznej „Dziecko w sieci" Fundacja Dzieci Niczyje w 2004 roku przeprowadziła badania sondażowe na blisko 9000 dzieciach w wieku 12–17 lat, które także miały pokazać, jaka jest skala zjawiska związana z bezpieczeństwem dzieci w Internecie. Wyniki badań okazały się mocno niepokojące, gdyż:

- 87% dzieci podało obcemu swój adres e-mail (81% wielokrotnie),
- 64% dzieci podało obcemu swój numer telefonu (43% wielokrotnie),
- 42% dzieci podało obcemu adres zamieszkania (19% wielokrotnie),
- 44% dzieci przesłało obcemu swoje zdjęcie (34% wielokrotnie),
- aż blisko 22% dzieci nie informuje nikogo o spotkaniach z osobami poznanymi przez Internet[13].

[13] Fundacja Dzieci Niczyje, http://www.fdn.pl/files/?id_plik=7, data dostępu 02.02.2013.

Badania pokazały, że mimo iż większość dzieci słyszała o zagrożeniach, jakie czyhają na nie w Internecie, ich zachowania w sytuacji zagrożenia są nieracjonalne. Ważne jest podejmowanie wszelkich działań ze strony środowiska oświatowo-wychowawczego mających na celu wyjaśnianie dzieciom kwestii zagrożeń związanych z niewłaściwym korzystaniem z Internetu, zwłaszcza z kontaktami z nieznajomymi.

20 **ROZPOZNANIE PROBLEMU / OBJAWY**

Działania pedofila w sieci są mocno przemyślane i ukierunkowane na doprowadzenie do spotkania z ofiarą w świecie rzeczywistym, stąd trudności w identyfikacji zjawiska. Uwodziciel bardzo starannie planuje i realizuje drogę swojego postępowania wg pewnego rozpoznanego już schematu działania.

21 **Pierwszy etap działania – to nawiązanie znajomości z dzieckiem**. Najczęściej odbywa się to na czacie lub przez komunikatory. Uwodziciel podszywa się pod rówieśnika i powoli wciąga dziecko w znajomość. Ten etap może trwać długo, nawet kilka miesięcy. W tym czasie obserwuje swoją ofiarę, oswaja ją z tym, że jest on osobą dorosłą.

22 **Drugi etap działania – tworzenie relacji z dzieckiem**. Rozmowy z dzieckiem stają się coraz dłuższe i bardziej zażyłe. Pedofil poświęca dziecku czas, interesuje się rodziną, szkołą. Dorosłego interesują emocje dziecka, jego doświadczenia, zainteresowania, marzenia. Opowiada też o sobie, najczęściej w kontekście doświadczeń dziecka. Każde jego działanie na tym etapie jest bardzo starannie przemyślane i delikatne. Nie może on zaniepokoić i zrazić swojej ofiary. Interesuje się dzieckiem w sposób specjalny, podsyca w nim przekonanie, że rodzice go nie rozumieją, że tylko on może być jego przyjacielem, na którego dziecko może liczyć.

ROZPOZNANIE OBJAWY

Po pewnym czasie proponuje prezenty, czy nawet wsparcie finansowe. Dziecko stopniowo zaczyna ufać swojemu internetowemu „przyjacielowi" i powoli więź między nimi się zacieśnia.

23 **Trzeci etap działania – ocena ryzyka odkrycia znajomości**. Uwodziciel sprawdza sytuację dziecka w domu. Chce mieć pewność, że aktywność dziecka przy komputerze nie jest kontrolowana przez domowników. Chce, aby znajomość była tajemnicą, która nie wyjdzie na jaw. Dlatego też zadaje pytania, gdzie jest ustawiony komputer, kto z niego korzysta, czy dziecko jest kontrolowane przez rodziców itp.

24 **Czwarty etap działania – ukazanie dziecku wzajemności w relacji**. Jest to etap, w którym pedofil utwierdza dziecko w przekonaniu, że ich wzajemne relacje są wyjątkowe. Nawiązuje więź, która ma coraz bardziej intymny charakter. Powoli przechodzi do rozmów o zabarwieniu seksualnym. Zapewnia je o wzajemnym zaufaniu. Stopniowo kieruje uwagę na ciało, zadając przy tym pytania związane z seksem. W pewnym momencie znajomości pedofil przesyła dziecku pierwsze zdjęcia pornograficzne, początkowo łagodne. W ten sposób pedofil oswaja dziecko z cyberseksem.

25 **Piąty etap – dążenie do spotkania**. Pedofil zmierza do spotkania. Jeśli dziecko opiera się, pedofil posuwa się do szantażu. Może zażądać nagich zdjęć dziecka, a jeśli ich nie dostanie, grozi, że powiadomi rodziców o tej znajomości. Kiedy już je dostanie, zmusi dziecko do spotkania, grożąc opublikowaniem zdjęć.

26 **Kto jest najczęściej narażony na działanie internetowych pedofilów?**

ludzie młodzi, zagubieni, szukający przyjaciół

aktywnie korzystający z komputera

mający problemy w relacjach z najbliższymi

poszukujący nowych lub odmiennych doznań

mający trudności w nawiązywaniu kontaktów w świecie realnym

osoby z zaburzonym obrazem własnej tożsamości

poszukujący zainteresowania własną osobą lub uczucia ze strony innych

DOBRE PRAKTYKI

27 **DOBRE PRAKTYKI**

Warto zapoznać się z serwisami internetowymi, które dokładnie i jasno opisują problematykę bezpieczeństwa w sieci, jak również sposoby walki z czyhającymi na dzieci i młodzież zagrożeniami. Te serwisy to między innymi:

- www.dyzurnet.pl,
- www.dzieckowsieci.pl,
- www.interpatrol.pl,
- www.saferinternet.pl,
- www.republikadzieci.org.[14]14

ĆWICZENIA 10

[14] S. Wilczewski, M. Wrzód, Bezpieczny *komputer w domu. Chroń swój domowy komputer*, Wydawnictwo HELION, Gliwice 2007, s. 102.

BIBLIOGRAFIA:

Aftab P., *Internet a dzieci*. *Uzależnienia i inne niebezpieczeństwa*, Wyd. Prószyński i S-ka, Warszawa 2003.

Carr J., *Internet a wykorzystywanie seksualne dzieci i pornografia dziecięca*, http://www.dzieckokrzywdzone.pl/UserFiles/File/kwartalnik13/13_carr.pdf, data dostępu 15.01.2013.

Fundacja *Dzieci Niczyje*, http://www.fdn.pl/files/?id_plik=7, data dostępu 02.02.2013.

Izdebska A., *Aktywność pedofilów w Internecie*, http://www.stoppedofilom.pl/index.p hp?s= artykuly&id=18, data dostępu 10.02.2013.

Lew-Starowicz Z., *Seks nietypowy*, Instytut Wydawniczy Związków Zawodowych, Warszawa 1988.

Olejnik P., *Internet-niebezpieczeństwo dezintegracji osobowości dziecka?*, w: Izdebska J., Sosnowski T. (red.), *Dziecko i media elektroniczne-nowy wymiar dzieciństwa*, t.2, Trans Humana, Białystok 2005.

Pospiszyl K., *Geneza pedofilii*, http://www.stoppedofilom.pl/index.php?s=artykuly&id=9, data dostępu 23.01.2013.

Possessing Internet Child Pornography is a Serious Crime with Serious Consequences, Study Finds, http://www.unh.edu/news /news_releases/2 005/june/em_050607study.html, data dostępu 20.02.2013.

Śpiewak J., *Internetowe stereotypy*, „Niebieska Linia", 2006, nr 1.

Wilczewski S., Wrzód M., *Bezpieczny komputer w domu. Chroń swój domowy komputer*, Wydawnictwo HELION, Gliwice 2007.

Zwoliński A., *Obraz w relacjach społecznych*, Wydawnictwo WAM, Kraków 2004.

ZAGROŻENIA SPOŁECZNO-WYCHOWAWCZE

PORNOGRAFIA

Anna Andrzejewska
Józef Bednarek

OPIS ZJAWISKA

1 OPIS ZJAWISKA

Pojęcie „pornografia” wywodzi się z języka greckiego: *pórne* – nierządnica; *gráphein* – skrobać, rytować, rysować, pisać; *pornográphos* – piszący o nierządnicach[1]. Obecnie, **encyklopedyczne określenie pornografii dotyczy „pism, druków, filmów, wizerunków i innych przedmiotów wykonywanych i rozpowszechnianych w celu wywołania u odbiorcy podniecenia seksualnego”**[2]. Od lat trwają batalie o zdefiniowanie i uściślenie słowa pornografia. Problem polega na tym, że to, co dla jednych jest pornografią, dla innych może być erotyką bądź zachowaniem obscenicznym. Rozumienie tego pojęcia zmienia się w zależności od czasu i ma tyle znaczeń, ile krajów, umysłowości, obyczajów i systemów kulturowych[3].

2 Zasadniczym celem pornografii w sieci jest pobudzenie seksualne użytkownika. Narusza ona godność człowieka, stanowiąc tym samym formę przemocy. Jej konsumpcja rozbudza pożądanie seksualne i prowadzi do szukania coraz mocniejszych wrażeń, co w konsekwencji sprzyja rozwiązłości seksualnej, niszczącej małżeństwo. Propagując seks bez żadnych zobowiązań, utrudnia rozwój prawidłowych relacji między kobietą i mężczyzną.

3 Pornografia propaguje prymitywną wizję człowieka, którego zainteresowania mają się koncentrować na zaspokojeniu pożądliwości zmysłowej.

4 „Rozpowszechnianie treści pornograficznych w Internecie zasługuje na szczególną uwagę. Nie ze względu na charakter tych treści, ponieważ w zdecydowanej większości stanowią one odpowiednik tego, co dostępne jest w tradycyjnych mediach, ale ze względu na specyfikę związaną z funkcjonowaniem Internetu”[4].

5 J. Bednarek podzielił strony pornograficzne znajdujące się w sieci, na następujące rodzaje[5]:

strony zawierające galerie zdjęć pornograficznych, podzielone tematycznie;

zbiory małych filmików, które można zapisać na dysku osobistego komputera;

telekonferencje internetowe z intymnymi dialogami i przekazami wideo, tzw. *live sex;*

sklepy internetowe tzw. *sex shopy*, w których można zamówić filmy video oraz gadżety erotyczne.

Jednym z najbardziej kontrowersyjnych aspektów jest bardzo łatwa dostępność pornografii w sieci dla dzieci i młodzieży.

6 Wpływ pornografii na człowieka zależy bardzo często od wieku użytkownika, częstotliwości kontaktów, rodzaju używanych materiałów oraz samokontroli emocji. Im użytkownik jest młodszy, tym bardziej destrukcyjnie działają na niego treści jawnie seksualne. Wykorzystywane są tu niewiedza i niedojrzałość psychiczna dzieci. Kontakt z pornografią przerasta zdolności adaptacyjne dzieci i prowadzić może do przyswajania wypaczonej i sprymityzowanej

[1] W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, Świat Książki, Warszawa 1999, s. 399.

[2] A. Zwoliński, *Obraz w relacjach społecznych*, Wydawnictwo WAM, Kraków 2004, s. 343.

[3] Por. A. Krawulska-Ptaszyńska, *Psychospołeczne uwarunkowania korzystania z pornografii przez mężczyzn*, Bogucki Wydawnictwo Naukowe, Poznań 2003, s. 10.

[4] J. Warylewski, *Przestępstwa seksualne*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2001, s. 305.

[5] Por. J. Bednarek, *Zagrożenia w cyberprzestrzeni*, w: M. Jędrzejko (red.), *Patologie społeczne*, Wyższa Szkoła Humanistyczna w Pułtusku, Pułtusk 2006, s. 99.

wizji seksualności. Ten negatywny wpływ prowadzić może do błędnego rozumowania wstrzemięźliwości seksualnej, jako niesłużącej zdrowiu, co zapoczątkować może wcześniejsze kontakty seksualne dzieci.

7 Strony erotyczne dostępne w Internecie przedstawiają fałszywy obraz kobiecości i męskości. Ukazują seksualność w kategorii procesów instynktownych. Szczególnie tzw. twarda pornografia może doprowadzić u młodego człowieka do nieświadomego warunkowania i kojarzenia przyjemności z brutalnością i agresją. Ukazuje to uprzedmiotowienie kobiety, płeć żeńska przedstawiana jest „jako prowokująca aktywność seksualną, podległa mężczyźnie i uległa mu, gorsza od niego, bezbronna, ukrywająca swoje pożądanie”[6]. Natomiast mężczyzna „jawi się w pornografii jako »macho«, seksualny rekordzista, zdobywający prestiż i podziw dzięki sile fizycznej i seksualnej sprawności”[7]. Prowadzić to może do wzrostu akceptacji dla przemocy w kontaktach interpersonalnych, dominacji mężczyzny w tych relacjach, oziębłości i wrogich postaw panów wobec pań, a także podświadome zezwolenie płci męskiej na przemoc i gwałt wobec kobiet[8].

8 S. Kozak zaznacza, że osobowość człowieka składa się z pięciu głównych sfer: emocjonalnej, poznawczej, społecznej, moralnej i etycznej, a każda z nich już w dzieciństwie zostaje zagrożona przez pornografię[9]. Jest ona wyjątkowo niebezpieczna, ponieważ zostawia ślad w psychice na całe życie.

9 Ponadto pornografia może stać się przyczyną agresywnych postaw wobec kobiet. Dzieje się tak, ponieważ fałszuje ona obraz kobiety i mężczyzny. Kobieta w materiałach pornograficznych traktowana jest jako obiekt pożądania i poniżania. Zdaniem S. Kozaka oglądanie takich treści powoduje stworzenie wizerunku kobiety jako uległej i mającej satysfakcję ze stosowania wobec niej przemocy, co z kolei może prowadzić młodych chłopców do gwałtów na rówieśnikach. Dzięki temu mogą zaspokoić potrzeby wytworzone podczas oglądania zakazanych treści[10].

10 Kolejnym niebezpiecznym aspektem zainteresowania treściami pornograficznymi jest ryzyko uzależnienia, co z kolei staje się przyczyną problemów w stosunkach z partnerem, a jak zastrzega S. Kozak, osoby takie nie potrafią w przyszłości stworzyć normalnej rodziny i normalnego związku małżeńskiego[11]. Istnieje potrzeba przedsięwzięcia konkretnych działań, które uniemożliwią zaistnienie takiego stanu.

11 Co więcej, A. Chrzanowska powołuje się na badania, które wykazały, że osoby korzystające z pornografii częściej usprawiedliwiają sprawców napaści seksualnych, a winę przypisują ofiarom[12].

---

6 D. Kornas-Biela, *Niszczący wpływ pornografii*, „Wychowawca”, 5/2006, s. 42.

7 Tamże.

8 A. Krawulska-Ptaszyńska, *Psychospołeczne uwarunkowania korzystania z pornografii przez mężczyzn*, Bogucki Wydawnictwo Naukowe, Poznań 2003, s. 27.

9 Por. S. Kozak, *Patologie wśród dzieci i młodzieży*, Wyd. Difin, Warszawa 2007, s. 55.

10 Por. S. Kozak, *Patologie komunikowania w Internecie*, Wyd. Difin, Warszawa 2011, s. 188.

11 Por. S. Kozak, *Patologie wśród dzieci i młodzieży*, Wyd. Difin, Warszawa 2007, s. 55.

12 Por. A. Chrzanowska, *Surfowanie po goliźnie*, „Charaktery”, 9/2010, s. 30.

ROZPOZNANIE OBJAWY

12 Wobec prezentowanych obrazów, sytuacji erotycznych, dzieci pozostają bezbronne. Bardzo często nie potrafią okazać sprzeciwu. **Polskie badania wykazały, że 80% dzieci natrafiło w Internecie na materiały o treści pornograficznej, wcale ich nie szukając, a 41% dostawało e-maile z linkami do stron pornograficznych**[13]. Z drugiej strony pornografia to nowość dla dzieci, dlatego zdarza się i tak, że same szukają stron internetowych zawierających erotyczny materiał.

13 Pornografia prezentuje często różne formy zachowań dewiacyjnych, dostarczając instruktażu i sprzyjając ich rozpowszechnianiu. Jest wykorzystywana jako źródło pomysłów i doping przed podjęciem czynów przestępczych. Jest to szczególnie niebezpieczne w wypadku młodzieży, która nie ma jeszcze ukształtowanych form zaspokajania potrzeb seksualnych, a dewiacyjne obrazy narzucają patologiczne wzorce o dużej sile oddziaływania. Tym bardziej, że działa tu prawo pierwszych połączeń, na zasadzie którego znaczenie wczesnych doświadczeń jest większe niż następnych. Spełniają one rolę torującą i prowadzą do ukształtowania tendencji do zaspokajania potrzeby więzi z drugim człowiekiem, np. przez redukcję napięcia seksualnego, czasem dodatkowo przez zadawanie mu cierpienia[14].

14 Niezwykle przerażający jest fakt, że internetowa pornografia dziecięca często stanowi wstępną fazę, przygotowanie do kontaktu w świecie rzeczywistym i próbę wykorzystania małoletniego, ponieważ pedofile podczas rozmów na czatach podszywają się pod młode osoby, pozyskując zaufanie i dążąc do możliwości spotkania[15].

15 ROZPOZNANIE PROBLEMU, OBJAWY I DIAGNOZA

Problemem dla dorosłych, a ułatwieniem dla dzieci jest fakt, że cyberpornografia jest łatwo dostępna, a jak zaznacza P. Wallace wywiera ona inny wpływ niż jej odpowiednik w prawdziwym życiu, ze względu na odległość fizyczną, anonimowość, subiektywne poczucie bezpieczeństwa i brak lęku o konsekwencje w wirtualnej przestrzeni[16].

16 Pochodną pornografii internetowej jest nowe zjawisko zwane sextingiem, które polega na wysyłaniu, w szczególności przez młodzież, wiadomości multimedialnych o zabarwieniu erotycznym, na przykład nagich zdjęć[17]. Po dostaniu się materiału do sieci lub nieprzyjaciół, takie nieprzemyślane zachowanie może mieć tragiczne skutki, takie jak kac moralny, ośmieszenie i kpiny ze strony rówieśników, obraźliwe komentarze czy też nachalne propozycje seksualne.

17 Ze względu na dostępność pornografii w cyberprzestrzeni, zwłaszcza dla nieletnich, zjawisko to należy do jednych z najbardziej kontrowersyjnych zagadnień Internetu, dlatego zdaniem P. Wallace'a wymaga „regulacji prawnych mających doprowadzić do kontroli i ograniczenia jego zawartości"[18].

---

[13] J. Cent, *Nowe media a dzieci – dylemat rodziców*, w: M. Bogunia-Borowska (red.), *Dziecko w świecie mediów i konsumpcji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006, s. 92.

[14] J. Augustyn, *Wychowanie do integracji seksualnej*, Wydawnictwo M, Kraków 1994.

[15] J. Bednarek, *Zagrożenia w cyberprzestrzeni*, w: M. Jędrzejko (red.), *Patologie społeczne*, Wyższa Szkoła Humanistyczna im. Aleksandra Gieysztora, Pułtusk 2006, s. 101.

[16] Por. P. Wallace, *Psychologia Internetu*, Dom Wydawniczy Rebis, Poznań 2001, s. 210.

[17] G. Kudlak, *Sexting – od zabawy do przestępstwa*, w: S. Bębas, (red.), *Oblicza patologii społecznych*, Wyd. Wyższej Szkoły Handlowej, Radom 2011, s. 425.

[18] P. Wallace, *Psychologia Internetu*, Dom Wydawniczy Rebis, Poznań 2001, s. 207.

18 Przez kontakt z pornografią następuje erotyzacja psychiki dziecka, jego przedwczesne rozbudzenie seksualne, a to prowadzi do występowania treści seksualnych w marzeniach sennych, podejmowania zabaw erotycznych, „twórczości" o charakterze seksualnym (np. w postaci sporządzania wulgarnych napisów lub rysunków), wypowiedzi o treściach seksualnych (np. tzw. brzydkich dowcipów – śmiech ma na celu rozładowanie napięcia). Czasem podejmowane są prowokacyjne zachowania seksualne, w tym wobec rówieśników lub młodszych dzieci (dzieci naśladują zachowania seksualne dorosłych dostrzeżone w materiałach pornograficznych). Niektórzy, zwłaszcza dziewczęta, stają się podatni na uwiedzenie, oddają się mniej lub bardziej jawnej prostytucji, a potem w życiu dorosłym wykazują promiskuityzm i tendencje orgiastyczne, homoseksualne lub biseksualne. Ich psychoseksualny rozwój może zostać zaburzony w kierunku dewiacji seksualnych, np. pedofilii, transwestytyzmu, fetyszyzmu[19].

19 Pornografia przyczynia się do powiększenia problemu patologii seksualnych i związanych z tym czynów kryminalnych, dlatego że kontakt z nią pozbawia młodego człowieka odruchu wstydu, zażenowania i niesmaku w sytuacji odsłaniania własnej lub czyjejś intymności, co sprzyja tendencji do ekshibicjonizmu, utraty zahamowań przed czynami naruszającymi prywatność własną lub innych ludzi (np. ocieractwo, podglądanie).

20 DOBRE PRAKTYKI, PRZECIWDZIAŁANIE

Według badań S. Kozaka, rodzice stosunkowo rzadko wykazują aktywność ograniczającą zagrożenia związane z korzystaniem z komputera i Internetu przez dzieci. Efektywne uchronienie dzieci przed zagrożeniami Internetu wymaga wielu kompleksowych działań edukacyjnych, technologicznych i prawnych[20]. Tak jest również w wypadku treści pornograficznych znajdujących się w cyberprzestrzeni.

21 Realizując obszar edukacji, rodzice powinni rozmawiać z dziećmi o zagrożeniach i niebezpieczeństwach występujących w Internecie, ale jednocześnie nie demonizować go, pokazać, że może być miejscem zabawy, nauki i pozyskiwania informacji. Powinni także kontrolować, czy dziecko nie spędza zbyt dużo czasu przed ekranem komputera, tak żeby cyberprzestrzeń nie zastąpiła świata realnego.

22 Zdaniem D. Heise w obszarze technologicznym rodzice mogą chronić swoje dziecko poprzez sprawdzanie historii wyszukiwarki albo instalowanie programów kontroli rodzicielskiej, które dają możliwość kontrolowania witryn oglądanych przez dziecko, a nawet blokowania wybranych stron internetowych[21]. Istnieją programy, które zmieniają przeglądarkę w taki sposób, że staje się ona przyjazna dziecku, zabezpieczają przed pornografią, agresją i nieodpowiednimi treściami, precyzują maksymalny czas spędzony przy komputerze. Warto, aby rodzice je znali i stosowali, ażeby skutecznie przeciwdziałać zagrożeniom.

23 Rola szkoły w zapobieganiu pornografii może być równie znacząca. S. Kozak uważa, że problematyka bezpieczeństwa w sieci powinna być trwałym elementem programów nauczania, szczególnie w gimnazjach i szkołach podstawowych, gdzie uczniowie dopiero

[19] Tamże.

[20] Por. S. Kozak, *Patologie komunikowania w Internecie*, Wyd. Difin, Warszawa 2011, s. 189.

[21] Por. D. Heise, *O zagrożeniach w Internecie*, „Wychowawca", 4/2010, s. 18.

DOBRE PRAKTYKI

zaczynają swoją przygodę w kontakcie z Internetem[22].

24 PODSUMOWANIE

Istotne jest również uregulowanie prawa tak, aby prezentowanie treści pornograficznych nie było aż tak powszechne i dostępne dla wszystkich, szczególnie nieletnich. Bowiem wejście na takie strony wiąże się jedynie z kliknięciem hasła „mam 18 lat", co jak wiadomo, nie stanowi żadnego zabezpieczenia. Walka z występowaniem cyberpornografii jest bardzo trudna i praktycznie zdana na porażkę, ze względu na dużą swobodę panującą w Internecie, dlatego powinno się zainwestować w edukację, dzięki której rodzice będą wiedzieli, jak radzić sobie z takimi problemami.

25 Istnieją pewne ograniczenia prawne co do publikowania pornografii, a także grupy nacisku dążące do zakazania jej w ogóle, przeszkadzające w sprzedaży pism pornograficznych w kioskach i protestujące przeciw takim scenom w telewizji. Jednak działania takie są dość nieskuteczne wobec komputerów i Internetu. Ustalenia prawne lub głos opinii publicznej mogą tylko zjawisko publikacji materiałów pornograficznych nieco ograniczyć, ale raczej nie zlikwidować. Natomiast sporo mogą w tej sprawie zrobić rodzice, nauczyciele i wychowawcy dzieci i młodzieży. Przede wszystkim jednak dobrze by było, by rodzice starali się wyjaśnić dziecku, dlaczego zapoznawanie się z pornografią jest według nich niewłaściwe, porozmawiać z dziećmi na temat spraw związanych z seksem. Gdy dziecko będzie przekonane co do słuszności stanowiska rodziców, a sprawy seksu przestaną być już dla niego tak tajemnicze, jego zainteresowanie pornografią spadnie.

ĆWICZENIA 11

[22] Por. S. Kozak, *Patologie komunikowania w Internecie*, Wyd. Difin, Warszawa 2011, s. 190.

BIBLIOGRAFIA:

Augustyn J., *Wychowanie do integracji seksualnej*, Wydawnictwo M, Kraków 1994.

Bednarek J., *Zagrożenia w cyberprzestrzeni*, w: Jędrzejko M. (red.), *Patologie społeczne*, Wyższa Szkoła Humanistyczna w Pułtusku, Pułtusk 2006.

Cent J., *Nowe media a dzieci – dylemat rodziców*, w: Bogunia-Borowska M. (red.), *Dziecko w świecie mediów i konsumpcji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006.

Chrzanowska A., *Surfowanie po goliźnie*, „Charaktery", 9/2010.

Heise D., *O zagrożeniach w Internecie*, „Wychowawca", 4/2010.

Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, Świat Książki, Warszawa 1999.

Kornas-Biela D., *Niszczący wpływ pornografii*, „Wychowawca", 5/2006.

Kozak S., *Patologie komunikowania w Internecie. Zagrożenia i skutki dla dzieci i młodzieży*, Wyd. Difin, Warszawa 2011.

Kozak S., *Patologie wśród dzieci i młodzieży*, Wyd. Difin, Warszawa 2007.

Krawulska-Ptaszyńska A., *Psychospołeczne uwarunkowania korzystania z pornografii przez mężczyzn*, Bogucki Wydawnictwo Naukowe, Poznań 2003.

Kudlak G., *Sexting – od zabawy do przestępstwa*, w: Bębas S., (red.), *Oblicza patologii społecznych*, Wyd. Wyższej Szkoły Handlowej, Radom 2011.

Wallace P., *Psychologia Internetu*, Dom Wydawniczy Rebis, Poznań 2001.

Warylewski J., *Przestępstwa seksualne*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2001.

Zwoliński A., *Obraz w relacjach społecznych*, Wydawnictwo WAM, Kraków 2004.

ZAGROŻENIA SPOŁECZNO-WYCHOWAWCZE

SEKSTING

Anna Andrzejewska
Józef Bednarek

OPIS ZJAWISKA

1 WPROWADZENIE

Termin *sexting* powstał z połączenia ze sobą słów *sex* oraz *texting* (przesyłanie wiadomości tekstowych). Jest to zjawisko popularne szczególnie wśród nastolatków. Polega na przesyłaniu treści o charakterze erotycznym, głównie własnych nagich lub półnagich zdjęć, za pomocą Internetu i telefonu komórkowego, szczególnie przez osoby w okresie dojrzewania. Popularność sekstingu bierze się przede wszystkim z typowej w tym wieku fascynacji seksem, zainteresowania płcią przeciwną, braku doświadczenia w relacjach z innymi, ciekawości lub nieśmiałości.

Seksting – czyli wysyłanie swoich nagich zdjęć lub filmików przez Internet lub telefony komórkowe, staje się coraz powszechniejszym zjawiskiem wśród młodzieży. Młodzi ludzie wysyłają sobie erotyczne zdjęcia i filmiki w formie żartu lub jako „dowód miłości".

2 PRZYCZYNY ZJAWISKA

Internauci w Polsce nie zawsze dbają o swoją prywatność w sieci. Coraz częściej umieszczają informacje na swój temat na różnego rodzaju portalach społecznościowych. Jak wynika z badań przeprowadzonych w 2011 roku przez firmę PBI *(Polskie Badanie Internetu)* w ramach sondażu „Prywatność i własny wizerunek", liczba użytkowników i zasięg serwisów społecznościowych wyraźnie wzrasta.

W 2006 roku z serwisów społecznościowych korzystało 57,5% internautów, natomiast w styczniu 2011 roku odwiedził chociaż jeden serwis tej kategorii prawie każdy internauta (99,3%)[1].

3 Od momentu, w którym powstały portale społecznościowe można zauważyć, że użytkownicy Internetu coraz częściej zamieszczają w nich również swoje fotografie. Do tego typu czynów przyznało się bowiem, aż 68% wszystkich badanych[2]. Niby nic złego, w końcu przecież taka jest idea tych portali. Sytuacja zmienia się jednak, kiedy zdjęcia te przepełnione są erotyką lub scenami przekraczającymi granice dobrego smaku.

4 Można stwierdzić, że internautów ogarnął internetowy ekshibicjonizm. Dzielą się informacjami na swój temat, pokazują swoje ciało w całości i bez jakichkolwiek ograniczeń. Dla tych, którzy lubią dzielić się swoją nagością powstały specjalne portale. Wypełniają je fotografie erotyczne i pliki filmowe o takim również charakterze, robione i nakręcone przez samych użytkowników. Nie odnajdziemy tam zdjęć, które są typowe dla każdego z nas. Raz umieszczone materiały czy zdjęcia w Internecie pozostają tam na zawsze, a niefrasobliwość młodych ludzi jest daleko idąca.

5 Warto zauważyć, że internauci, którzy zamieszczają takie fotografie lub filmy nie zdają sobie sprawy z olbrzymiego zagrożenia, jakie na nich czyha. Nawet po długim czasie mogą stać się dla nich kompromitujące. Przecież każdy może zrobić z tych informacji dowolny użytek.

6 Zjawisko **sekstingu** można uznawać za jedną z form podtrzymywania kontaktów z bliskimi. Jednak wszystko zaczyna się komplikować, kiedy związek się rozpada a pliki, którymi dysponował nasz ekspartner, czyli zdjęcia, pokazujące nas w różnych dwuznacznych sytuacjach tracą pierwotne znaczenie i nabierają nowego, czasem potwornego, charakteru.

[1] Badanie *Prywatność i własny wizerunek* przeprowadzone przez PBI wśród 510 internautów w wieku 18–54 lata, Polskie Badanie Internetu, www.pbi.org.pl, data dostępu 13.01.2013.

[2] Tamże.

ROZPOZNANIE

7 Nie zawsze mamy wpływ na to, co dostaje się do sieci. Niejednokrotnie nasza tożsamość oraz prywatność może zostać ujawniona przez inne osoby, które bez jakichkolwiek zahamowań, a przede wszystkim trudności mogą ujawniać informacje o nas, nawet jeśli sami dbamy skrupulatnie o swoją prywatność. Trzeba pamiętać, że komunikacja w sieci pozwala na rozpowszechnianie informacji w błyskawicznym tempie i praktycznie bez kontroli. Materiał umieszczony w Internecie, bądź znajdujący się w pamięci telefonu komórkowego, w ciągu kilku chwil jest w stanie dotrzeć do szerokiego grona odbiorców. Osoby zamieszczające zdjęcia bądź filmy ukazujące nagość ich samych lub innych osób nie zawsze są świadome, jak poważne konsekwencje mogą przynieść takie zachowania.

8 Do świadomości przede wszystkim młodego człowieka są dostarczane informacje, że erotyczne zachowania, podteksty, sposób życia są na porządku dziennym. Zatem nie widzą nic złego w wysyłaniu sobie nawzajem, czy umieszczaniu w Internecie własnych nagich zdjęć czy filmów. Biorą przykład z gwiazd show biznesu, których filmy namiętnego stosunku można znaleźć w sieci. Bez względu na przyczyny, jakimi kierują się nastolatki wysyłając nagie zdjęcia na telefon czy umieszczając je w sieci, zachowanie takie niesie za sobą poważne konsekwencje. Mogą one dotyczyć zarówno złej opinii społeczeństwa, jak i sankcji prawnych czy nawet skutkować samobójstwem.

9 Najczęściej robienie i przesyłanie nagich lub półnagich zdjęć motywowane jest jako dowód miłości lub żart. „**W Polsce nie ma danych na temat skali zjawiska, jednak w USA z sekstingiem styka się co piąty nastolatek**”[3]. Według portalu „kafeteria.pl” ponad 40%[4] ludzi z różnych krajów w wieku 11–18 lat fotografowało się telefonem komórkowym, by później rozesłać zdjęcia znajomym. „Niektóre dziewczyny twierdzą, że inicjowanie i dostarczanie seksualnych doznań chłopcom daje im pewien rodzaj poczucia władzy, wydaje się jednak, że same nie odczuwają żadnej przyjemności fizycznej czy emocjonalnego spełnienia. Takie tendencje są szkodliwe dla dziewczynek i stoją na przeszkodzie tworzeniu w przyszłości satysfakcjonujących – seksualnych czy jakichkolwiek – związków”[5].

10 SKUTKI SEKSTINGU

Młodym ludziom seksting jawi się jako dobra zabawa, forma rozrywki, możliwość zaistnienia wśród rówieśników. Jest to również sposób na wyrażanie zainteresowania płcią przeciwną, przeżywanie pierwszych fascynacji i doświadczeń seksualnych. Niestety seksting niesie za sobą wiele negatywnych skutków. Większość młodych ludzi nie myśli perspektywicznie, a także nie posiada wiedzy odnośnie bezpieczeństwa tego typu korespondencji w sieci, nie ma więc pojęcia, że z pozoru niewinna zabawa może skończyć się tragicznie.

Młodzi ludzie nie zdają sobie sprawy, że np. były partner w ramach zemsty za rozstanie może wrzucić zdjęcie do Internetu czy rozesłać kolegom. Nie myślą o tym, że **zdjęcia raz wrzucone do sieci zostają w niej na zawsze**, nie biorą pod uwagę faktu, że ich telefon komórkowy może zostać skradziony wraz z całą zawartością.

[3] *Seksting. Wysyłanie nagich zdjęć do Internetu*, http://www.deon.pl/inteligentne-zycie/wychowanie-dziecka/art,341,seksting-wysylanie-nagich-zdjec-do-internetu.html, data dostępu 11.08.2011.

[4] *Seksting. Nastolatki uprawiają autopornografię*, http://www.kafeteria.pl/przykawie/obiekt.php?id_t=1062, data dostępu 22.01.2012.

[5] M. G. Durham, *Efekt Lolity. Wizerunek nastolatek we współczesnych mediach,* Wydawnictwo Prószyński i S-ka, Warszawa 2010, s. 54.

Skutki sekstingu mogą być bardzo poważne, często wręcz tragiczne. Upublicznienie nagich zdjęć wiąże się z ogromnym upokorzeniem dla młodej osoby, co z kolei skutkuje poważnymi problemami emocjonalnymi, utratą poczucia własnej wartości, depresją, niemożnością poradzenia sobie z sytuacją.

Poza konsekwencjami emocjonalnymi seksting niesie za sobą również **konsekwencje prawne**. Regulacje Kodeksu karnego mówią, iż **umieszczanie, rozpowszechnianie i kopiowanie pornograficznych zdjęć osób nieletnich jest karalne**. Zgodnie z przepisami Kodeksu karnego grozi za to kara od 3 miesięcy do 5 lat pozbawienia wolności.

11 Bardzo często zabicie nudy, fascynacja płcią przeciwną, fascynacja seksem, chęć rozbudzenia namiętności między partnerami, zwrócenia na siebie uwagi otoczenia, chęć zawarcia nowej znajomości, są przyczynami, które powodują, że zbyt łatwo i lekkomyślnie ludzie wysyłają swoje roznegliżowane zdjęcia albo filmiki. Nie zdają sobie sprawy z powagi sytuacji i konsekwencji takich zachowań. Dziś Internet to przecież także jedno z podstawowych narzędzi kontaktowania się pedofili z dziećmi.

12 Nastolatki świadome powszechnej erotyzacji życia nie widzą nic złego w prowokacyjnym zachowaniu czy w umieszczaniu na portalach społecznościowych nagich bądź półnagich zdjęć. Ponadto duży odsetek takich zachowań jest prowokatorskim zabiegiem o finansowych korzyściach. Slogany typu: doładuj konto a wyślę więcej zdjęć, często widnieją pod zdjęciami. „Takie dziecko kalkuluje sobie i wychodzi mu, że to się opłaca, bo nikt nie uświadomił mu, że nagość jest wartością, którą należy chronić" – mówi Jakub Śpiewak, założyciel fundacji „Kidprotect", zajmującej się ochroną dzieci przed niebezpieczeństwami czyhającymi na nie m.in. w Internecie[6]. Jest to patologia seksualna, zatem zaburzenie, na które składają się dewiacje seksualne, jak odchylenia seksualne i zboczenia seksualne, dotyczące zaburzeń w zakresie fantazji i zachowań seksualnych w relacjach z partnerem w wymiarze rzeczywistym i wyobrażeniowym. Ponadto dotyczą odchylenia od normy medycznej, a także praktyk seksualnych naruszających normy społeczne.

13 W dzisiejszym świecie wiele czynników może wpłynąć na zachowania dewiacyjne. Dzieci najbardziej narażone są na przetwarzanie niewłaściwych informacji, gdyż w młodym wieku nie umieją jeszcze krytycznie i obiektywnie podejść do dostarczanych do ich świadomości obrazów czy wiadomości. Tym bardziej, jeśli wychowywane są w dobie technologii informacyjnych, konsumpcjonizmu oraz erotyzacji życia codziennego. Tylko prawidłowe relacje międzyludzkie i przekazywane wartości uchronią przed rozwojem patologii społecznych. Seksting oraz inne zagrożenia, z jakimi mamy do czynienia na co dzień, są skutkiem chaosu panującego w systemie społecznym i politycznym. Człowiek staje w obliczu dysonansu poznawczego, gdzie z jednej strony musi się rozwijać wraz z postępem technologicznym, a z drugiej strony przed nim chronić, by się nie uzależnić i nie dopuścić do strat mierzonych w kategoriach emocjonalnych i materialnych. Świadomość otaczającego świata, próba charakteryzacji i zwalczania jego poszczególnych elementów może być sposobem na lepsze funkcjonowanie w społeczeństwie informacyjnym.

14 **BADANIA**

Badanie amerykańskiej organizacji NCTUP (National Campaign to Prevent Teen and Unplanned Pregnancy) dowodzi, że wy-

[6] M. Kaczmarek, *Seksting, czyli dlaczego dziewczyny nie mają nic do ukrycia*, http://www.nto.pl/apps/pbcs.dll/ article?AID=/20110820/REPORTAZ/236337781, data dostępu 20.08.2011.

syłanie swoich aktów innym jest niezwykle popularne w grupie od 13 do 19 lat, a więc problem dotyczy również niepełnoletnich. W grupie od 20 do 26 lat wysyłanie zdjęć zdarza się nieco rzadziej[7].

15 Badania przeprowadzone w Australii potwierdzają niepokój związany z sekstingiem. 40% dziewcząt spośród wszystkich badanych przyznało, że koledzy namawiali je do przesyłania roznegliżowanych zdjęć[8].

16 Zjawisko sekstingu starano się zbadać również w Wielkiej Brytanii. CEOP (Britain's Child Exploitation and Online Protection Center) przepytał 2000 nastolatków w wieku od 11 do 18 lat. Jak się okazało, zjawisko sekstingu przybrało tam niepokojące rozmiary. Aż 40% badanych przyznało się, że brało w nim udział, a ok. 70% badanych zna prywatnie nadawców erotycznych wiadomości[9].

W Polsce nie ma danych na temat skali tego zjawiska. Nie prowadzono również żadnych badań, które pokazywałyby te kwestie w odniesieniu do osób niepełnosprawnych.

17 **DOBRE PRAKTYKI – SEKSTING A PRAWO**

Art. 81. Ustawy o prawie autorskim i prawach pokrewnych

§ 1. Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.

Art. 191a. Kodeksu karnego

§ 1. Kto utrwala wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej, używając w tym celu wobec niej przemocy, groźby bezprawnej lub podstępu, albo wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody rozpowszechnia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 202. Kodeksu karnego

§ 3. Kto w celu rozpowszechniania produkuje, utrwala lub sprowadza, przechowuje lub posiada albo rozpowszechnia lub publicznie prezentuje treści pornograficzne z udziałem małoletniego albo treści pornograficzne związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 4. Kto utrwala treści pornograficzne z udziałem małoletniego poniżej lat 15, podlega karze pozbawienia wolności od roku do lat 10.

§ 4a. Kto sprowadza, przechowuje lub posiada treści pornograficzne z udziałem małoletniego poniżej lat 15, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4b. Kto produkuje, rozpowszechnia, prezentuje, przechowuje lub posiada treści pornograficzne przedstawiające wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

7 *Sex and Tech. Results for a Survey of Teens and Young Adults*, The National Campaign to Prevent Teen and Unplanned Pregnancy, http//: www.thenationalcampaign.org/sextech/PDF/Sextech_Summary.pdf (02.01.2013).

8 *Sexting – fears as teens targeted*, http//:www.stuff.co.nz/technology/digital-living/528950 (05.02.2013).

9 http//:www.thesurvivorstrust.org/uploaded/documents/CEOP%20E-Bulletin%20NovDec%2009%20Final.pdf (03.04.2011).

DOBRE PRAKTYKI

ĆWICZENIA 12

BIBLIOGRAFIA:

Durham M. G., *Efekt Lolity. Wizerunek nastolatek we współczesnych mediach,* Wydawnictwo Prószyński i S-ka, Warszawa 2010.

M. Kaczmarek, *Seksting, czyli dlaczego dziewczyny nie mają nic do ukrycia*, http://www.nto. pl/apps/pbcs.dll/article?AID=/20110820/REPORTAZ/236337781, data dostępu 20.08.2011.

Prywatność i własny wizerunek, Polskie Badanie Internetu, www.pbi.org.pl data dostępu 13.01.2013.

Seksting. Nastolatki uprawiają autopornografię, http://www.kafeteria.pl/przykawie/obiekt . php?id_t=1062, data dostępu 22.01.2012.

Seksting. Wysyłanie nagich zdjęć do Internetu, http://www.deon.pl/inteligentne-zycie/wyc howanie-dziecka/art,341,seksting-wysylanie-nagich-zdjec-do-internetu.html, data dostępu 11.08.2011.

Sex and Tech. Results for a Survey of Teens and Young Adults, The National Campaign to Prevent Teen and Unplanned Pregnancy, http//:www.thenationalcampaign.org/sextech /PDF/SextechSummary.pdf, data dostępu 02.01.2013.

Sexting – fears as teens targeted, http//:www.stuff.co.nz/technology/digital-living/528950 (05.02.2013).

SEKTY

Anna Andrzejewska
Józef Bednarek

OPIS ZJAWISKA

1 WPROWADZENIE

Pojęcie „sekta" pochodzi z języka łacińskiego, „Secta" wywodzi się z czasownika „sequor" – iść, podążać za kimś (a nie od „secare" – odcinać, oddzielać). Stąd słowniki wyjaśniają; sekta – droga, którą się podąża, sposób postępowania. Niektórzy wolą stosować określenia – grupa, ruch[1].

2 DEFINICJA

W ujęciu socjologicznym **sektę definiuje się obecnie jako „grupę społeczną izolującą się od reszty społeczeństwa, mającą też własną hierarchię wartości i zespół norm zachowania się z silnie akcentowaną rolą przywódcy" bądź „małą grupą, w której realizuje się dążenie do wytworzenia osobistych, bezpośrednich więzi między członkami, a której stosunek do świata, państwa czy społeczeństwa pozostaje obojętny lub niechętny"**[2].

3 Sekta oznacza „grupę społeczną, charakteryzującą się ostrą izolacją względem otoczenia, wynikającą z własnego, odrębnego, najczęściej opozycyjnego systemu wartości i z mocno akcentowaną rolą przywódcy. Cechuje ją bardzo silna więź wewnętrzna, najczęściej dla jej członków jedyna, a także wymóg bezwzględnej lojalności"[3].

4 Socjologowie uznają zaś, że określenie sekty jest wieloznaczne i dlatego poszczególni autorzy, biorąc pod uwagę silne oddziaływanie czynników historycznych, społecznych i kulturowych podają własne wyjaśnienia. W obrębie socjologii istnieje zgoda co do tego, że sekty mogą pojawiać się nie tylko w społecznościach religijnych. Z tego też względu termin „sekta" bywa używany w kilku znaczeniach – szerszym i węższym. **W szerszym znaczeniu sekta to każdy zbiór ludzi pozostający w opozycji do reszty społeczeństwa lub społeczności, w której dana sekta istnieje.** Tak pojęta sekta jest więc grupą społeczną, której najistotniejszą cechą jest izolacja w stosunku do pozostałych grup społecznych. Nie chodzi wyłącznie o izolację przestrzenną, lecz o izolację o charakterze światopoglądowym, ideologicznym czy psychologicznym. Natomiast **w węższym znaczeniu sektą nazywamy grupę ludzi połączonych wspólnym przeżywaniem stanów zachwytu i uniesień religijnych, która oddzieliła się od oficjalnego kościoła lub wyznania**[4].

5 PRZYCZYNY ZJAWISKA

Poszukiwanie własnej tożsamości religijnej staje się obecnie ogromnym problemem jednostkowym i społecznym. W poszukiwaniu samego siebie jednostka nie może oprzeć się na środowiskach, w których wzrasta. One także przechodzą właśnie swój kryzys.

6 Jednym z najbardziej bolesnych jest **kryzys rodziny**, dotąd ostoi tradycji, ciągłości kulturowej i jedności myśli. Pierwotny wybór wyznania, w rodzinie, dokonuje się automatycznie, bez angażującego udziału zainteresowanych, w drodze wychowania rodzinnego. Odrzucenie rodzinnego przekazu na rzecz nowej wiary nie jest zjawiskiem powszechnym, lecz występuje coraz częściej. Rodzina ma ogromny wpływ na wprowadzenie dzieci w świat kultury religijnej, symboliki, tradycji, obyczajów, języka, systemu wartości. Wrastanie w kulturę, które jest „zadomowieniem się" w świecie, dokonuje się głównie poprzez rodzinę. Bardzo niepokojące są wszelkie oznaki osłabie-

[1] Z. Pawłowicz, *Kościół i sekty w Polsce*, Wydawnictwo Diecezji Gdańskiej „Stella Maris", Gdańsk 1992, s. 109.

[2] P. T. Nowakowski, *Sekty, co każdy powinien wiedzieć*, MATERNUS MEDIA, Tychy 1999, s. 10.

[3] A. Zwoliński, *Anatomia sekty*, Polskie Wydawnictwo Encyklopedyczne „Powlen", Radom 2004, s. 17.

[4] K. Olechnicki, P. Załęcki, *Słownik socjologiczny*, Toruń 1997, s. 805.

nia roli rodziny, co ma bezpośredni związek z podjęciem przez dzieci poszukiwań nowych wspólnot i grup.

7 Współcześnie obserwuje się również wyraźne **osłabienie związków przyjaźni i bliskości**. Po utracie kogoś bliskiego, w sytuacji zawodu miłosnego czy kryzysu emocjonalnego młody człowiek szuka małych grup, przypominających „prawdziwą rodzinę”[5], za którą tęskni, która dałaby mu uczucie przyjaźni i bliskości. Niekiedy za poszukiwaniem prawdziwej wspólnoty i możliwości osobowych kontaktów kryją się neurotyczne zahamowania i nieśmiałość oraz pewne braki osobowościowo-charakterologiczne, jak np. niedojrzałość osobowa lub egocentryzm. Współczesny świat daje poczucie osamotnienia. Kolejne bolesne doświadczenia w bliskich kontaktach z innymi utwierdzają w przekonaniu, że niełatwo o przyjaźń.

8 **Środowisko, w którym wychowuje się człowiek, może mieć wpływ na jego skierowanie się w stronę sekt i nowych ruchów religijnych**, elementami takimi mogą być: problemy szkolne (trudności w szkole, drugoroczność, brak uznania u nauczycieli), brak możliwości ciekawego spędzenia wolnego czasu, wpływ środków masowej informacji, moda, przykład kolegów, zgorszenie zachowaniem się osób znanych sobie jako religijne, nadmiar zakazów i brak prywatności, brak akceptacji w środowisku.

9 **Do cech osobowości i charakteru, które mogą mieć wpływ na poszukiwanie kontaktu z sektą i nowymi ruchami religijnymi**, należą m.in.: niedojrzała osobowość, egocentryzm, naiwność, infantylizm, brak realnych planów życiowych, mała odporność na sytuacje stresowe, odczuwanie silnej potrzeby afiliacji i uznania, a także przewodzenia i imponowania w środowisku rówieśniczym, niepowodzenia seksualne i kompleksy oraz pragnienie wyżycia seksualnego i perwersji, łatwa fascynacja muzyką i tekstami, a także obrzędowością, rytuałami i symboliką. Pośród tych przymiotów należy także umieścić szczególną wrażliwość religijną, poszukiwanie celu i sensu życia, życia wewnętrznego, wspólnoty na ludzką miarę, utożsamiania się z kimś lub czymś, potrzebę pewności i bezpieczeństwa, uczestnictwa oraz zaangażowania. Jeśli te potrzeby i poszukiwania nie zostają zaspokojone we wspólnocie religijnej, łatwo mogą się stać przedmiotem obietnic i manipulacji ze strony sekt.

Sekty, podobnie jak wiele zjawisk w świecie rzeczywistym, zaczynają z powodzeniem funkcjonować w Internecie. Wielu młodych ludzi zaspokaja potrzebę społecznych kontaktów, siadając przed komputerem. Przez Internet odbywa się nie tylko wymiana towarów i usług, ale też idei. Sieć jest miejscem rozpowszechniania wielu skrajnych ideologii, destrukcyjnych poglądów, w tym antyracjonalizmu, pseudo nauki, okultyzmu, aż do faszyzmu, komunizmu i satanizmu.

10 WEJŚCIE DO SEKTY

Istnieją różne sposoby werbowania do sekt. Proces werbunku przeprowadzany jest w trzech etapach[6]:

Faza uwodzenia – to swoiste preludium procesu indoktrynacji. Nie zwerbuje się kogoś do sekty, jeśli uwaga tej osoby nie zostanie przyciągnięta, skoncentrowana na ideach lub proponowanych ich złudnych realizacjach. Mało prawdopodobne jest, by przyszły adept został przyciągnięty przez werbującego człon-

[5] E. Mudrak, *Fenomen sekt,* Oficyna Wydawnicza „Impuls”, Kraków 2007, s. 37–38.

[6] J. Abgrall, *Sekty – manipulacja psychologiczna*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2005, s. 96–103.

ka grupy o szorstkim sposobie bycia. Uwieść to przede wszystkim spodobać się, ale również odwieść od prawdy. Celem wszystkich wysiłków sekty jest zaproponowanie świetlanej utopii zamiast codziennej szarej egzystencji. Werbujący – uwodziciel stosuje wszelkie dostępne sekciarskie iluzje. Działa jak kuglarz, żeby przyciągnąć potencjalnych adeptów; proponuje proste odpowiedzi na zadawane pytania; urzeka rozmówcę, żeby stworzyć złudzenie uczuciowej wymiany; nieustannie sprawdza emocje, pozbawiając dialog wszelkiej logiki; niezdrowej rzeczywistości przeciwstawia perspektywę miłości idyllicznej, która panuje wewnątrz jego wspólnoty. Pierwszy kontakt między obiektem a sektą następuje najczęściej z inicjatywy tej organizacji. Stosuje ona taktykę sprzedaży czynnej, czyli szuka kolejnej „zdobyczy". Na kontakt z konkretną osobą sekta poświęca większość czasu. Tymczasem, aby sprzedać produkt, niezbędne jest nawiązanie bezpośredniego kontaktu z potencjalnym kupującym. Ten kontakt rozpoczyna proces identyfikacji między werbującym a werbowanym.

Faza Perswazji – wymaga nawiązania szczególnego układu, relacji nadawczo-odbiorczej między osobami. Wytwarza się pomiędzy nimi specyficzna więź, podtrzymywana w celu wymiany informacji na temat głoszonej doktryny. Nadawca, czyli członek sekty, ma przekonać swego rozmówcę, czyli odbiorcę, który jest celem, potencjalnym adeptem, przedmiotem werbowania. Komunikatem są, jak wspomniano wyżej, informacje dotyczące ideologii. Aby perswazja była skuteczna, każdy z trzech wymienionych wyżej elementów (nadawca, odbiorca oraz komunikat) muszą spełnić szczególne wymagania. Celem perswazji jest doprowadzenie odbiorcy do zaakceptowania propozycji zawartej w informacji. Na proces przekonywania składają się następujące elementy: percepcja, zrozumienie, forma, synteza wiadomości, ich akceptacja, zmiana sposobu myślenia albo postawy.

Wiadomości podstawowe, pochodzące z głównego nurtu doktryny sekty, powinny być bardzo czytelne i przejrzyste. Wiadomości z kanałów pobocznych zawierają natomiast wiele elementów irracjonalnych, emocjonalnych oraz ewidentne oszustwa dodane przez nadawcę.

Jeśli nadawca zauważy, że odbiorca przyjął przekazaną wiadomość, skorzysta z głównego kanału komunikacji. W przeciwnym razie, jeśli trzeba będzie odpierać zarzuty i przekonywać rozmówcę, do manipulacji zostaną wykorzystane kanały poboczne. Nadawca musi być wiarygodny i wzbudzać zaufanie. Udaje sympatię, żeby wytworzyć empatię – to jeden z kanałów pobocznych. Rolę nadawcy może pełnić pojedyncza osoba, mała grupa a nawet cała sekta.

Faza fascynacji – jest kluczowym elementem procesu wprowadzania osoby do sekty. Fascynacja służy „zdobywaniu rynku". Po fazie rozwiewania wstępnych wątpliwości kandydat zostaje przekonany o słuszności swojego wyboru i staje się coraz bardziej uzależniony od sekty. Kiedy spotyka guru, ostatecznie przestaje się wahać.

Zaczyna się wtedy nowy etap indoktrynacji, mający ustanowić magiczną relację między przyszłym adeptem a grupą. Stopniowo są zrywane więzi ze światem zewnętrznym po to, by pozostał tylko symboliczny wszechświat tego, co sakralne i boskie. Fascynacja tym wszechświatem odbierze adeptowi wszelką chęć do uwolnienia się

spod wpływu sekty i jej członków. Fascynacja nowego kandydata opiera się na rzeczywistym zachwycie symboliczną postacią guru. Guru wydaje się dysponować nadnaturalną mocą, graniczącą z boskością. W tym stadium wolna wola rekruta zaczyna słabnąć wobec wywieranej na nim silnej doktrynalnej presji. Ostatecznie „nawrócenie" adepta będzie zależało od stosunku między siłą zniewolenia wywieranego przez sektę a mocą uprzednich jego więzów ze społeczeństwem.

Proces fascynacji można porównać do hipnozy. Kiedy występuje, oznacza to przewagę relacji empatycznej nad racjonalną analizą. Fascynacja ucznia wskazuje na stan jego uzależnienia.

11 **ZNACZENIE PRZYWÓDCY**

Osobą, która uczy i prowadzi na drodze do boskiego objawienia jest guru. Musi być on postrzegany przez swoich uczniów jako boska istota. Zadaniem guru jest uczynić swoją osobę wiarygodną oraz odpowiednio zareklamować swój wizerunek uczniom. Aby osiągnąć swój cel, wymyśla on kłamstwa na swój temat. Stopniowo sam zaczyna wierzyć w swoje historie i przestaje już rozróżniać prawdę od kłamstwa. Swoje historie układa od momentu narodzin i dzieciństwa. Jedni rodzą się już jako guru, drudzy dopiero się nimi stają np. po doznaniu objawienia. Istnieją również guru, którzy roszczą sobie prawo do kontynuowania czyjegoś dzieła, powołując się na pokrewieństwo inicjacyjne lub kulturalne, są również przypadki występowania jedynie pokrewieństwa duchowego. Guru swoją nadzwyczajność ogłasza zazwyczaj już w wieku dojrzałym. Guru, czyli mistrz musi być najlepszy we wszystkich dziedzinach życia, nawet najbardziej prozaicznych, dlatego też posługuje się różnego rodzaju dyplomami, oczywiście jedne z nich są prawdziwe, a inne fałszywe. Jeśli nawet nie powołuje się na prestiżowe dyplomy, uważa się za wszechwiedzącego oraz, że jego kompetencje rozciągają się na wszystkie dzieciny wiedzy. Ulubioną dziedziną guru jest medycyna alternatywna, gdyż najłatwiej jest udawać obszerną wiedzę na jej temat.

12 **TYPY SEKT**

Sekta żyje wokół guru i pod jego przewodnictwem. Adepci powiększają jej szeregi, lecz nie każdy z nich ma taki sam status, nie utrzymuje takiej samej relacji z guru i nie korzysta z przywilejów. Można wyróżnić następujące typy, ze względu na rodzaj i struktury organizacji sekty[7]:

13 **Struktura piramidy.** Zakłada hierarchizację wiedzy, władzy i przywilejów. Porównując sytuację: „dołów" (rekrutów) i „góry" (guru i jego otoczenie), można zaobserwować, że:

- im wyżej w hierarchii, tym większy stopień uprzywilejowania,
- im niżej, tym większe zniewolenie.

14 Wstępowanie na wyższy poziom w strukturze grupy dokonuje się powoli, stopień po stopniu. Celem tego systemu jest utrzymywanie osoby należącej do sekty w stanie ciągłej zależności. Struktura przypominająca piramidę zapewnia sekcie korzyści: sprzyja rywalizacji, oferując adeptowi uczucie dumy, kiedy zdobywa coraz wyższe szczeble hierarchii oraz wzmacnia jego poczucie przynależności, uzależniając go od sekty.

15 **Struktura pajęczyny.** Niektóre sekty budują strukturę podobną do pajęczyny. Jest to połączenie wielu struktur piramidalnych, spełniających rozmaite funkcje. Adept może awansować w jednej piramidzie, a być degradowany w innej. Zawsze jednak jest zależny

7 Tamże, s. 77–81.

od hierarchii, bez względu na to, na którym jej szczeblu się znajduje.

16 **Struktura gwiazdy.** Struktura ta przypomina koło rowerowe, gdzie guru stanowi centrum, a adepci – obręcz. Informacje przepływają z obręczy do centrum i na odwrót. Wszyscy członkowie grupy mają bezpośredni kontakt z guru, on zaś pobudza energię każdego z nich.

17 Jedną z głównych cech sekty jest „modlitwa", która ułatwia przejście w stan hipnozy. Mamy tu do czynienia również z ciągłym i rytualnym powtarzaniem mantry, czyli „om". Następną cechą tej grupy są rytuały, podczas ich uczestnictwa wzmacnia się poczucie przynależności. Podczas takiego rytuału każda osoba przynależąca do sekty ma przypisaną konkretną rolę, a rytualne ceremonie scalają grupę. Uczestnictwo w rytuale daje wrażenie uczestnictwa w jakiejś nadprzyrodzonej, boskiej lub „kosmicznej" sprawie. Bardzo często polega on na powtarzaniu zdań w celu wprowadzenia uczestników w stan hipnozy. Odbywa się to na przykład tak[8]:

PROWADZĄCY: Mój umysł jest zaniepokojony.
WSZYSCY: Mój umysł jest zaniepokojony.
PROWADZĄCY: Moje serce jest poruszone.
WSZYSCY: Moje serce jest poruszone.
PROWADZĄCY: Moje ciało jest napięte.
WSZYSCY: Moje ciało jest napięte.

ROZPOZNANIE OBJAWY

DIAGNOZA

18 **OBJAW, ROZPOZNANIE, DIAGNOZA**

Niewątpliwe jest to, że grupa ta uzależnia psychicznie, czego przykładem jest np. **uczestniczenie w rytuałach**. Sekta uzależnia również fizycznie. **Przykładami uzależnienia fizycznego jest izolacja od środowiska**. Początkowo sekta odizolowuje rekruta od rodziny. Jednocześnie wraz z izolacją od środowiska prowadzona jest **kontrola finansowa**. Adept oddaje swoje dobra materialne na rzecz całej sekty, aby wyzbyć się rzeczy „zbędnych" do życia. Można również zaobserwować pozbawienie snu, wynikające zazwyczaj z przymusu uczestniczenia w rytuałach. Oprócz pozbawienia snu widoczne jest również ograniczenie snu, wielokrotnie budzi się adepta w środku nocy w celu odbycia rytuałów. Następnym uzależnieniem fizycznym stosowanym przez sekty jest **przymusowa praca**, która jest źródłem utrzymania dla sekty. Każda sekta posiada swój własny **rytuał pozdrawiania, który jest symbolem poddaństwa i posłuszeństwa**. Większości takich grup przymusowo każe się pozbyć osobistych ubrań i narzuca noszenie specyficznego stroju, który jest symbolem przynależności do danej grupy, sekta oprócz narzucenia sposobu ubierania, decyduje również o wyglądzie skóry czy fryzury. Większość zgrupowań stosuje medycynę niekonwencjonalną lub „naturalną". Bardzo ważnym elementem uzależnienia od sekty jest **posiadanie przedmiotów symbolicznych**.

Przedmiot symboliczny (będący rzekomo nośnikiem tajemnej siły) ma podwójne znaczenie[9]:

- potwierdza przynależność adepta do grupy,
- ochrania go (amulet, talizman, fetysz).

19 **NIEPOKOJĄCE SYGNAŁY**

Pierwszymi niepokojącymi objawami, jakie możemy zaobserwować po zapoznaniu się z sektą lub po wstąpieniu do niej, to między innymi zmiana diety. Bliska osoba przestaje spożywać produkty, które dotychczas lubiła lub zwyczajowo jadła (mięso, jajka, kawa, herbata, itp.). Następną rzeczą łatwą do zaobserwowania jest zmiana wyglądu zewnętrznego, ciągłe noszenie tych samych spodni czy koszulki,

[8] Tamże, s. 170.

[9] Tamże, s. 186.

preferowanie jednego koloru, czy noszenie dziwnej szaty, co jest bardzo łatwe do zaobserwowania. Osoba mająca kontakt z sektą może zaniechać dbania o higienę osobistą lub wręcz przeciwnie. Możliwe do zaobserwowania jest również noszenie różnego rodzaju amuletów lub nagła zmiana fryzury. Po kontakcie z sektą radykalnie zmieniają się przyzwyczajenia osoby werbowanej, np. nagle rezygnuje ona z dotychczasowych form spędzania wolnego czasu lub przestaje spotykać się ze znajomymi. Adept zmienia też nastawienie do religii oraz ma nowe zwyczaje i przyzwyczajenia.

Szeroką działalność prowadzą sekty w Internecie. Wykorzystują one sieć do komunikacji i werbowania nowych członków. Młodzież opisuje swoje problemy, lęki na blogach i forach internetowych, a tam z dużym prawdopodobieństwem może czekać osoba werbująca. Szczególnie narażone są osoby znajdujące się w trudnych sytuacjach życiowych, zarówno pod względem materialnym, jak i emocjonalnym. Sekty wykorzystując to, oferują swoją pomoc, mają zawsze czas, aby wysłuchać i doradzić w przeciwieństwie do osób bliskich.

W zależności od grupy werbunek przebiega różnie, można jednak wskazać pewne punkty wspólne. Członek sekty usiłuje zgromadzić jak najwięcej informacji od werbowanego, jednocześnie nie mówiąc prawie nic o grupie. Osoba werbująca dowiaduje się o werbowanym wszystkiego, począwszy od imienia, nazwiska, adresu, numeru telefonu, poprzez jego marzenia, nadzieje, lęki, zainteresowania, a skończywszy na charakterze wykonywanej pracy, przyjaźniach i znajomościach.

20 PODSUMOWANIE

Skuteczny werbunek opiera się na jak najlepszym poznaniu kandydata. Im więcej informacji uzyska się na jego temat, tym skuteczniej można do niego trafić. Werbownicy są na ogół dobrze przygotowani do swojej roli, z łatwością inicjują kontakt i umiejętnie go podtrzymują. Potrafią również obserwować i rozpoznawać potrzeby osób, z którymi mają do czynienia. Już krótka rozmowa z kandydatem daje możliwość zdobycia wystarczającej wiedzy na jego temat oraz opracowania odpowiedniego klucza do „rozpracowania" go[10].

ĆWICZENIA 13

[10] P. Nowakowski, *Sekty – oblicza werbunku*, Wyd. Maternus Media, Tychy 2001, s. 19.

BIBLIOGRAFIA:

Abgrall J., *Sekty – manipulacja psychologiczna*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2005.

Mudrak E., *Fenomen sekt*, Oficyna Wydawnicza „Impuls", Kraków 2007.

Nowakowski P. T., *Sekty – oblicza werbunku*, Wyd. Maternus Media, Tychy 2001.

Nowakowski P. T., *Sekty, co każdy powinien wiedzieć*, Wyd. Maternus Media, Tychy 1999.

Olechnicki K., Załęcki P., *Słownik socjologiczny*, Toruń 1997.

Pawłowicz Z., *Kościół i sekty w Polsce*, Wydawnictwo Diecezji Gdańskiej „Stella Maris", Gdańsk 1992.

Zwoliński A., *Anatomia sekty*, Polskie Wydawnictwo Encyklopedyczne „Powlen", Radom 2004.

STALKING

Anna Andrzejewska

OPIS ZJAWISKA

1 WPROWADZENIE

Wśród wielu najnowszych analiz dotyczących współczesnych szans mediów cyfrowych[1] i ich zagrożeń, zwłaszcza społeczno-wychowawczych i moralnych, a także zdrowia psychicznego[2] mieści się stalking. Tłumaczenie słowa stalking w języku polskim może oznaczać „nękanie, osaczanie, prześladowanie. Samo **pojęcie stalking oznacza ustawicznie dręczyć, trapić, niepokoić, (czymś) kogoś; dokuczać komuś, nie dawać chwili spokoju**"[3]. Zdaniem B. Hołysta „stalking to celowe, złośliwe, wielokrotne prześladowanie i molestowanie innej osoby zagrażające jej bezpieczeństwu"[4].

Można zatem powiedzieć, że stalking to nic innego jak nękanie oraz ograniczanie wolności innej osoby poprzez zastraszenie, śledzenie, nieszanowanie czyjejś prywatności, co może powodować u zastraszanej osoby poczucie zagrożenia, skrępowanie, a także ogólny strach przed potencjalnym agresorem i innymi ludźmi.

2 CHARAKTERYSTYKA ZJAWISKA

Początkowo prześladowanie takie objawiało się śledzeniem, obrażaniem innej osoby na forum publicznym, grożeniem, obserwowaniem, nachodzeniem w pracy bądź w domu itp. Natomiast w obliczu szeroko dostępnych mediów, takich jak telefonia komórkowa czy Internet, stalking może stanowić także wirtualne dręczenie ofiary poprzez natrętne telefony, obraźliwe esemesy, a także wysyłanie wiadomości e-mail z pogróżkami i innymi obraźliwymi treściami[5].

3

Anonimowość, jaką stwarzają nowoczesne media cyfrowe, daje poczucie władzy i sprawstwa, a także przewagi nad ofiarą, dzięki czemu zwalnia się poczucie odpowiedzialności za czyny związane ze stalkingiem. Stalkerzy mają coraz „większe pole do popisu". Coraz częściej zatem spotyka się wykorzystywanie tych technologii do zastraszania swojej ofiary. Jest to rozpowszechnione do tego stopnia, że wygenerowano specjalną odmianę stalkingu bazującą na wykorzystaniu telefonu i Internetu, a mianowicie **cyberstalking. „Polega on na prześladowaniu e-mailowym w postaci przekazywania wiadomości na konto pocztowe ofiary wbrew jej woli, uniemożliwiania korzystania ze skrzynki pocztowej, rozsyłania niechcianych przesyłek do ofiary jako nadawcy**"[6].

4

Zdaniem W. Woźniaka i M. Lattanzi stalking ma miejsce, gdy zachowania są zaplanowane, prześladowanie i zastraszanie występuje dziesięć razy w ciągu miesiąca, a także gdy zachowania sprawcy wywołują negatywne skutki u ofiary (bezsenność, poczucie zagrożenia, lęk)[7]. Może dotyczyć każdego i przydarzyć się każdemu. Nie ma tutaj określonej grupy osób, które byłyby reprezentantami tego zjawiska. **Stalkerem może być każda osoba: nieznajoma, a nawet ta, która wcześniej była prześladowanemu znana, lubiana, czy kochana**. Oprócz wymienionych korelacji i związków między ofiarą a sprawcą przemocy, stalking może także występować wśród osób, które się nie znają, a mianowicie między osobą anonimową a osobą publiczną np. sportowcem, aktorem, piosenkarzem itd.

---

[1] Por. J. Bednarek (red.), *Człowiek w obliczu szans cyberprzestrzeni*, Wyd. Difin, Warszawa 2014.

[2] Por. A. Andrzejewska, J. Bednarek (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Wyd. Difin, Warszawa 2014.

[3] M Szymczak (red.), *Słownik języka polskiego*, PWN, Warszawa 1992, s. 317.

[4] B. Hołyst, *Psychologia kryminalistyczna,* Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2009, s. 732.

[5] http://www.psychologia.net.pl/artykul.php?level=415, data dostępu: 02.01.2012.

[6] http://www.ies.krakow.pl/wydawnictwo/prokuratura/pdf/2008/10/4kosinska.pdf, data dostępu: 02.01.2012.

[7] W. Woźniak, M. Lattanzi, *Stalking – między przemocą a uzależnieniem,* Wydawnictwo Bernard Cichosz, Kutno 2010, s. 9.

5 Istotną i charakterystyczną cechą stalkingu jest długotrwałe dręczenie przy stosowaniu określonych zachowań, które regularnie się powtarzają. Stalker działa z premedytacją w celu osiągnięcia określonych korzyści: wzbudzenia strachu i poczucia zagrożenia w swojej ofierze, poniżenia jej, a nawet zmuszenia do określonych czynów. Motywy takiego działania mogą być bardzo różne, jednak najczęściej wymienia się zazdrość, odrzuconą miłość czy upokorzenie. Zatem nie ulega wątpliwości, że stalkerami najczęściej kieruje chęć zemsty na innej osobie[8].

6 DZIAŁANIA STALKERÓW

Stalkerzy wykorzystują do swojego działania coraz bardziej popularne serwisy społecznościowe. Bez zahamowań umieszczają tam różnorodne wpisy, komentują zdjęcia użytkowników, potrafią podszywać się pod inną osobę w celu zdobycia określonych informacji, które służą do zastraszania i nękania[9]. Zdarza się wykorzystywanie informacji o danej osobie i tworzenie w jej imieniu fikcyjnych profili na portalach społecznościowych; wykorzystywanie danych ofiar w ogłoszeniach erotycznych; podszywanie się za nie na czatach. Osoba prześladowana zostaje uwikłana przez agresora w intrygę, swego rodzaju „grę", której reguły ustala stalker. Sprawca jest mocno i silnie nastawiony na osiąganie wyznaczonych celów. Jego motywacją jest zdobycie władzy, wyższości nad ofiarą, dzięki czemu będzie mógł nie tyle planować swoje działania, co sterować zachowaniem ofiary.

7 Badania dotyczące występowania stalkingu, przeprowadzone przez Ministerstwo Sprawiedliwości w 2009 roku, jednoznacznie pokazują, że zjawisko to jest powszechne wśród Polaków. „Z 10 200 respondentów co dziewiąty odpowiedział twierdząco na pytanie, czy był ofiarą uporczywego nękania"[10].

Zachowania, które można określić jako stalking występują wtedy, kiedy:

- są zamierzone;
- wywołują strach (lęk);
- występują przez co najmniej trzydzieści dni;
- ma miejsce co najmniej dziesięć czynów w ciągu trzydziestu dni;
- powodują negatywne skutki psychiczno-relacyjne (niepokój, zaburzenia snu, konieczność zmiany telefonii, miejsca pracy, przyjaciół, znajomych, kolegów z pracy)[10].

8 MOTYWY STOSOWANIA STALKINGU

Stalking jest zjawiskiem, które charakteryzuje się zróżnicowaną specyfiką. Może występować w każdej grupie, bez względu na wiek czy płeć, a motywy stosowania nękania przez stalkerów są różnorodne, w zależności od związków, jakie ich łączyły z ofiarami oraz wieku.

Jedną z głównych przyczyn, dla której człowiek posuwa się do zastraszania i nękania innych osób jest niespełniona miłość. Człowiek odrzucony, szczególnie o niskim poczuciu własnej wartości, nie może pogodzić się z odejściem ukochanej osoby i „na siłę" próbuje zatrzymać ją przy sobie. Dotyczy to zarówno zerwania związku między osobami, jak również zabieganie o czyjeś względy, jednak bez rezultatu. Stalking staje się wówczas znakomitym sposobem, aby wzbudzić w ofierze poczucie zagrożenia i lęku[12].

[8] bip.kprm.gov.pl/download.php?s=75&id=488, data dostępu: 02.01.2012.

[9] *Jak się bronić przed agresją w Internecie,* pod. red. A. Szumilak, „Świat Wiedzy", 3/2011, s. 58.

[10] bip.kprm.gov.pl/download.php?s=75&id=488, data dostępu: 02.01.2012.

[11] M.Lattanzii In. tł. J. Skarzyńska, *Ciemna strona relacji interpersonalnych*, www.stalking.it, data dostępu: 11.04.2007.

[12] http://psychologia.net.pl/artykul.php?level=282, data dostępu: 03.01.2012.

ROZPOZNANIE OBJAWY

ĆWICZENIA 14

9 Osoba, której uczucie zostało odrzucone, szuka odpowiedniego sposobu, aby się zemścić lub aby zmusić ofiarę do powrotu. Stalkerem wówczas kieruje złość, frustracja i wściekłość z powodu odtrącenia. Stanowi to swoisty sposób na ukrycie rzeczywistych uczuć, takich jak zażenowanie i wstyd.

10 Ze względu na to, iż stalkerowi nie łatwo jest zrezygnować ze sprawowania władzy, to jego obsesyjne dążenie do osiągnięcia celu może leżeć w jego zaburzonej psychice i osobowości.

Sprawcy stalkingu mogą charakteryzować się:

- niską samooceną, co wiąże się z zaprzeczaniem i niedopuszczeniem do niepowodzeń;
- nieumiejętnością rozpoznawania intencji i działań innych ludzi;
- zmniejszoną empatią i dążeniem do celu za wszelką cenę, bez zważania na potrzeby i emocje innych;
- zapatrzeniem w siebie (narcyzmem) oraz brakiem umiejętności budowania relacji interpersonalnych[13].

11 Wśród powodów, dla których młodzież dopuszcza się stalkingu można wymienić:

- brak akceptacji,
- zaniżoną samoocenę,
- negatywne wzorce wyniesione z domu,
- brak poczucia bezpieczeństwa w rodzinie,
- nieprawidłowe relacje z otoczeniem.

12 Zjawisko to dotyczy nie tylko dorosłych, ale także rozpowszechnia się wśród młodzieży. Zastraszanie, nękanie innych, w szczególności rówieśników, stało się dla niektórych młodych osób sposobem na rozwiązanie swoich własnych problemów, sposobnością sprawowania władzy i kontroli nad innymi.

13 Warto odnieść się do badań przeprowadzonych przez B. Hołysta, które ukazują skalę zjawiska w tej grupie społecznej. Okazuje się, że wyniki wśród osób dorosłych oraz wśród młodocianych są bardzo porównywalne. Zdecydowaną większość prześladowców wśród młodzieży stanowią chłopcy, a ofiarami stalkingu są z reguły dziewczęta. Najczęstsza forma stalkingu to stosowanie gróźb (ponad 50%). Do zastraszania najczęściej wybierany jest telefon komórkowy, listy, a także przemoc stosowana wobec ofiar (aż 31% przypadków). Na szczególną uwagę zasługuje fakt, że stalking występuje wśród coraz młodszych dzieci, nawet już w szkole podstawowej[14].

14 PRZEJAWY STALKINGU

Przejawy stalkingu mogą być różnorodne i w dużej mierze zależą od intencji agresora oraz od jego skłonności do agresji. Najczęściej stalker chce przestraszyć ofiarę, a następnie spowodować u niej poczucie lęku i strachu. Czyni to za pomocą wysyłania esemesów, e-maili, następnie posuwa się do wykonywania głuchych telefonów oraz natrętnych, częstych telefonów. Do tych form nękania dochodzi także obserwowanie i śledzenie swojej ofiary, przesiadywanie pod jej domem, bądź w miejscach jej stałego pobytu (np. w okolicach pracy), wysyłanie niechcianych prezentów. Takie czynności mają na celu osłabienie psychiki ofiary i wywołanie u niej poczucia zagrożenia, co może doprowadzić nawet do załamania się psychiki ofiary. Stalker jest na tyle zdeterminowany, że aby osiągnąć swój cel jest w stanie sięgnąć po najbardziej radykalne środki.

[13] http://stalking.prv.pl/, data dostępu: 03.01.2012.

[14] B. Hołyst, *Psychologia kryminalistyczna,* Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2009, s.745—747.

15 Stalkerzy wykorzystują w swoich działaniach manipulację na szeroką skalę. Przygotowują przypadkowe spotkania. Wymuszają na swoich ofiarach podtrzymywanie kontaktów, a sprzeciw ze strony ofiary jest tylko zachętą do dalszych prześladowań. Posuwają się także do gróźb w przypadku sprzeciwu.

Wyróżnia się trzy formy cybernękania:
- napastowanie, które odbywa się tylko w sieci;
- nękanie dziejące się głównie w sieci, ale wychodzące również poza sieć lub mające jakieś komponenty w realnym świecie;
- dręczenie i nękanie dziejące się w realnym świecie, które ma także jakieś komponenty w sieci.

Ze względu na sposoby stosowania w cyberstalkingu wyróżnia się:
- e-mail stalking, polegający na prześladowaniu ofiary przy pomocy esemesów i e-maili;
- Internet stalking – najbardziej popularna forma – polega na podszywaniu się pod ofiarę na czatach, forach itp.;
- komputer stalking – charakteryzuje się sprawowaniem kontroli nad komputerem ofiary, uszkadzania sprzętu oraz danych[15].

16 Groźby mogą mieć charakter bezpośredni – wysyłanie wiadomości z pogróżkami, lub charakter pośredni, np. niszczenie przedmiotów należących do ofiary, wybijanie szyb w oknach domu, itp. Działania stalkera mogą również przerodzić się w liczne przestępstwa zagrażające życiu ofiary. Często przemoc jest jednak nieplanowana przez stalkera, podczas prześladowania może być raczej traktowana jako impuls[16].

17 „Stalker po prostu zamienia cudze życie w koszmar, nie interesuje go reakcja otoczenia, dopóki nie przybierze ona stosownej formy procesowej w postaci zastosowania np. środków przymusu”[17].

Oprócz nękania bezpośredniego, za pomocą listów, telefonów i e-maili, do zjawiska stalklingu można także zaliczyć „podszywanie się” pod kogoś innego. Zabieg taki, celowo wykonany przez stalkera ma doprowadzić do wyrządzenia krzywdy ofierze, krzywdy osobistej, prywatnej[18]. W takim wypadku znacznie trudniej jest ustalić prześladowcę. Nie ma się wówczas kontaktu ze sprawcą przestępstwa twarzą w twarz. Stalker działa w ukryciu, jako anonimowy internauta.

18 Należy zwrócić uwagę na istotną prawidłowość: najczęściej stalking dotyczy osób odmiennej płci, osób, które łączy lub łączyła znajomość, w większości sprawcami są mężczyźni (od 66%–90%). Najczęściej osobnik taki jest niezrównoważony emocjonalnie, nie potrafi zapanować nad swoją złością, nie radzi sobie z porażkami, ma niskie poczucie własnej wartości[19].

Wśród młodzieży najczęściej stalkerami bywają dzieci o niskim poziomie socjalizacji, które nie potrafią łatwo nawiązywać kontaktów międzyludzkich. Często ucie-

[15] J. Plis, *Cyberstalking. Podstawowe problemy prawnokarnej ochrony,* w: J. Bednarek, S. Bębas, J. Plis, *Patologie w cyberprzestrzeni*, WSH w Radomiu, Radom 2002, s. 349–350.

[16] B. Hołyst, *Psychologia kryminalistyczna,* Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2009, s. 733–739.

[17] http://www.ies.krakow.pl/wydawnictwo/prokuratura/pdf/2008/10/4kosinska.pdf, data dostępu 04.01.2012.

[18] A. Szumilak, *Jak się bronić przed agresją w Internecie,* „Świat Wiedzy”, 3/2011, s. 58.

[19] B. Hołyst, *Psychologia kryminalistyczna,* Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2009, s. 734–747.

kają się do stalkingu, aby udowodnić sobie oraz innym, że nie są słabą jednostką. Wywołując strach i niepokój u swojej ofiary starają się podnieść własną samoocenę, uzyskać własne korzyści, których nie mogliby osiągnąć poprzez bezpośrednią konfrontację z ofiarą. Stalkerami często także bywają osoby, które są przywódcami w grupie i wykorzystują swoją wysoko zajmowaną pozycję do zastraszania innych oraz wzbudzania poczucia zagrożenia i lęku.

19 Prześladowanie ofiary może obejmować różne przedziały czasowe. Wszystko jest uzależnione od celu, jaki postawił sobie sprawca. Chcąc przestraszyć osobę, która jest słaba psychicznie, stalkerowi wystarczy zaledwie wysłanie kilku wiadomości z groźbami lub wyzwiskami. Natomiast, gdy stalkerowi zależy na czymś więcej niż tylko wzbudzenie poczucia strachu w ofierze, zastraszanie może rozciągnąć się w czasie. Dodatkowo może się przyczynić do tego niezłomność i silna osobowość ofiary.

20 Analiza działalności stalkera (cyberstalkera) pozwala na wyodrębnienie kilku typów osobowości (portretów psychologicznych) stalkera:

1) stalker odrzucony;
2) stalker obrażony (urażony);
3) poszukiwacz intymności;
4) nieudolny konkurent (zalotnik);
5) stalker drapieżny;
6) prostoduszny natręt;
7) maniak seksualny (erotoman);
8) miłosny natręt[20].

21 Stalking zatem może trwać kilka dni, tygodni, miesięcy, a nawet lat. Średnia długość prześladowania wynosi ok. 21 miesięcy. Długotrwałość prześladowania zależy także od wieku agresora. Im starszy, tym jego działania są lepiej zaplanowane, precyzyjne. Młodsi, szczególnie młodzież, nie posuwa się raczej do długotrwałego zastraszania i prześladowania[21]. Stalking jest coraz bardziej powszechnym zjawiskiem w Polsce. Badania przeprowadzone w 2011 roku przez Instytut Wymiaru Sprawiedliwości pokazują, że aż 9,9% Polaków przyznało się, że było ofiarą stalkingu[22].

22 VIDEOCZATY

W tym miejscu celowe jest zasygnalizowanie nowego niebezpiecznego procesu mogącego być wykorzystywanym w ramach stalkingu – wideoczatów. Jest to w zasadzie już nie tylko proces, ale wprost nowe zjawisko w sieci, co potwierdzają najnowsze badania. Sondaż prowadzony był w reprezentacyjnej grupie 976 gimnazjalistów – internautów w wieku 13–16 lat przez NASK. Z badań wynika, że 2% badanych rozbiera się w sieci na żywo, a wśród 16- latków – aż 5%. Tyle samo nastolatków namawiało do rozbierania rówieśników. Osiem procent przyznało, że choć tego nie robią, to znają kogoś takiego w swoim wieku. Połowa badanych nastolatków przyznała, że nie zdaje sobie sprawy z tego, że za pomocą czatu, ktoś może nagrać wideo, a potem wrzucić do sieci. Połowa deklaruje też, że po poznaniu kogoś na czacie spotyka się z nim w „realu". Ktoś rozpoznał 16-latkę, która licytowała pokaz erotyczny, pod warunkiem, że będzie ją oglądało co najmniej 80 osób. Na tej samej stronie rozbierał się 9-latek[23]. Blisko 80% licealistów, ok. 70% gimnazjalistów i 21% uczniów twierdzi, że

[20] J. Kosińska, *Prawnokarna problematyka stalkingu*, „Prokuratura i Prawo", 10/2008, s. 33.

[21] B. Hołyst, *Psychologia kryminalistyczna,* Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2009, s. 733, 740.

[22] http://prawo.gazetaprawna.pl/grafika/ 520050, 70610,stalking_3_lata_wiezienia_za_uporczywe_nekanie.html, data dostępu 04.01.2012.

[23] A. Pezda, *Twoje dziecko na sekszczacie. Nowa plaga w Internecie*, „Gazeta Wyborcza" 28.11.2013, s. 1.

przynajmniej raz zostało zaatakowanych w Internecie.[24]

23 PODSUMOWANIE PROCEDURA POSTĘPOWANIA W WYPADKU STALKINGU

Procedura obejmuje ochronę i przeciwdziałanie. Najlepszym zabezpieczeniem jest zastosowanie narzędzi filtrujących lub blokujących połączenie z konkretną osobą. Każde postępowanie związane z nowymi zagrożeniami ma ścisły związek z ukształtowanymi kompetencjami[25] . Należy zwrócić uwagę, że o ile w ramach ochrony nie pomoże ignorowanie cybernapaści (co jest najlepszym rozwiązaniem), a wiec niereagowanie na wszelkie e-maile i wiadomości na komunikatorze, celowym jest rozważenie utworzenia bezpiecznego profilu. Nie można też udostępniać swojego hasła, a w nim wrażliwych danych osobowych. Najlepiej posługiwać się pseudonimami. Najgorsze jest zareagowanie, co może inicjować dalsze postępowanie cyberprześladowcy lub też spotkanie ze sprawcą twarzą w twarz. Nie można także prowokować i dać się sprowokować. Osoby niepełnoletnie o takiej sytuacji powinny powiadomić rodziców lub opiekunów, a nawet pedagoga szkolnego.

W wypadku znanego sprawcy nękania należy:

- **wysłać wyraźne ostrzeżenie na piśmie, powinna się w nim znajdować informacja, że kontakt jest nieodpowiedni, niechciany, a także prośba o zaprzestanie wysyłania jakichkolwiek komunikatów;**
- **jeżeli prośba nie pomogła, ofiara powinna złożyć skargę na sprawcę także własnemu operatorowi;**
- **zbierać wszelkie dowody działań sprawcy, wskazane jest zapisywanie przejawów aktywności oraz podejmowanych przeciwdziałań;**
- **zmienić dostawcę usług internetowych, numeru telefonu i adresu e-mailowego.**

O czym jeszcze należy pamiętać?:

- o bezwzględnym przestrzeganiu etykiety podczas aktywności w swawolnych kawiarenkach i grupach dyskusyjnych;
- o uczestniczeniu w czatach moderatora;
- o znajomości narzędzi pozwalających na ignorowanie lub blokowanie uczestników czatów;
- o przestrzeganiu jednoznacznych zasad uczestnictwa w czacie;
- o niekorzystaniu z kamerek internetowych, każda informacja w jakiejkolwiek postaci może być źródłem manipulacji.

Celowe jest zapoznanie się z najnowszymi przepisami (paragrafy Kodeksu karnego) dotyczącymi nękania[26]. Przestępstwo nękania określa art. 207 KK oraz groźbę karalną art. 190 KK[27].

DOBRE PRAKTYKI

ĆWICZENIA 15

[24] J. Ćwiek, *Przemoc i seks w „wirtualnej szkole”*, „Rzeczpospolita” 15.05.2013, s. A4.

[25] Por. A. Andrzejewska, *Nowe kompetencje nauczyciela w zakresie możliwości i zagrożeń cyberprzestrzeni*, w: J. Bednarek, A. Andrzejewska (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Wyd. Difin, Warszawa 2014.

[26] M. Budyń-Kulig, *Kodeks karny. Komentarz do zmian wprowadzanych ustawą z dnia 25 lutego 2011 r.* o zmianie ustawy – Kodeks karny. LEX/EL, 2011.

[27] Tamże, teza 15–31 i 44–49.

BIBLIOGRAFIA:

Andrzejewska A., Bednarek J. (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Wyd. Difin, Warszawa 2014.

Andrzejewska A., *Nowe kompetencje nauczyciela w zakresie możliwości i zagrożeń cyberprzestrzeni*, w: Bednarek J., Andrzejewska A. (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Wyd. Difin, Warszawa 2014.

Bednarek J. (red.), *Człowiek w obliczu szans cyberprzestrzeni*, Wyd. Difin, Warszawa 2014.

Budyń-Kulig M., *Kodeks karny. Komentarz do zmian wprowadzanych ustawą z dnia 25 lutego 2011 r*. o zmianie ustawy – *Kodeks karny*. LEX/EL, 2011.

Ćwiek J, *Przemoc i seks w „wirtualnej szkole"* , „Rzeczpospolita" 15.05.2013, s. A4. Źródło: http://przemocwsieci.cba.pl/ data dostępu: 12. 08.2010.

Hołyst B., *Psychologia kryminalistyczna,* Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2009.

Hołyst B., *Psychologia kryminalistyczna,* Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2009.

Hołyst B., *Psychologia kryminalistyczna,* Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2009, http://www.ies.krakow.pl/wydawnictwo/Prokuratura / pdf/2008/10/4kosinska.pdf, data dostępu 04.01.2012.

Hołyst B., *Psychologia kryminalistyczna,* Wydawnictwo Prawnicze Lexis Nexis, Warszawa 2009.

Kosińska J., *Prawnokarna problematyka stalkingu*, „Prokuratura i Prawo", 10/2008.

Lattanzii M. w: tł. J. Skarzyńska, *Ciemna strona relacji interpersonalnych*, www.stalking.it, data dostępu 11.04.2007.

Pezda A., *Twoje dziecko na seksczcie. Nowa plaga w Internecie*, „Gazeta Wyborcza" 28.11.2013.

Plis J., *Cyberstalking. Podstawowe problemy prawnokarnej ochrony,* w: Bednarek J., Bębas S., Plis J., *Patologie w cyberprzestrzeni*, WSH w Radomiu, Radom 2002.

Szumilak A., *Jak się bronić przed agresją w Internecie,* „Świat Wiedzy", 3/2011.

Szymczak M. (red.), *Słownik języka polskiego*, PWN, Warszawa 1992.

Woźniak W., Lattanzi M., *Stalking – między przemocą a uzależnieniem,* Wydawnictwo Bernard Cichosz, Kutno 2010.

STRONY INTERNETOWE:

bip.kprm.gov.pl/download.php?s=75&id=488,
data dostępu 02.01.2012.

bip.kprm.gov.pl/download.php?s=75&id=488,
data dostępu 02.01.2012.

http://prawo.gazetaprawna.pl/grafika/520050,70610,stalking_3_lata_wiezienia_za_uporczywe_nekanie.html,
data dostępu 04.01.2012.

http://psychologia.net.pl/artykul.php?level=282, data dostępu 03.01.2012.

http://stalking.prv.pl/,
data dostępu 03.01.2012.

http://www.ies.krakow.pl/wydawnictwo/prokuratura/pdf/2008/10/4kosinska.pdf,
data dostępu 02.01.2012.

http://www.psychologia.net.pl/artykul.php?level=415, data dostępu 02.01.2012.

ZAGROŻENIA SPOŁECZNO-WYCHOWAWCZE

SZCZEGÓŁOWY
PROGRAM SZKOLENIA

Anna Andrzejewska

PROGRAM KSZTAŁCENIA - ZAGROŻENIA SPOŁECZNO-WYCHOWAWCZE	
Sposób realizacji	Wykład, warsztaty
Materiały	**Materiały dydaktyczne dla uczestników szkolenia składają się z:** podręcznik, materiały szkoleniowe
Treści merytoryczne	Sekty (rodzaje sekt, charakterystyka najbardziej groźnych sekt, fazy werbunku, charakterystyka ofiary). Pedofilia (charakterystyka zjawiska, charakterystyka ofiary i sprawcy, praca z dzieckiem wykorzystywanym i jego rodziną). Pornografia dziecięca (charakterystyka zjawiska, wpływ na psychikę dziecka, charakterystyka sprawcy i ofiary, omówienie możliwości ograniczenia dostępu do stron z treściami pornograficznymi, omówienie podstawowych zasad bezpieczeństwa przy korzystaniu z sieci). Seksting (omówienie zjawiska, charakterystyka ofiar sekstingu, omówienie wpływu zjawiska na psychikę dzieci).
Obszary	Efekty kształcenia
Wiedza zdobyta w czasie zajęć	W wyniku przeprowadzonych zajęć, Uczestnik powinien być w stanie: zdiagnozować zagrożenia związane z korzystaniem z portali poświęconych sektom, pornografii, pedofilii, sekstingowi. Znać terminy takie jak: seksting videoczat, skalę zjawiska
Umiejętności zdobyte w czasie zajęć	W wyniku przeprowadzonych zajęć Uczestnik powinien umieć: udzielać wsparcia osobom korzystającym z portali poświęconych: sektom, pornografii, pedofilii, sekstingowi w tym: wymienić podstawowe objawy zjawisk, charakteryzować sprawców i ofiary, znać podstawowe zapisy prawne
Forma zajęć	Dyskusja i ćwiczenia aktywizujące
Metody prowadzenia zajęć	Prezentacja Power Point, dyskusja, ćwiczenia w grupach, analiza case study
Zalecane ćwiczenia	Ćwiczenia 9-14 znajdujące się w module *Kształcenie*

Sprawdzenie efektów szkolenia	Ankiety, testy kompetencyjne

ZAGROŻENIA ZWIĄZANE Z UZALEŻNIENIAMI

INTERNET ŹRÓDŁEM
INFORMACJI O SUBSTANCJACH ODURZAJĄCYCH I DOPINGUJĄCYCH

Anna Andrzejewska

1 WPROWADZENIE

Zagrożenia te stanowią kolejny obszar wielu tradycyjnych i nowych zagrożeń. W tym kontekście należy podkreślić, iż

termin uzależnienie należy postrzegaćna dwa sposoby[1]:

- uzależnienie od przdmiotów i czynności z nim związanych,
- lub jako uzależnienie od treci przez te media przekazywanych[2].

Najmłodsze pokolenie znajduje w internecie wiele interesujących informacji o możliwościach nabycia substancji odurzających i dopingujących po znacznie niższej cenie i o „wspaniałych" efektach działania. Dynamicznie zatem, w ostatnich latach, poszerza się oferta kupowania i zażywania tych pozornie bezpiecznych substancji o nieznanym składzie chemicznym. W tym miejscu dodajmy, że nie są to już tylko narkotyki, papierosy czy alkohol, ale coraz nowsze generacje sterydów i anabolików, napojów energetyzujących i dopalaczy oraz innych substancji niezwykle groźnych dla najmłodszego pokolenia. Wśród nich znajdują się także lekarstwa nabywane legalnie w dużych ilościach nie tylko w aptekach, ale także w sieci. Szerszy kontekst tych zagrożeń w kontekście właśnie narkotyków i leków przedstawia w swoich analizach J. Korczak[3].

2 W poniższych rozważaniach celowe jest zwrócenie uwagi na przemiany związane z funkcjonowaniem i modą najmłodszego pokolenia oraz jego aktywnością w cyberprzestrzeni. Warto dodać, że w ewolucji zostaliśmy obdarzeni przez los skłonnością do nałogów, zakorzenioną dysfunkcją sprawności woli, przejawiającą się chronicznym podejmowaniem szkodliwych dla organizmu decyzji. Są one sprzeczne z przesłankami zdrowego rozsądku. Od alkoholizmu, poprzez uzależnienie od nikotyny, poszerzyliśmy gamę możliwości wraz z rozwojem cywilizacji.

3 Współczesny świat charakteryzuje się dynamicznym tempem zmian i dążeniem do doskonałości, co niesie za sobą nieustanny stres, pęd i brak czasu. Taka rzeczywistość wymusza na młodych ludziach szybsze wchodzenie w świat ludzi dorosłych i skrócenie okresu dzieciństwa. Dorastająca młodzież, goniąc za ideałem, nie radzi sobie z rzeczywistością i coraz częściej sięga po różnego rodzaju substancje dopingujące zwiększające wydajność ich mózgu i organizmu.

4 Sieć jest przepełniona informacjami o substancjach odurzających i dopingujących, ofertami ich kupna i sprzedaży, blogami zawierającymi wyznania ludzi uzależnionych. Wszystko to może mieć duży wpływ na młodzież, jej psychikę i relacje społeczne.

5 INTERNET JAKO NOWA PRZESTRZEŃ HANDLU NARKOTYKAMI

Internet stał się w ostatnim czasie popularnym miejscem dystrybucji substancji odurzających i dopingujących. Wystarczy wpisać w przeglądarkę internetową słowa „narkotyki", „dopalacze", „sterydy", lekarstwa itp., a natychmiast wyświetlą się strony, za pośrednictwem których można nabyć odpowiednią substancję. Strony te na pierwszy rzut oka mają charakter informacyjny, ale wystarczy zagłębić się w nie, a okaże się, że dotrzemy do bardziej szczegółowych informacji. Na forach internetowych także możemy uzyskać wiele informacji, jakie środki zażywać i jak działają. Wypowiedzi są sprzeczne, dlatego młody człowiek poszukujący informacji na ten temat bardzo

[1] według takiej logiki zostały ułożone treści w niniejszym module (przyp. red.)

[2] M. Filipiak, *Homo Comunicans. Wprowadzenie do teorii masowego komunikowania*. Wyd. Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2003, s. 192.

[3] Por. J. Korczak, *„Kop" i „odlot" w wirtualnym świecie*, w: A. Andrzejewska, J. Bednarek (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Wyd. Difin, Warszawa 2014.

często jest zdezorientowany co do sposobu zażywania i szkodliwości tych specyfików.

6 W sieci potencjalnemu młodemu i nieświadomemu internaucie dostarczana jest szeroka gama różnego rodzaju argumentów pronarkotykowych. Budowane są pozytywne skojarzenia, które odwołują się do psychologicznych procesów charakterystycznych dla okresu dojrzewania, np. poszukiwania tożsamości, a także do procesów kulturowych i liberalizacji postaw.

7 Wiele ze stron internetowych zajmujących się tematyką związaną z substancjami psychoaktywnymi często zawiera informacje nieprawdziwe. Zjawisko, które również dotyczy tych stron, to pomijanie ważnych informacji dotyczących wpływu narkotyków na zachowanie czy też zdrowie człowieka.

8 Młodzież, która jest częstym bywalcem takich stron, nie porównuje wiadomości zdobytych w sieci z wiarygodnymi źródłami, takimi jak podręczniki czy encyklopedie. Interesuje się tylko doznaniami i opiniami ludzi, którzy zażywali bądź zażywają jakąś substancję. Szczególnie młodzież w wieku gimnazjalnym cechuje ciekawość i chęć poznawania nowych, zakazanych rzeczy. Cóż innego może zaspokoić ciekawość młodego człowieka, jak nie przepełniony informacjami Internet. Można tu znaleźć wszystko: informacje o samych substancjach, możliwościach ich zażywania, potencjalnych skutkach oraz całą gamę ofert handlowych z nimi związanych.

9 **DOSTĘPNOŚĆ NARKOTYKÓW W SIECI**

Aby przedstawić, jak prosty jest proceder związany z handlem substancjami odurzającymi w Internecie i jak łatwy dla młodzieży, dziennikarka „Gazety Wyborczej", dokonała pewnego eksperymentu. Siedząc w domu i korzystając tylko z Internetu i karty kredytowej, już w kilka dni zdobyła uchodzący za jeden z najbardziej uzależniających i niebezpiecznych narkotyków – heroinę. Za 200 złotych kupiła porcję tego narkotyku, którą można podzielić na 70 mniejszych porcji. Od komputera odeszła tylko raz – by wyjąć narkotyk ze skrzynki pocztowej. Był on zapakowany w kopertę i wyglądał jak najzwyklejsza przesyłka pocztowa. W drugiej przesyłce diler z Holandii – po uznaniu dziennikarki za stałego klienta – zaoferował jej 25 gramów heroiny, czyli grubo ponad 2 tys. działek[4].

10 Młodzi ludzie bardzo często sięgają po pierwszą substancję psychoaktywną właśnie z ciekawości, czasem z nudy, a bardzo często za namową rówieśników.

11 Przy promowaniu środków psychoaktywnych, najczęstszym chwytem jest dostarczenie odbiorcy pozytywnego skojarzenia zarówno z tematyką, jak i poszczególnymi substancjami psychoaktywnymi. Podstawowym narzędziem promocji środków psychoaktywnych jest humor, odwoływanie się do takich wartości, jak wolność, korzyści natury społecznej oraz kreowanie wizji nowoczesnego, wyluzowanego stylu życia.

12 Portale rozrywkowe, które są bardzo popularne w Internecie, reklamując się jako np. „plotka o gwiazdach", „sensacja" lub też „komentarz", często przyciągają całe rzesze młodych odbiorców, którzy żądni są informacji o idolach swojego życia. Na łamach tych portali dzielą się oni również między sobą poglądami, wymieniają informacjami, nie tylko na temat mody czy urody, ale również na temat narkotyków i innych substancji psychoaktywnych obecnych w show biznesie. Portale te są tworzone pod młodego odbiorcę, odpowiadając zawartością swoich materiałów – plotek, sensacji – jego aspiracjom a także potrzebie naśladownictwa.

[4] Pełna treść artykułu na stronie, http://wyborcza.pl/10,82983,11440174,Heroina_w__Gazecie_Wyborczej_.html

13 **Eksperymentowanie ze środkami psychoaktywnymi polega zwykle na nieplanowanym i spontanicznym ich zażywaniu i to w niewielkich ilościach**. Motywem nastolatków jest przeważnie pokusa podkreślenia dorosłości i chęć zrobienia czegoś na przekór rodzicom.

Eksperymentując, nastolatki uświadamiają sobie efekt zmian nastroju i uczą się umiarkowanego dawkowania, a więc takiego, które pozwala osiągnąć pożądany poziom poprawy nastroju. Gdy ta sztuka zostanie opanowana, „eksperyment" dobiega końca, a kolejne oszołomienie się jest przeżyciem zaplanowanym i pożądanym.

14 TYPY UZALEŻNIEŃ I PRZYCZYNY ZAŻYWANIA SUBSTANCJI PSYCHOAKTYWNYCH

„Substancje psychoaktywne są to substancje chemiczne, które oddziałują na centralny układ nerwowy, wpływając bezpośrednio na pracę mózgu i wywołując zmiany w zachowaniu, postrzeganiu, nastroju i świadomości"[5].

15 Do uzależnień od substancji psychoaktywnych zaliczamy: „alkoholizm, nikotynizm, narkomanię, lekomanię, uzależnienie od substancji wzmacniających – sterydy, dopalacze, uzależnienie od innych substancji psychoaktywnych"[6].

Są to substancje chemiczne najbardziej charakterystyczne dla dzisiejszych czasów, dla szybkiego postępu cywilizacyjnego oraz dla nowych wzorców zachowań i nowych warunków życia.

16 Przyczyny uzależnień chemicznych są bardzo różne i nie są do końca jednoznacznie określone. Do najczęściej spotykanych przyczyn uzależnienia w literaturze wymieniane są: biopsychiczne, psychospołeczne i kulturowe.

„**Przyczyny biopsychiczne** – bardzo wysoka indywidualna podatność na uzależnienie, pobudliwość psychiczna, labilność układu nerwowego, bardzo niska odporność na stres, zaburzenia rozwoju osobowości oraz natury emocjonalnej, neurotyzm, uszkodzenie mózgu, choroby somatyczne takie jak bezsenność, silne bóle.

Przyczyny psychospołeczne – brak zaspokojenia potrzeb psychicznych lub też trudności w ich zaspokojeniu na skutek złego oddziaływania środowiska rodzinnego, szkolnego i wychowawczego np. akceptacji, bezpieczeństwa, identyfikacji, wszelkie niepowodzenia życiowe, zawodowe, osobiste – jest to pewnego rodzaju ucieczka od tych problemów w wyimaginowany świat iluzji.

Przyczyny kulturowe – jest to moda, postawy hedonistyczne, dostępność środków uzależniających, brak celów i perspektyw życiowych a także rozrywek i innych atrakcji spędzenia wolnego czasu, przynależność do grup subkultury młodzieżowej, w której zażywa się środki uzależniające, chęć eksperymentowania i odniesienia sukcesu"[7].

17 DIAGNOZA

Do stwierdzenia uzależnienia, muszą wystąpić najmniej trzy z sześciu podanych niżej objawów:

1. **„Silne pragnienie lub też poczucie przymusu przyjmowania substancji.**

[5] A. Miszczak, *Na czym polega profilaktyka uzależnień?,* http://nalogi.wieszjak.pl, data dostępu: 13.01.2013.

[6] M. Jędrzejko, *Współczesne teorie uzależnienia od substancji psychoaktywnych,* Oficyna Wydawnicza ASPRA-JR, Pułtusk – Warszawa 2009, s 35.

[7] A. Nowak, E. Wysocka, *Problemy i zagrożenia społeczne we współczesnym świecie. Elementy patologii społecznej i kryminologii,* Wydawnictwo Naukowe „Śląsk", Katowice 2001, s. 73.

W praktyce oznacza to, iż osoba musi przyjąć substancję psychoaktywną, od której jest uzależniona, aby poczuć się dobrze lub nie czuć się źle.

2. **Trudności w kontrolowaniu zachowania, które związane jest z przyjmowaniem substancji psychoaktywnej, zakończenia lub ilości przyjmowanej substancji**. Jeśli dana osoba już sięgnie po środki odurzające, to w bardzo krótkim czasie zaczyna powtarzać tę czynność – dochodzi zatem do tzw. ciągu.

3. **Fizjologiczne objawy odstawienia** – tzw. zespół abstynencyjny. Substancje uzależniające, które przyjmowane są przez daną osobę, dają nie tylko objawy podczas ich brania, ale także w czasie ich odstawiania.

4. **Wzrost tolerancji** – małe, początkowe dawki już nie wystarczają, potrzebne są coraz większe dawki do wywołania upragnionego stanu przyjemności.

5. **Zaniedbywanie innych, wcześniejszych źródeł przyjemności**. Osoba uzależniona traci wszelkie zainteresowanie dotychczasowymi pasjami. Interesuje się tylko i wyłącznie braniem narkotyków. Zamyka się również w środowisku osób, które zażywają daną substancję uzależniającą.

6. **Przyjmowanie substancji psychoaktywnych mimo doświadczania jej szkodliwości.** Pomimo pobytów w izbie wytrzeźwień, uszkodzenia wątroby, osoby uzależnione wciąż zażywają dany narkotyk. Przymus jest silniejszy niż zdrowy rozsądek”[8].

CHARAKTERYSTYKA WYBRANYCH NARKOTYKÓW

18 Substancje odurzające, w tym także narkotyki, towarzyszą światu od wieków. W miarę rozwoju cywilizacji zmieniało się ich przeznaczenie: były zarówno lekarstwem, jak i substancją ułatwiającą kontakt z bogami i innym światem[9]. Elementem łączącym te formy jest niewątpliwie chęć oderwania się od realnej rzeczywistości i przeniesienie się w inny wymiar, z dala od zmartwień życia codziennego. Każde zażycie substancji psychoaktywnych będzie niosło za sobą ryzyko uzależnienia. **Uzależnienie od środków psychoaktywnych występuje wtedy, kiedy osoba traci kontrolę nad częstotliwością i ilością przyjmowanej substancji i w konsekwencji dochodzi do tzw. przymusu jej zażywania.**

19 Należy jednak pamiętać, że w każdym indywidualnym przypadku o uzależnieniu decyduje inny splot przyczyn. Etiologia uzależnienia od środków psychoaktywnych jest bardzo złożona, co w efekcie znacznie utrudnia prawidłową diagnozę, a co za tym idzie skuteczne działania profilaktyczne i terapeutyczne. Pojęcie „narkotyk” obejmuje „substancje uzależniające, które mają działanie pobudzające, czyli środki psychostymulujące np. amfetamina, kokaina, substancje o działaniu silnie hamującym np. barbiturany, alkohole, benzodiazepiny oraz środki psychodysleptyczne – halucynogenne np. LSD-25, meskalina”[10].

20 Mianem narkotyku określa się substancje odurzające pochodzenia naturalnego lub syntetycznego. Do grupy narkotyków naturalnych zaliczamy:

[8] J. Uziałło, *Biologiczne podstawy uzależnień,* Serwis Informacyjny Narkomania, 2(46)/2009, s. 21.

[9] W. Knapik, *Uzależnienia jako problem cywilizacyjny XXI wieku,* Wyd. Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie, Kraków 2010, s. 85.

[10] *Narkotyki i ty*, http://www.narkotyk.co, data dostępu: 14.02.2013.

- pochodne makowca – opium, heroina, kodeina, morfina;
- pochodne rośliny koka i kokaina;
- pochodne konopi indyjskich – haszysz, marihuana;
- pochodne wybranych grzybów, kaktusów, krzewów i roślin posiadających właściwości halucynogenne[11].

21 Największą popularnością wśród substancji o pochodzeniu syntetycznym cieszą się narkotyki z grupy amfetaminowej.

22 **Amfetamina** to środek psychostymulujący, który powoduje długotrwałe pobudzenie. W ciągu ostatniego stulecia używana była w medycynie jako środek odchudzający stosowany przez osoby otyłe, a także przez sportowców jako tzw. koks (doping). Pod inną nazwą – benzedryna, była stosowana w medycynie ok. 80 lat temu, do leczenia astmy oskrzelowej oraz napadowej senności. Amfetamina przyjmowana jest dożylnie, doustnie, palona i wdychana przez nos. Występuje w postaci bezwonnego proszku o gorzko-cierpkim smaku w kolorze od białego do ceglastego. Pobudzenie, które towarzyszy zażyciu amfetaminy może trwać od 2 do 3 godzin, w zależności od spożytej dawki[12].

23 Objawy zażycia amfetaminy (działanie fizjologiczne):

- brak apetytu,
- jadłowstręt,
- silne pobudzenie psychomotoryczne,
- rozszerzenie źrenic,
- przyspieszona akcja serca i szybki oddech,
- podwyższone ciśnienie krwi,
- częstsze wydalanie moczu,
- uczucie suchości w ustach,
- uszkodzenia szkliwa zębów.

24 Efektem zażycia amfetaminy jest ogromny przypływ energii i znaczne podwyższenie nastroju, aż do euforii. Osoby będące pod wpływem tego narkotyku wykazują się wzmożoną aktywnością, której towarzyszy bezsenność. Mają polepszoną koncentrację i możliwość maksymalnego skupienia uwagi. Towarzyszy im poczucie pewności i mocy. Negatywnymi efektami działania amfetaminy są: drażliwość i agresywność, przymglona świadomość oraz wrażenie obecności insektów na skórze tzw. formikacje[13].

25 Amfetamina wykazuje bardzo silne właściwości uzależniające, które wywołuje atrakcyjny przebieg działania narkotyku. Zależność psychiczna wzmacniana jest przez przykre dolegliwości związane z jej odstawieniem.

26 **Ecstasy (MDMA)** jest pochodną amfetaminy i meskaliny – z jednej strony działa stymulująco na układ nerwowy, z drugiej posiada właściwości halucynogenne. W przeszłości środek ten miał zastosowanie w psychoterapii, co było związane z jego właściwościami wyzwalającymi empatię[14]. Tabletki ecsta-

[11] T W. Knapik, *Uzależnienia jako problem cywilizacyjny XXI wieku,* Wyd. Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie, Kraków 2010, s. 87.

[12] L. Jurek, *Dopalacze, narkotyki niewinny początek,* Wyd. Śląskie Centrum Wydawniczo-Handlowe „Lexdruk", Rybnik 2010, s. 47.

[13] Tamże, s 48.

[14] Empatia – w psychologii zdolność odczuwania stanów psychicznych innych osób (empatia emocjonalna), umiejętność przyjęcia ich sposobu myśle-

sy to bardzo kolorowe lub też białe pastylki, które mają wytłoczone napisy lub wzorki (np. sierp, kot, ptak itp.). „Jest to najczęściej mieszanka zawierająca kilka rodzajów środków psychoaktywnych o różnym składzie, jakości oraz stężeniu np. amfetaminy i LSD”[15]. Wszystko to powoduje, że konsumenci sięgając po tabletki ecstasy grają w „rosyjską ruletkę”. Jej działanie ustępuje po kilku godzinach od chwili zażycia.

27 Objawy zażycia ecstasy (działanie fizjologiczne):

- rozszerzenie źrenic,
- wzmożenie odruchów,
- wzrost temperatury ciała,
- pobudzenie i brak łaknienia,
- szczękościsk,
- nudności i wymioty,
- odwodnienie,
- kołatanie serca i tachykardia[14],
- nagłe wzrosty ciśnienia i uderzenia krwi do głowy.

28 Działanie ecstasy zależy od nastroju i sytuacji osoby, która zażywa środek. Jeśli stan psychiczny danej osoby jest zły, może ulec pogorszeniu po zażyciu ecstasy. Pozornie „pozytywnymi” skutkami zażycia MDMA są: euforia i przypływ energii, uczucie empatii i silnej więzi z otoczeniem, intensyfikacja przeżyć emocjonalnych, pobudzenie seksualne i zaostrzenie percepcji otoczenia. Do negatywnych oddziaływań możemy zaliczyć: napięcie emocjonalne, poczucie utraty kontroli, niepokój, który może przerodzić się w panikę, nadwrażliwość na bodźce zewnętrzne, nieprzyjemne halucynacje i depresję[17].

29 Uczucie silnej euforii towarzyszące działaniu ecstasy i przykre dolegliwości związane z jej odstawieniem decydują o uzależniających właściwościach tej substancji. Po zażyciu MDMA następnego dnia często pojawia się tzw. kac, który charakteryzuje się: mdłościami, zmęczeniem, słabą koncentracją, sennością lub pobudzeniem i irytacją.

30 Przełom XIX i XX wieku przyniósł rozwój narkomanii kokainowej. **Kokaina** charakteryzuje się silnym działaniem pobudzającym, wprowadza układ nerwowy w stan nadaktywności. Podana miejscowo wykazuje właściwości znieczulające, przez co znalazła zastosowanie w medycynie. Obecnie z powodu skutków ubocznych jest ona zastępowana przez nowe, mniej szkodliwe środki znieczulające. Pozostaje jednak wciąż wykorzystywana jako miejscowy środek znieczulający w okulistyce i otorynolaryngologii.

31 **Kokaina** występuje pod postacią krystalicznie białego proszku. Zazwyczaj przyjmowana jest wziewnie do nosa, gdzie śluzówka wchłania ją niemal natychmiast, wywołując wpływ na ośrodki przyjemności w mózgu. Bywa też wcierana w środek małżowiny usznej lub dziąsła. Przyjmowana doustnie działa dużo słabiej, jednak znieczula błonę śluzową żołądka, przez co zanika uczucie głodu. Kokaina może być także palona poprzez dodanie jej do skrętów marihuany lub papierosów.

nia, spojrzenia z ich perspektywy na rzeczywistość (empatia poznawcza).

[15] H. Kuntz, *Narkotyki i uzależnienia. Wszystko o czym należy wiedzieć*, Wydawnictwo Edukacyjne Parpamedia, Warszawa 2009, s. 96.

[16] Tachykardia inaczej częstoskurcz – przyspieszenie akcji serca powyżej 100 uderzeń na minutę.

[17] L. Jurek, *Dopalacze, narkotyki niewinny początek,* Wyd. Śląskie Centrum Wydawniczo-Handlowe „Lexdruk”, Rybnik 2010, s. 56.

32 Działanie fizjologiczne kokainy:

- opóźnia objawy zmęczenia,
- zmniejsza potrzebę jedzenia i snu,
- silnie rozszerza źrenice, zakłóca pracę serca,
- prowadzi do pobudzenia psychoruchowego,
- jest przyczyną wzrostu ciśnienia krwi i przyspieszenia oddechu,
- zażycie większych dawek może spowodować wzrost temperatury ciała i drżenie mięśniowe.

33 Pozornie pozytywnymi efektami działania, z powodu których młodzież sięga po kokainę są: odczucie silnej euforii, pobudzenie ruchowe i podniecenie seksualne, intensywne poczucie mocy fizycznej i umysłowej, zanik zdolności odczuwania przykrych wrażeń, poczucie wyższości, odsunięcie poczucia lęku. Zażycie kokainy powoduje również skrócenie czasu reakcji psychicznej – przyśpieszeniu ulegają procesy myślowe. Negatywne odczucia, z jakimi mogą spotkać się osoby przyjmujące kokainę to: niepokój i napięcie, bezsenność, załamanie nerwowe, urojenia o nieprzyjemnej treści oraz brak krytycyzmu co do własnych zachowań[18].

34 Przyjmowanie kokainy prowadzi do powstania silnego uzależnienia psychicznego, szczególnie u osób palących tzw. crack, który jest krystaliczną formą kokainy. Wykazuje on od 20 do 30 razy silniejsze działanie od kokainy będącej w nielegalnym handlu. Można spotkać go w formie białych kawałeczków przypominających z wyglądu płatki mydlane lub pod postacią jasnobrązowych kuleczek.

35 Nadużywanie kokainy prowadzi do silnego wyniszczenia organizmu, które spowodowane jest brakiem łaknienia i snu. Może powodować zaburzenia osobowości oraz przygnębienie skutkujące próbami samobójczymi.

36 Najbardziej rozpowszechnionymi i popularnymi narkotykami w Polsce i na świecie są pochodne konopi indyjskich – **marihuana i haszysz**. W medycynie działanie THC[19] wykorzystywane jest do obniżenia ciśnienia śródgałkowego, przeciwwymiotnie i przeciwdrgawkowo. Marihuana jest suszem z kwiatostanu i liści konopi, zawiera 0,5–5% THC. Haszysz to żywica krzewu konopi, zawiera 2–19% THC. Największą zawartość THC (10–30%) zawiera olej haszyszowy powstały z rozpuszczonej żywicy konopi. Najczęstszą formą przyjmowania preparatów powstałych z konopi jest ich palenie[20].

37 W zależności od warunków konopie mogą działać pobudzająco, uspakajająco, znieczulająco lub lekko halucynogennie.

38 Przy zażywaniu pochodnych konopi można zaobserwować następujące objawy fizjologiczne:

- wzrost ciśnienia krwi i przyśpieszone tętno,
- pocenie się,
- wysuszenie śluzówek jamy ustnej, niekiedy ataki kaszlu,
- zwiększenie apetytu,
- przekrwienie gałek ocznych, spojówek, czasami obrzęk powiek,
- zawroty i bóle głowy,
- zaburzenia pamięci,
- zaburzenia koordynacji ruchowej, uwagi i możliwości uczenia się,
- gorszą ogólną sprawność psychofizyczną.

[18] M.Jędrzejko, A. Kowalewska, W. Janiszewski, *Charakterystyka narkotyków*, w: M. Jędrzejko (red.), *Narkomania spojrzenie wielowymiarowe*, Wyd. Akademia Humanistyczna im. Aleksandra Gieysztora, Pułtusk-Warszawa 2009, s. 242.

[19] THC (Tetrahydrokannabinol) – organiczny związek chemiczny z grupy kannabinoidów, izomer kannabidiolu i główna substancja psychoaktywna zawarta w konopiach.

[20] L. Jurek, *Dopalacze, narkotyki niewinny początek,* Wyd. Śląskie Centrum Wydawniczo-Handlowe „Lexdruk", Rybnik 2010, s. 71.

39 Odczucia po zażyciu THC są zależne od cech osobowości danej osoby, wielkości i drogi przyjętej dawki, stanu emocjonalnego w momencie przyjęcia, obecności innych osób oraz od współdziałania tego preparatu z innymi np. z alkoholem. Pozornie „pozytywnymi" aspektami zażywania preparatów konopi jest: odprężenie i poczucie spokoju, zwiększenie poczucia przyjemności seksualnych, optymizm i podniesiona samoocena, wzrost wrażliwości zmysłów, zmiana poczucia mijającego czasu (mijający wolniej). Do negatywnych efektów ich działania możemy zaliczyć: skłonność do ulegania sugestiom, nieracjonalne myśli, zagubienie, zwiększone napięcie i niepokój, pogorszenie pamięci, apatia, lęki i urojenia oraz niemożność skupienia uwagi na wielu rzeczach naraz[21].

40 DOPALACZE

Termin **„dopalacze"** jest określeniem używanym w języku potocznym dla określenia grupy substancji czy produktów pochodzenia naturalnego lub syntetycznego, które posiadają psychoaktywne właściwości i oddziałują na ośrodkowy układ nerwowy. Uważa się również, że zażywanie tych substancji może wiązać się z ryzykiem zdrowotnym, a w szczególności z uzależnieniem[22].

41 Na rynku polskim możemy znaleźć szeroki asortyment środków zmieniających świadomość. W ofercie są środki relaksujące, pobudzające, jak i o działaniu halucynogennym. Zażywa się podobnie do narkotyków, doustnie, poprzez palenie lub wciąganie do nosa.

42 Wśród dopalaczy syntetycznych największą popularnością do tej pory cieszyła się pochodna piperazyny, czyli **benzylpiperazyna (BZP)**. BZP występuje pod postacią białego proszku, najczęściej w tabletkach lub kapsułkach. Jest to substancja psychoaktywna o działaniu stymulującym, która imituje działanie substancji MDMA, wchodzącej w skład ecstasy oraz amfetaminy.

43 U użytkowników BZP mogą pojawić się następujące efekty uboczne:

- bóle brzucha i głowy,
- wymioty, nudności,
- kołatanie serca,
- brak apetytu,
- stany lękowe,
- bezsenność,
- zmiany nastroju,
- dezorientacja,
- drgawki,
- okresowa impotencja.

44 **TFMPP (trifluorometylofenylpiperazyna)** jest substancją psychoaktywną o działaniu stymulującym. Zwykle występuje w połączeniu z BZP pod postacią kapsułek i tabletek. Mechanizm działania, wg niektórych źródeł, podobny jest do MDMA, wg innych przypomina raczej mieszankę LSD[23] z amfetaminą.

45 Jej zażycie powoduje następujące działania niepożądane:

- bóle głowy i migreny,
- brak apetytu,
- bezsenność,
- wymioty,
- przyspieszenie tętna.

[21] Tamże, s. 70–71.

[22] B. Bukowska, M. Kidawa, D. Chojecki, *Dopalacze,* „Remedium Profilaktyki i Promocja Zdrowego Stylu Życia", 5 (195)/2009.

[23] LSD– Dietyloamid kwasu D-lizergowego, organiczny związek chemiczny, psychodeliczna substancja psychoaktywna, pochodna ergoliny.

46 **JWH-018** jest to substancja charakteryzująca się dużym powinowactwem do receptorów kanabinoidowych, określana jako kanabinopodona[24]. Występuje w postaci grudkowatej, twardej, lepkiej substancji przypominającej haszysz. Może mieć barwę od ciemnej do jasnobrązowej, czasem rudej przypominającej rdzę. Sprowadzana jest głównie z Chin, najczęściej dodawana jest do mieszanek ziołowych. Działanie JWH-018 nie zostało zbadane klinicznie. Użytkownicy substancji twierdzą, że wykazuje ona działanie zbliżone do marihuany i haszyszu.

47 Podaje się, że JWH-018 wywołuje:

- wzrost ciśnienia krwi,
- przekrwienie gałek ocznych,
- zaburzenia uwagi i koordynacji ruchowej,
- wysuszenie śluzówek,
- zawroty głowy.

48 **Mefedron (4-MMC)** jest syntetyczną substancją wykazującą zarówno działanie stymulujące jak i entaktogenne[25]. Postać fizyczna mefedronu to biały proszek, który stanowi sól rozpuszczalną w wodzie. Występuje także w formie tabletek i pigułek, rzadziej w postaci płynnej. Fizjologiczne efekty działania tej substancji zbliżone są do amfetaminy i jej pochodnych. W niewielkich dawkach mefedron prowadzi do poprawy nastroju, wywołuje euforię i pobudzenie, zwiększa chęć konwersacji i otwartość oraz zmniejsza łaknienie. Mogą pojawić się również: halucynacje, zaburzenia pamięci krótkotrwałej, spadek koncentracji, rozdrażnienie, bezsenność, stany paranoidalne i depresyjne.

49 Objawy zażycia mefedronu (działanie fizjologiczne):

- tachykardia (kołatanie serca),
- wzrost ciśnienia krwi,
- zgrzytanie zębami i szczękościsk,
- oczopląs,
- podrażnienie śluzówek nosa,
- zawroty i bóle głowy,
- problemy z oddychaniem,
- bóle w klatce piersiowej,
- drżenie rąk,
- nudności,
- drgawki.

50 Oprócz dopalaczy syntetycznych, możemy wyróżnić całą gamę dopalaczy naturalnych, do których zaliczamy **mieszanki ziołowe** o działaniu psychodelicznym[26]. Mieszanki ziołowe można łatwo przedawkować.

51 Jedną z najpopularniejszych mieszanek ziołowych jest **szałwia wieszcza**, zwana też **Lady SD** lub **Boską szałwią**. Głównym składnikiem tej mieszanki jest salwinoryna, jedna z najsilniejszych naturalnych substancji halucynogennych. Postacią fizyczną Lady SD jest susz roślinny (skręty, liście) i ekstrakt. Najczęstszym sposobem zażywania szałwii jest palenie lub zażywanie drogą doustną. Bezpośrednio po zapaleniu szałwii, palący traci kontrolę nad swoim zachowaniem. Efekty działania tej substancji są bardzo zróżnicowane, zależą od indywidualnych cech organizmu osoby użytkującej, nastroju i dawek przyjmowania.

[24] K. Warecki, *Dopalacze,* Polskie Wydawnictwo Encyklopedyczne, Radom 2010, s. 53.

[25] Entaktogenny – wyzwalający empatię.

[26] Psychodeliczny – odznaczający się wzmożoną wrażliwością na bodźce i skłonnością do urojeń, zwłaszcza euforycznych.

52 Po jej zażyciu mogą wystąpić:

- silne halucynacje i urojenia,
- ataki szału,
- koszmary,
- utrata świadomości,
- przejściowa utrata pamięci,
- dreszcze i zlewne poty.

53 Dużym zainteresowaniem wśród konsumentów dopalaczy cieszą się grzyby halucynogenne. Pod komercyjną nazwą **Flyagaric** kryje się substancja, której składnikiem jest **muchomor czerwony**. Żucie wysuszonych lub świeżych owocników grzyba oraz wypijanie wywarów z nich wywołuje stan odurzenia przypominający stan upojenia alkoholowego[27]. Następnie występują halucynacje słuchowe i wzrokowe. Czasem pojawia się pobudzenie psychomotoryczne i nadmierna wrażliwość wszystkich zmysłów.

54 W dalszej fazie działania występują:

- osłabienie i zmęczenie,
- zaburzenia równowagi,
- pocenie się,
- zawroty głowy,
- szum w uszach,
- nudności, wymioty i biegunka,
- przyspieszenie tętna,
- gorączka do 40°C,
- zaczerwienienie skóry,
- zniesienie reakcji źrenic na światło (przy silnym ich rozszerzeniu może doprowadzić do oślepienia),
- przy dużych dawkach mogą wystąpić: skurcze, głęboka śpiączka z obniżeniem ciśnienia krwi i zaburzeniami oddechu.

55 **Kratom** jest dopalaczem uzyskanym z wysuszonych i sproszkowanych liści lub z ekstraktu z suszonych liści drzewa **Mitragynaspeciosa**. Ekstrakt działa około 30 razy silniej niż same liście. Żucie liści oraz picie wywarów lekko pobudza. W wyższych dawkach może powodować kolejno euforię, błogostan i senność.

56 Wyżej wymienionym objawom towarzyszą:

- wymioty,
- brązowienie skóry,
- osłabienie potencji seksualnej,
- obniżenie sprawności psychomotorycznej.

57 Dopalacz **Argyreianervosa**, czyli tzw. **powój hawajski** uzyskiwany jest z nasion rośliny pochodzącej z południowej Azji. Najważniejszym psychoaktywnym składnikiem tego surowca jest ergina, zwana też LSA. Syntetycznym odpowiednikiem LSA jest LSD, jednakże działanie LSA jest ok. 10–15 razy słabsze, a efekty psychiczne po jego spożyciu mogą być bardziej przygnębiające i depresyjne niż po LSD. Działanie LSA może być bardzo zróżnicowane, jest to uwarunkowane indywidualnie. Często przytaczane jest występowanie przemyśleń i autorefleksji o niepokojącym i ponurym charakterze[28].

58 Zażycie powoju hawajskiego może spowodować:

- nadwrażliwość na światło,
- silne halucynacje słuchowe i wzrokowe,
- bezsenność,
- myśli samobójcze,
- nudności, wymioty i biegunki,
- swędzenie i mrowienie ciała,
- bóle brzucha.

[27] K. Warecki, *Dopalacze*, Polskie Wydawnictwo Encyklopedyczne, Radom 2010, s. 56.

[28] L. Jurek, *Dopalacze, narkotyki niewinny początek,* Wyd. Śląskie Centrum Wydawniczo-Handlowe „Lexdruk", Rybnik 2010, s. 27.

59 W oferowanym asortymencie sklepów z dopalaczami można było również zakupić specyfik o nazwie **CaleaZacatechichi**. Jest to gatunek rośliny z rodziny astrowatych występujący w Meksyku i Kostaryce zwany także „Dream Herb", „liście bogów" lub „gorzka trawa"[29]. Na polskim rynku pojawia się w mieszankach ziołowych i przyjmuje się ją najczęściej przez palenie lub picie w postaci wywaru. Użytkownicy Calei wskazują na działanie zbliżone do marihuany i lekkie działanie euforyzujące.

60 Specyfik wywołuje m.in.:

- osłabienie fizyczne,
- zawroty głowy,
- reakcje alergiczne,
- senność,
- mdłości i wymioty,
- wysypkę i podrażnienia skóry.

61 **Lion'sTail** znany również jako **Lions'sEar** i **Wild Dagga** jest rośliną z rodziny wargowatych. Rośnie w Afryce Południowej i Wschodniej. Alkaloidem zawartym w tej roślinie jest leonuryna. Lion'sTail w tradycyjnej medycynie użytkowany jest jako lek odrobaczający, zwalczający gorączkę, bóle głowy i kaszel[30]. Zwykle występuje w postaci suszu lub ekstraktu z liści/kwiatów, rzadziej w postaci świeżej. Jest jednym ze składników mieszanek ziołowych przeznaczonych do palenia. Działanie psychoaktywne Wild Daggi podobne jest do objawów wywołanych zażyciem słabszych odmian konopi indyjskich.

62 Objawami zażycia tej substancji są:

- zaburzenia percepcji i świadomości,
- wymioty i nudności,
- czasem napięcie mięśni.

63 **STERYDY**

Sterydy, zwane inaczej steroidami to organiczne związki chemiczne, z których wytwarza się leki o działaniu przeciwzapalnym. Samo pojęcie sterydy może być rozumiane w dwojaki sposób, w medycynie mianem sterydów przyjęło się określać leki, natomiast w środowisku kulturystów sterydy są grupą środków służących do sterowania anabolizmem organizmu. Kilkaset różnego rodzaju steroidów, pełniących rozmaite funkcje, występuje w organizmach roślin i zwierząt. Sterydy są związkami syntetycznymi o farmakologicznej i chemicznej budowie podobnej do testosteronu, który wpływa na funkcjonowanie i rozwój organów płciowych człowieka. Bardziej popularne są pod nazwą **sterydów anaboliczno-androgennych** (SAA), z powodu przyczyniania się zarówno do rozwoju muskulatury ciała, jak również do efektu maskulinizującego[31]. Pojęcie androgeniczny oznacza wywoływanie wtórnych cech płciowych męskich, takich jak męski typ owłosienia, pogrubienie strun głosowych i psychiczny typ zachowań. Pod pojęciem anaboliczny kryje się natomiast męska budowa ciała. Niektóre sterydy mogą być bardziej androgenne, inne bardziej anaboliczne. Preparaty anaboliczne, które mają małe działanie androgenne odnajdują zastosowanie w terapii u kobiet i dzieci. Zwiększenie masy mięśniowej, przyspieszenie wzrostu, gojenie kości oraz pobudzenie szpiku kostnego do produkcji krwinek czerwonych jest wynikiem działania ana-

[29] K. Warecki, *Dopalacze*, Polskie Wydawnictwo Encyklopedyczne, Radom 2010, s. 58.

[30] L. Jurek, *Dopalacze, narkotyki niewinny początek,* Wyd. Śląskie Centrum Wydawniczo-Handlowe „Lexdruk", Rybnik 2010, s. 29–30.

[31] J. Krzywiński, *Działania niepożądane środków dopingujących,,* w: W. Granowska (red.), *Doping zabija sport,* Towarzystwo Lekarskie Warszawskie, Warszawa 2007, s. 84.

bolicznego sterydów polegającego na wzmożeniu biosyntezy białek, co powoduje zatrzymanie azotu, potasu, chloru i wody[32].

64 W Polsce występuje szeroka gama sterydów dostępnych pod różnymi nazwami i postaciami. Występują zazwyczaj w postaci różnokolorowych pastylek oraz w postaci płynnej w zawiesinie olejowej, rzadziej wodnej. Sterydy używane pozamedycznie przyjmowane są najczęściej doustnie lub wstrzykiwane domięśniowo.

65 Jednym z najbardziej popularnych i chętnie kupowanym przez młodzież sterydem jest **metanabol** (dianabol, metka, mietek). Przyjmowanie metanabolu powoduje szybki przyrost masy mięśniowej. Jego działanie jest widoczne już pod 2–3 dniach kuracji. Najczęściej przyjmowany jest doustnie w tabletkach. Popularność tego środka wynika głównie z: ceny, szybkiego efektu działania, dostępności oraz braku informacji na temat jego skutków ubocznych. Skutkami jego stosowania są: uszkodzenie wątroby, trzustki i nerek; nadciśnienie, obrzęki, przeciążenie serca spowodowane szybkim przyrostem wagi, łysienie, zmiany zapalne skóry, ginekomastia[33], u młodych ludzi może nastąpić zahamowanie wzrostu, zaburzona zostaje spermogeneza oraz mogą występować zaburzenia libido.

66 Równie często kupowanym i zażywanym sterydem jest **omanadren 250**. W zależności od przyjętej dawki może spełniać różne funkcje. Pozamedyczne zastosowanie omanadrenu powoduje duże magazynowanie wody w organizmie, obrzęki w okolicach podudzi, podwyższony poziom agresji, trądzik posterydowy oraz zmiany zapalne skóry[34].

67 Jeden z najsilniej działających sterydów to **anapolon** (anadrol). Stosowanie anapolonu powoduje niezwykle szybki przyrost masy mięśniowej, w ciągu tygodnia zwiększa masę ciała aż o ok. 3 kg. Jego przedawkowanie może doprowadzić do śpiączki.

68 **Winstrol** (stanozolol) wpływa na uzyskanie suchej masy mięśniowej. Wśród młodzieży zażywającej ten środek powoduje przyrost siły, ale nie masy mięśniowej. Jednym z ważniejszych skutków ubocznych winstrolu jest wysuszanie stawów, przez co siłowe treningi mogą być bardzo bolesne dla młodego człowieka. Przyjmowany przez dłuższy czas, w ilościach znacząco przekraczających dawki lecznicze działa bardzo toksycznie, powodując silne uszkodzenie wątroby[35].

69 **Testosteron** jest sterydem kupowanym przez młodzież nie tylko poprzez Internet, ale często w miejscach ćwiczeń, na siłowniach. Najczęściej dostępny jest w formie zastrzyków na podłożu olejowym. Osoby przyjmujące tę substancję często nie wiedzą, że jej odstawienie powoduje szybką utratę masy mięśniowej. Najczęstsze skutki jego stosowania to: zatrzymywanie wody w organizmie, nadciśnienie tętnicze, obrzęki twarzy i łydek, ginekomastia, trądzik posterydowy, wzmożone magazynowanie tłuszczu w okolicach bioder, przerost pro-

[32] A. Nitka, J. Korczak, *Zjawisko nadużywania sterydów przez chłopców (implikacje zdrowotne, społeczne, moralne),* Informator metodyczny dla pedagogów i nauczycieli, Fundacja Pedagogium, Warszawa 2008, s. 13.

[33] Ginekomastia – powiększenie się sutka u mężczyzny, na skutek rozrostu tkanki gruczołowej, włóknistej i tłuszczowej.

[34] A. Adamczyk, *Młodość i sterydy – hormon „szczęścia" w strzykawce i tabletce nieszczęścia,* w: A. Adamczyk (red.), *Współczesne zagrożenia młodzieży szkolnej,* Oficyna Wydawnicza ASPRA-JR, Warszawa 2011, s. 169.

[35] Tamże, s. 160.

staty, zaburzenia elektrolitowe oraz zmiany zapalne w mieszkach włosowych[36].

70 **Deca-durabolin**, potocznie zwany jako deka, jest z chęcią stosowany przez początkujących sterydowców. Jest mało szkodliwy dla wątroby, pięknie buduje masę i rzeźbę mięśni, pomaga w regeneracji między treningami, łagodzi bóle mięśni, stawów i wiązadeł. Stosowaniu deki towarzyszą: krwotoki z nosa i ran, wysoka retencja wody, słabe krzepnięcie krwi, bóle głowy, wysokie ciśnienie tętnicze krwi, seksualna stymulacja, wstrzymanie procesu spermatogenezy oraz zmniejszenie produkcji testosteronu. U dziewcząt występują ponadto: szybki wzrost owłosienia, zwiększenie owłosienia łonowego i przerost łechtaczki oraz zanik cyklu miesiączkowego[37].

71 **Clenbuterol** jest stosowany w celu uzyskania „rzeźby" mięśni. Własności tej substancji sprzyjają spalaniu tkanki tłuszczowej. Skutkami zastosowania pozamedycznego clenbuterolu są: pobudzenie psychoruchowe, bóle głowy, bezsenność, drżenie rąk, kołatanie serca, pojawienie się bolesnych skurczów mięśni, nudności, podwyższona temperatura ciała[38].

72 Od kilku lat, głównie w Stanach Zjednoczonych oraz w Europie Zachodniej można zaobserwować stosowanie przez młodzież substancji o nazwie **synthol**. Środek ten bezpośrednio wstrzykiwany do mięśni powoduje ich szybki przyrost bez potrzeby ćwiczeń fizycznych. Nie jest to steryd anaboliczny w pełnym tego słowa znaczeniu. Jest mieszaniną trzech substancji: CT – oleju stosowanego w odżywkach oraz substancjach energetycznych, lidokainy – środka znieczulającego oraz alkoholu benzylowego. Środek ten jest niezwykle niebezpieczny, gdy dostanie się do krwi, może doprowadzić do zgonu[39].

73 **NAPOJE ENERGETYZUJĄCE**

Do substancji o działaniu dopingującym ludzki mózg możemy zaliczyć także środki popularne, takie jak: kawa, herbata, żeń-szeń, guarana, karnityna, **napoje energetyzujące.** Napoje „rozjaśniające mózg" typu kawa czy herbata, stosowane były od dawien dawana. W czasach współczesnych dużą popularnością, szczególnie w grupie młodzieży, cieszą się napoje energetyczne zwane także energy drinkami. Dostępne prawie w każdym sklepie, niebudzące najmniejszych podejrzeń, zawierają niewielkie dawki substancji uzależniających[40].

74 Po napoje energetyzujące sięga coraz więcej gimnazjalistów, uważając że w ten sposób dodadzą sobie energii do nauki. Młodzież pije napoje energetyzujące zwłaszcza przed sprawdzianami, podczas dyskoteki szkolnej oraz uprawiając sport. Puszkę tego napoju można kupić w sklepie bez żadnych problemów – sprzedawca nie zapyta o wiek i nie zażąda dowodu osobistego.

75 Napoje energetyzujące dostarczają tylko 23% dziennego zapotrzebowania na kalorie, dlatego nie są dobrym źródłem energii, ich zasadnicza funkcja to stymulowanie aktywności psychofizycznej, nie zaś dostarczanie energii.

76 Głównym biostymulatorem, który występuje we wszystkich napo-

[36] Tamże, s. 164.

[37] A. Nitka, J. Korczak, *Zjawisko nadużywania sterydów przez chłopców (implikacje zdrowotne, społeczne, moralne),* Informator metodyczny dla pedagogów i nauczycieli, Fundacja Pedagogium, Warszawa 2008, s. 27.

[38] Tamże, s. 20.

[39] Tamże, s. 30.

[40] J. Vetulani, *Mózg: fascynacje, problemy, tajemnice,* Wyd. Homini, Kraków 2010, s. 233.

jach energetyzujących jest kofeina, której działanie jest bardzo szerokie w szczególności: „pobudza układ nerwowy i stymuluje wydzielanie neuroprzekaźników dopaminy oraz serotoniny jak również hormonów – adrenaliny, wywołuje tzw. efekt czuwania, poprawia koncentrację oraz refleks, poprawia proces logicznego myślenia, wpływa na poprawę nastroju, utrudniania zasypianie, ułatwiania oddychanie poprzez rozkurcz mięśni w oskrzelach”[41].

77 Producenci napojów energetycznych reklamują je jako zastrzyk energii dla pracoholików, odświeżenie umysłu dla studentów, ratunek przed zaśnięciem dla kierowców. Ich zadaniem jest likwidacja stresu i zmęczenia, zwiększenie metabolizmu, pobudzenie i usprawnienie koncentracji. Energy drinki są dostępne w postaci płynnej, tabletek musujących oraz gum do żucia. Jedno opakowanie bardzo często zawiera dawkę substancji i minerałów przekraczających dzienne zapotrzebowanie człowieka.

78 Tymczasem lekarze alarmują: napojów energetycznych nie powinny pić osoby poniżej 13 roku życia. Konsekwencji sięgania młodego człowieka po napoje energetyzujące jest zbyt wiele, przedawkowanie oznacza ból głowy, wystąpienie nadpobudliwości, arytmię serca, niepokój oraz stany lękowe. Naukowcy uważają, iż młodzież, która w tym wieku zaczyna sięgać po napoje energetyzujące, nie dożyje 60 lat.

Przy nadmiernym spożywaniu napojów energetyzujących mogą pojawić się:

- uczucie zmęczenia,
- otępienie,
- mdłości,
- ból głowy,
- skoki ciśnienia,
- zwiększone napięcie mięśni,
- zaburzenia snu,
- arytmia serca[40].

79 PODSUMOWANIE

W minimalizowaniu skutków zażywania substancji psychoaktywnych, istotne jest znaczenie ich monitorowania. Monitoring tradycyjny obejmuje:

- rozmiary i charakter problemu narkotyków;
- zinstytucjonalizowanie reakcji społecznych (zasoby i działania – profilaktyka, leczenie, ograniczenie szkód, pomoc społeczna, ściganie i karanie);
- lokalny kontekst kulturowy, leczenie, ograniczenie szkód, pomoc społeczna, ściganie i karanie) społeczny i ekonomiczny, w jakim rozwija się problem i w jakim prowadzi działania[43].

W tym miejscu warto zwrócić uwagę, że działania te nie obejmują zagrożeń chemicznych w sieci i z jej inspiracji.

80 Osoby z problemem uzależnień szukające pomocy związanej z narkotykami i innymi substancjami mogą skorzystać z informatorów, w których podano konkretne placówki i zakres świadczeń[44].

[41] J. Gądek, *Napoje energetyczne na celowniku,* http://wiadomosci.onet.pl, data dostępu: 14.02.2013.

[42] Informacje zostały zaczerpnięte z programu telewizyjnego *Wiem co jem – napoje energetyczne,* sezon 4, odcinek 8.

[43] Monitorowanie narkotyków i narkomanii na poziomie lokalnym, Wyd. Krajowe Biuro Przeciwdziałania Narkomani, Warszawa 2007, s. 17–18.

[44] Narkomania. Informator na temat placówek udzielających pomocy osobom z problemem narkotykowym, Wyd. Krajowe Biuro Przeciwdziałania Narkomanii, Warszawa 2009.

BIBLIOGRAFIA:

Adamczyk A., *Młodość i sterydy – hormon „szczęścia" w strzykawce i tabletce nieszczęścia,* w: Adamczyk A. (red.), *Współczesne zagrożenia młodzieży szkolnej,* Oficyna Wydawnicza ASPRA-JR, Warszawa 2011.

Bukowska B., Kidawa M., Chojecki D., *Dopalacze,* „Remedium Profilaktyki i Promocja Zdrowego Stylu Życia", 5 (195)/2009.

Gądek J., *Napoje energetyczne na celowniku,* http://wiadomosci.onet.pl, (dostęp: 14.02.2013).

http://wyborcza.pl/10,82983,11440174, Heroina_w__Gazecie_Wyborczej_.html

Jędrzejko M. Kowalewska J., Janiszewski W., *Charakterystyka narkotyków*, w: Jędrzejko M. (red.), *Narkomania spojrzenie wielowymiarowe*, Wyd. Akademia Humanistyczna im. Aleksandra Gieysztora, Pułtusk–Warszawa 2009.

Jędrzejko M., *Współczesne teorie uzależnienia od substancji psychoaktywnych,* Oficyna Wydawnicza ASPRA-JR, Pułtusk – Warszawa 2009.

Jurek L., *Dopalacze, narkotyki niewinny początek,* Wyd. Śląskie Centrum Wydawniczo-Handlowe „Lexdruk", Rybnik 2010.

Jurek L., *Dopalacze, narkotyki niewinny początek,* Wyd. Śląskie Centrum Wydawniczo-Handlowe „Lexdruk", Rybnik 2010.

Jurek L., *Dopalacze, narkotyki niewinny początek,* Wyd. Śląskie Centrum Wydawniczo-Handlowe „Lexdruk", Rybnik 2010.

Knapik T.W., *Uzależnienia jako problem cywilizacyjny XXI wieku,* Wyd. Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie, Kraków 2010.

Knapik W., *Uzależnienia jako problem cywilizacyjny XXI wieku,* Wyd. Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie, Kraków 2010.

Korczak J., *„Kop" i „odlot" w wirtualnym świecie*, w: Andrzejewska A., Bednarek J. (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Wyd. Difin, Warszawa 2014.

Krzywiński J., *Działania niepożądane środków dopingujących,,* w: Granowska W. (red.), *Doping zabija sport,* Towarzystwo Lekarskie Warszawskie, Warszawa 2007.

Kuntz H., *Narkotyki i uzależnienia. Wszystko o czym należy wiedzieć*, Wydawnictwo Edukacyjne Parpamedia, Warszawa 2009.

Miszczak A., *Na czym polega profilaktyka uzależnień?,* http://nalogi.wieszjak.pl , data dostępu: 13.01.2013.

Monitorowanie narkotyków i narkomanii na poziomie lokalnym, Wyd. Krajowe Biuro Przeciwdziałania Narkomanii, Warszawa 2007.

Narkomania. Informator na temat placówek udzielających pomocy osobom z problemem narkotykowym, Wyd. Krajowe Biuro Przeciwdziałania Narkomanii, Warszawa 2009.

Narkotyki i ty, http://www.narkotyk.co, data dostępu: 14.02.2013.

Nitka A., Korczak J., *Zjawisko nadużywania sterydów przez chłopców (implikacje zdrowotne, społeczne, moralne),* Informator metodyczny dla pedagogów i nauczycieli, Fundacja Pedagogium, Warszawa 2008.

Nowak A., Wysocka E., *Problemy i zagrożenia społeczne we współczesnym świecie. Elementy patologii społecznej i krymi-*

nologii, Wydawnictwo Naukowe „Śląsk", Katowice 2001.

Uziałło J., *Biologiczne podstawy uzależnień,* Serwis Informacyjny Narkomania, 2(46)/2009.

Vetulani J., *Mózg: fascynacje, problemy, tajemnice,* Wyd. Homini, Kraków 2010.

Warecki K., *Dopalacze,* Polskie Wydawnictwo Encyklopedyczne, Radom 2010.

ZAGROŻENIA ZWIĄZANE Z UZALEŻNIENIAMI

UZALEŻNIENIE
OD GIER KOMPUTEROWYCH

Anna Andrzejewska
Józef Bednarek

OPIS ZJAWISKA

1 WPROWADZENIE

Definicja gier komputerowych

Trudno jest wyjaśnić pojęcie „gier komputerowych", chociaż mamy z nimi do czynienia od ponad dwudziestu lat. Poszukiwanie wyjaśnienia w słownikach i encyklopediach nie przyniesie zadowalających rezultatów.

Według poglądu J. Skrzypczaka, **gra komputerowa** to „program komputerowy, tj. zestaw poleceń zrozumiałych i wykonywanych przez procesor. Uzyskana w ten sposób elastyczność (…) pozwala na uruchamianie wielu różnorakich gier o charakterze rozrywkowym lub edukacyjnym na tym samym zestawie komputerowym"[1].

2 S. Łukasz podaje definicję gry komputerowej, utożsamiając ją z grą wideo. Zdaniem autora,

„gra wideo jest to zapisany w dowolnej postaci i na dowolnym nośniku cyfrowym (taśma, dyskietka, układy elektroniczne itp.) program komputerowy, spełniający funkcję ludyczną poprzez umożliwienie manipulacji generowanymi elektronicznie na ekranie wizyjnym (wyświetlaczu ciekłokrystalicznym, monitorze, telewizorze itp.), zgodnie z określonymi przez twórców gry, regułami. W odróżnieniu od np. programów graficznych, gry służą wyłącznie celom rozrywkowym, a zatem nie spełniają żadnej funkcji użytkowej, umożliwiającej jakąkolwiek pracę twórczą"[2].

3 Jednak **gier komputerowych nie należy utożsamiać z grami wideo**, ponieważ istnieje między nimi zasadnicza różnica. Gry wideo mają bardziej zręcznościowy charakter, a do grania w nie służą automaty i konsole, niemające poza tym innych zastosowań. Do grania w gry komputerowe jest potrzebny komputer, który wykorzystywany jest do wielu innych zadań.

4 Gra komputerowa to specyficzny typ programu komputerowego, którego naczelnym lub jednym z głównych celów jest rozrywka. Gra stawia przed graczem jakieś zadanie do zrealizowania i jednocześnie zawiera szereg przeszkód mających utrudnić jego wykonanie. Każda gra rządzi się swoimi regułami.

5 CECHY CHARAKTERYSTYCZNE GIER KOMPUTEROWYCH

Jako charakterystyczne cechy gry komputerowej wymienia się[3]:

- odrębność i ograniczoność w czasie i przestrzeni,
- podporządkowanie ograniczającym regułom,
- intensywność i energiczność,
- powtarzalność,
- bezinteresowność – ponieważ nie służy zaspokajaniu życiowych konieczności,
- dobrowolność – uczestnik ma swobodę podejmowania decyzji: czy chce grać, czy nie,
- charakter rywalizacyjny.

[1] J. Skrzypczak, *Aktualizacje encyklopedyczne*, Wyd. Kurpisz, Poznań 1998, s. 74–75.

[2] S. Łukasz, *Magia gier wirtualnych*, MIKOM, Warszawa 1998, s. 75.

[3] J. Chwaszcz, M. Pietruszka, D. Sikorski, *Media*, Wyd. KUL, Lublin 2005, s. 30.

6 Nowym zjawiskiem są gry, w których wykorzystuje się **technikę wirtualnej rzeczywistości**. Daje ona grającemu złudzenie uczestnictwa w środowisku gry, w sztucznej rzeczywistości. Występuje tu trójwymiarowy obraz, stereofoniczny dźwięk, a nawet różnego rodzaju wrażenia dotykowe. Urządzenia do realizacji takiej gry to hełm z małymi monitorami, słuchawkami oraz specjalna rękawica. Hełm i rękawica połączone są z komputerem, który wytwarza obrazy i przesyła je do monitorów umieszczonych w hełmie. Dźwięk słyszany przez słuchawki jest skojarzony z obrazami, a dzięki rękawicy można dotykać wirtualnych przedmiotów. Gracz nie ma świadomości znajdowania się poza monitorem komputera, ale doświadcza przeniesienia się i pozostawania w nowym otoczeniu. Może w nim spotkać wykreowane przez komputer postacie, oglądać komputerowo stworzone krajobrazy, uczestniczyć w wydarzeniach, nawet sam może przyjąć dowolną postać.

7 **Gry sieciowe** pełnią obecnie funkcję medium. Pozwalają uczestnikom na zabawę w dużej grupie. Jest wiele przyczyn komunikacji między graczami, jak np. umówienie się na grę, współpraca w grupie, która wymaga ustalenia działań, wymiana doświadczeń, poszukiwanie pomocy oraz rozmowy o samej grze. Gry masowe to przede wszystkim komunikacja. Twórcy gry nie mają możliwości kontrolowania jej przebiegu, to gracze mają wielką swobodę zachowań, często wbrew intencjom autorów.

W **masowych grach sieciowych**, jak i **e-sportach,** użytkownicy mają do dyspozycji trzy rodzaje interakcji.

Pierwszy rodzaj takiej interakcji zachodzi na poziomie użytkownik–gra, np. przydzielenie graczowi przez tzw. bot (automat) zadania, chociażby w postaci zdobycia pewnej rzeczy. Drugi rodzaj ma miejsce na poziomie awatar–awatar; występuje, gdy gracz nawiązuje kontakt z postaciami prowadzonymi przez innych graczy. Przykładem może być planowanie wraz z postaciami innych graczy ataku na ich wirtualnych przeciwników. Trzeci rodzaj to poziom użytkownik – użytkownik. Ma miejsce wówczas, gdy gracz komunikuje się z innymi graczami jako postać realna.

8 **RODZAJE GIER KOMPUTEROWYCH**

Według M. Filiciaka **gry sieciowe można podzielić ze względu na**:

1. „**integrację wieloosobowej gry sieciowej**:
   - opcjonalny tryb gry wieloosobowej,
   - gra tylko wieloosobowa,
2. **technologię**:
   - obsługiwanie przez przeglądarkę internetową,
   - peer-to-peer: zdecentralizowana sieć, każdy komputer może funkcjonować jako serwer,
   - centralny serwer sterujący połączeniami graczy,
3. **gatunki**:
   - akcja/zręcznościowe,
   - strategie,
   - przygodowe,
   - symulacje,
   - role-playing,
4. **przeznaczenie**:
   - wyimaginowane środowiska,
   - laboratoryjne środowiska,
   - rozrywkowe,
5. **model biznesowy/sposób dystrybucji**:
   - płatny program/gra wieloosobowa za darmo,
   - płatny program/miesięczny abonament,
   - bezpłatny program + abonament,
   - opłata za każdą grę,
   - opłata za dodatkowe epizody, funkcje”[4].

[4] Tamże, s. 74.

9 CHARAKTERYSTYKA GIER KOMPUTEROWYCH

Gdyby nie atrakcyjność, wyrażająca się także w oddziaływaniu na emocje, gry komputerowe nie byłyby tak popularne. Szczególnego znaczenia nabierają gry, które cechuje wyjątkowy ładunek przemocy i agresji. Należy się zastanowić: jak tego rodzaju gry wpływają na dzieci i młodzież, którzy nie mają w pełni rozwiniętego myślenia krytycznego? Co się wtedy dzieje z nimi?

10 Oprócz pozytywnych aspektów, o których była mowa wcześniej, gry komputerowe mogą wpływać w niekorzystny sposób na odbiorcę. W sprzedaży znajduje się wiele gier, które, niestety, zawierają bardzo dużo negatywnych treści. Niebezpieczeństwo gier polega również na tym, że ich uczestnicy wcielając się w role niekoniecznie pozytywnych bohaterów, utożsamiają się z nimi.

11 Niektóre gry komputerowe są szczególnie niebezpieczne, ponieważ pozwalają symulować i kreować rzeczywistość, bardzo często zawierając obrazy agresji i przemocy, które charakteryzują się ogromnym, wręcz niewyobrażalnym okrucieństwem i sadyzmem. Mimo że jest to przemoc symulowana, niemająca miejsca w świecie rzeczywistym, nie należy tego bagatelizować.

Symulowane obrazy przemocy, a właściwie samodzielne jej realizowanie w grach komputerowych, prowokuje dzieci do powtarzania okrutnych zachowań. Natychmiastowy efekt wyraża się w agresywnych myślach i wyobrażeniach o wrogich emocjach, natomiast długotrwały skutek jest związany z kształtowaniem agresywnych skryptów poznawczych i może prowadzić to do trwałych zmian w strukturze osobowości gracza.

12 Sposób przedstawiania przemocy w grach komputerowych powoduje, że użytkownik nabiera przekonania o powszechności agresji w świecie, akceptując ją jako element relacji międzyludzkich. Ważnym czynnikiem wpływającym na oswajanie się dzieci z przemocą jest to, że przemoc w grach nie jest karana, tylko nagradzana. Gry o charakterze agresywnym powodują znieczulenie na agresję wobec ludzi.

13 Można więc powiedzieć, że dzieci poświęcające dużo czasu na „agresywne" gry komputerowe cechują się większą agresywnością, natomiast ich wrażliwość moralna jest mniejsza. **Dzieci uzależnione od gier komputerowych często reagują wybuchami niekontrolowanej złości i agresji**. Rodzice powoli tracą kontakt z dzieckiem, a ono powoli zatraca kontakt z rzeczywistym światem. Najważniejsza staje się dla dziecka gra i czas spędzony przed monitorem komputera. **Silne uzależnienie od komputera i gier może prowadzić do obojętności, agresji, depresji, rozdrażnienia, bezsenności, a nawet prób samobójczych**.

14 Duże znaczenie w graniu ma trening, który prowadzi do wyuczenia i przyzwyczajenia się do wykonywania jakiejś czynności; oraz prowokacja sytuacyjna, która polega na samodzielnym rozwiązywaniu problemu i wymaga od dziecka odpowiedniego zachowania się w danym momencie, czyli aktywności.

15 Podczas aktywnego uczestnictwa w grze następuje „odwrażliwienie" i znieczulenie na przemoc. Jest to wynikiem wielokrotnego powtarzania ataków agresji. Zachowania agresywne, których doświadczają dzieci podczas gry, kojarzą się z nagrodą i przyjemnością. Stosowana przemoc w grach jest nagradzana. W konsekwencji negatywne zachowania mogą być przenoszone do realnego świata[5]. Współczesne dziecko przez wiele godzin przebywa w różnych

[5] A. Andrzejewska, *Uzależnienie od mediów cyfrowych,* w: T. Pilch (red.), *Encyklopedia pedagogiczna XXI* w., *t. 6*, Wyd. Akademickie „Żak", Warszawa 2007.

wymiarach sztucznej, medialnej rzeczywistości, właściwie na każdym kroku styka się z różnymi przejawami agresji, warto więc przypomnieć, że wielość obrazów przemocy uodparnia na ich emocjonalny odbiór, zobojętnia na nie i pozbawia altruizmu.

16 Bohater agresywnych gier komputerowych jest osobą centralną, agresorem, który kierowany przez grającego, stosuje przemoc w stosunku do innych. Walka i niszczenie to jego podstawowe zadania. Te reguły i zasady obowiązują w grze agresywnej. Nie stosując się do nich – „bohater" sam zginie.

17 Oprócz agresji w grach komputerowych premiowane są także inne zachowania negatywne. W wielu grach z udziałem samochodów wyścigowych ci zawodnicy wygrywają, którzy łamią wszelkie reguły uczciwej sportowej rywalizacji. Nasuwa się więc kontrowersyjne, ale coraz bardziej realne pytanie, czy wychowujemy prawego człowieka, czy profesjonalnego mordercę?

18 Nie można zapominać o tym, iż **w grach komputerowych bardzo często pojawiają się obrazy i animacje pornograficzne**. Są one dodatkiem do gry lub formą nagrody za przejście do następnego etapu. Bardzo niepokojącym aspektem jest także wykorzystywanie elementów o wyraźnie satanistycznym charakterze (np. *Doom, Hexen*). W ten sposób dzieci oswajają się z symboliką satanistyczną i z czasem odbierają ją jako element pozytywny, ponieważ konkretne symbole satanistyczne (np. pentagram, głowa kozła, odwrócony krzyż) często oznaczają miejsca, w których są np. tajne przejścia, schowki zawierające broń i inne „dobra" przeznaczone dla gracza. Z kolei wartości chrześcijańskie często są ośmieszane.

Główna postać może być przedstawiana w grze na dwa sposoby: z perspektywy zewnętrznej, widoczna jest wtedy jej twarz i cała sylwetka, a także charakterystyczny sposób poruszania się jej w przestrzeni. W nowych grach komputerowych postać wydaje się być bardzo realistyczna, np. porusza ustami, gdy mówi. Drugi sposób przedstawienia to widok z perspektywy pierwszej osoby (czyli tzw. widok z oczu gracza), zazwyczaj widać wtedy przedmioty, jakie trzyma – najczęściej jest to broń.

19 Gracz silniej utożsamia się ze swoim bohaterem, który jest osobą sprawną fizycznie, zazwyczaj o nadludzkiej sile i dużej wytrzymałości. Posiada przeróżne możliwości władania bronią i stosuje czary. Jego celem jest zgładzenie przeciwników za wszelką cenę. Jego działania są egocentryczne i utylitarne, pozbawione zasad moralnych. Pragnienie sprawowania władzy jest silniejsze od stosowania jakichkolwiek zasad. Zazwyczaj bohater z gier komputerowych jest skoncentrowany wyłącznie na sobie, na potrzeby innych zwraca uwagę tylko wtedy, gdy ma w tym jakiś cel. Zabiega głównie o swój interes, uważając, że słusznie działa. Nie ma tu miejsca na altruizm i współczucie, gdyż nie powoduje to postępu w grze. Dominuje tu prawo silniejszego i brak jest takich wartości, jak przyjaźń czy miłość. Punktem odniesienia oraz kryterium dobra i zła jest skuteczność w osiąganiu celów.

20 OBJAWY UZALEŻNIENIA OD GIER KOMPUTEROWYCH

ROZPOZNANIE OBJAWY

Uzależnienie od gier komputerowych rozwija się stopniowo i niezauważalnie, wypierając dotychczasowe zainteresowania i obowiązki – najpierw drugorzędne, potem podstawowe, stając się wreszcie jedynym sposobem na życie. **Pierwsze objawy najczęściej spostrzega najbliższa rodzina, choć początkowo mylnie interpretuje je,**

jako pozytywne zainteresowanie informatyką. Utrwalaniu uzależnienia sprzyja brak dezaprobaty społecznej i znikoma świadomość niebezpieczeństwa. Rozwija się ono niewidocznie i osoby, które zgłaszają się po pomoc, często są już w później fazie tego procesu. Dysfunkcja zachowań jest tu odwrotnie proporcjonalna do wieku. **Im młodsze osoby, tym bardziej zagrożone są uzależnieniem.** „Uzależnienie od komputerów i kreowanych przez nie sztucznych rzeczywistości to takie samo uzależnienie, jak wszystkie pozostałe. To ciężka choroba emocji. Ludzie uciekają w świat iluzji. Sami tworzą lepszą rzeczywistość. Tu nikt nie zagraża ich uczuciom, nie może odrzucić. Potem nie potrafią już normalnie egzystować. **Pojawiają się coraz większe kłopoty w kontaktach społecznych. Spanie, jedzenie stają się uciążliwą koniecznością. Sens życia ogranicza się do czasu spędzonego przed komputerem** (…)”[6].

„Komputer odbiera osobom uzależnionym poczucie wolności, prywatności, a także uniemożliwia im krytyczne ustosunkowanie się do otaczającego świata. Komputer staje się czymś w rodzaju »superczłowieka«, a użytkownik - podatny na manipulację - nie potrafi odnieść się do przekazywanych mu informacji”[7].

21 Pojęcie **„uzależnienia”** odnosi się do wielu aspektów jednostki i jest zjawiskiem bardzo złożonym. Nie daje się w pełni zdefiniować[8]. Uzależnienie dotyka człowieka na wielu poziomach: na poziomie behawioralnym ujawnia się poprzez poszukiwanie pewnych substancji czy powtarzanie określonych zachowań. Jednocześnie uzależniony jest tak pochłonięty przedmiotem uzależnienia, że nie może się bez niego obejść i zaniedbuje inne sprawy, od relacji uczuciowych - po sprawy zawodowe[9]. Jest to (…) proces rozpoczynający się w chwili, kiedy osoba dzięki kontaktowi z pewnym wyjątkowym przedmiotem odbiera siebie w sposób inny niż dotychczas i postrzega zmianę wizerunku samej siebie jako coś pozytywnego lub lepiej odpowiadającego swoim potrzebom”[10]. Skutki uzależnienia mają wpływ na życie jednostki i są przyczyną jej problemów.

22 Charakterystyczne cechy uzależnienia od gier komputerowych to[11]:

- dziecko spędza przed monitorem cały wolny czas, tracąc poczucie czasu,
- jest niespokojne,
- nie potrafi znaleźć sobie innego zajęcia,
- ma trudności w nawiązywaniu kontaktów,
- nie spotyka się z rówieśnikami,
- nie podejmuje żadnych innych form aktywności.

Ponadto należy zwrócić uwagę na:

- zaniedbywanie nauki,
- stawanie się agresywnym w stosunku do otoczenia,
- miewanie fantazji i marzeń sennych związanych z komputerem,
- pojawiające się objawy abstynencyjne – zaprzestanie grania powoduje złe samopoczucie, rozdrażnienie, a nawet niekontrolowaną agresję.

[6] K. Kowalewska, *Komputerowi mordercy,* „Kultura i Życie”, 7.11.1996, s. 13.

[7] S. Łukasz, *Magia gier wirtualnych*, MIKOM, Warszawa 1998.

[8] Więcej nt. problemów definicyjnych uzależnień w artykule Infoholizm

[9] C. Guerreschi, (tłum.) A. Wieczorek-Niedzielska, *Nowe uzależnienia*, Wydawnictwo SALWATOR, Kraków 2006, s. 19.

[10] Tamże, s. 19.

[11] J. Bednarek, *Zagrożenia w cyberprzestrzeni*, w: M. Jędrzejko (red.), *Patologie społeczne*, Wyższa Szkoła Humanistyczna w Pułtusku, Pułtusk 2006, s. 133.

23 Uzależnienie objawia się podobnie w wypadku wszystkich mediów. Jeżeli trudno się obyć bez danego sprzętu, a czynności dnia codziennego są zaburzone przez podporządkowanie ich jakiemuś medium, można przypuszczać, że jest się na drodze do uzależnienia.

24 Do objawów uzależnienia należy zaliczyć[12]:

1. potrzebę korzystania z danego medium w coraz większym wymiarze czasowym,
2. występowanie złego samopoczucia, drażliwości, pobudzenia psychoruchowego, lęku, depresji przy zerwaniu kontaktu z danym sprzętem (włącznie z zaistnieniem zespołu abstynenckiego),
3. nieudane próby zaprzestania, okłamywanie rodziców, którym dziecko nie mówi o rzeczywistym czasie poświęcanym na użytkowanie danego medium.
4. doznawanie satysfakcji i poczucia własnej wartości poprzez udział w grach i sesjach internetowych,
5. ograniczenie innych zajęć, ucieczka od problemów życia realnego.
6. pochłonięcie myśli i wyobraźni przez prezentowane treści w mediach,
7. zaniedbywanie nauki, pracy, rezygnacja ze spotkań rówieśniczych, odkładanie w czasie innych ważnych spraw na rzecz korzystania z wybranego medium,
8. pojawienie się konfliktów rodzinnych w związku z korzystaniem z danego medium,
9. przeznaczanie coraz większej ilości pieniędzy np. na zakup sprzętu komputerowego, oprogramowania, akcesoriów czy książek i czasopism o tematyce komputerowej.

25 Nieracjonalne **korzystanie z komputera może prowadzić do problemów z zasypianiem, wzrostu lęku i sennych koszmarów**. Komputer nie wymaga żadnej aktywności fizycznej, nawet wychodzenia z domu. Jest bardzo łatwym, lecz biernym sposobem spędzenia wolnego czasu. W dużym stopniu **sprzyja lenistwu umysłowemu oraz obniżeniu sprawności myślenia abstrakcyjnego**. Zmniejsza się czas przeznaczany na sen, spotkania towarzyskie, zabawy z rówieśnikami, słuchanie radia, czytanie książek i czasopism, ruch na świeżym powietrzu czy zajęcia domowe. Jednocześnie następuje **ograniczenie czasu przeznaczonego na kontakty między rodzicami a dziećmi, a przede wszystkim na rozmowy**.

„Zdarzają się już kilkunastoletni pacjenci z całym zespołem objawów uzależnienia od komputera. Przypominają one zaburzenia nerwicowe – niepokoje, lęki, zaburzenia snu, a w sferze fizjologicznej – nadmierne pocenie się, naprzemienne uczucie gorąca i zimna, moczenie się. Takie dzieci czują się źle, kiedy nie mają przed sobą włączonego monitora”[12].

26 Dla osoby uzależnionej gry komputerowe stają się czymś najważniejszym, nawet potrzeby fizjologiczne stają się uciążliwe. Gra komputerowa daje poczucie bezpieczeństwa, przegrana niczym nie grozi, można próbować jeszcze raz, stosując inną taktykę. Kiedy uzależniony nie ma dostępu do komputera, nie porzuca swych myśli związanych z grą, szuka nowych rozwiązań, jak przejść np. na kolejny etap gry bądź stosuje alternatywne rozwiązania grając w gry w telefonach komórkowych. Uzależnieni kolekcjonują materiały związane z grami. Bogatą ofertę można znaleźć w popularnych czasopismach komputerowych, takich jak np.:

[12] Por. A. Andrzejewska, *Dziecko w cyberprzestrzeni*, Wyd. Pedagogium, Warszawa 2007, s. 44.

[13] A. Kłodecki, *Przyjaźń z komputerem – korzyść czy zagrożenie,* „Twoje Dziecko”, 6/2000, s. 64.

„CD Action", „PC Word" „Komputer", „PC Format" czy „Komputer Świat". Dostarczają one informacji o najlepszych i najpopularniejszych grach. Do czasopism takich dołączane są płyty z bogatą ofertą różnych gier. Osoby zafascynowane grami komputerowymi dyskutują na ich temat w szkole, na czacie, forach itp., spotykają się z innymi graczami, aby omówić strategię dojścia do celu, grają wirtualnie z innymi graczami, tworzą własne strony internetowe.

Skutków niekontrolowanego grania jest bardzo wiele. Najważniejszym jest wyzwalanie agresji i przemocy wśród dzieci i młodzieży. Dziecko poprzez obserwację brutalnych scen uczy się negatywnych zachowań, wydaje mu się, że można mieć dwa bądź trzy życia, dzieli świat na sprzymierzeńców i wrogów. Oprócz negatywnego wpływu gier komputerowych na psychikę dziecka, istnieją też zagrożenia związane ze zdrowiem, jak choroby oczu czy obciążenie układu mięśniowo-szkieletowego, co powoduje wady postawy i ogólne osłabienie organizmu. Dlatego bardzo ważne jest prawidłowe korzystanie z komputera: odpowiedni ekran i oświetlenie, wygodne miejsce pracy, zmienianie pozycji ciała, robienie przerw oraz wietrzenie pomieszczenia.

27 Coraz częściej w literaturze przedmiotu zwraca się uwagę na możliwość uzależnienia od gier komputerowych, porównując je do „elektronicznego LSD". Istnieją bowiem pewne podobieństwa między kompulsywnym graniem a zaburzeniami z grupy uzależnień psychoaktywnych. Równocześnie towarzyszą temu specyficzne objawy psychiczne i fizyczne pojawiające się po zaprzestaniu uzależniającej aktywności – np. rozdrażnienie, trudności z koncentracją uwagi, drżenia w sytuacji braku dostępu do gry. **Osoby uzależnione od gier komputerowych nie potrafią więc normalnie egzystować – gra staje się czymś najważniejszym w życiu, natomiast w kontaktach z rodzicami i rówieśnikami pojawiają się trudności.** Nawet naturalne potrzeby fizjologiczne, jak spanie, jedzenie, wydalanie, stają się uciążliwymi, choć koniecznymi przerwami podczas gry.

28 PRZYCZYNY UZALEŻNIENIA OD GIER KOMPUTEROWYCH

Komputer, ale przede wszystkim gry komputerowe mogą stanowić źródło uzależnienia.

29 Gry komputerowe stanowią niewątpliwie atrakcyjną rozrywkę, która nie nudzi, lecz przeciwnie – coraz bardziej wciąga i angażuje. Gry mają bardzo interesującą grafikę, tworzącą plastyczny trójwymiarowy obraz, nieodróżniający się jakością od filmu wideo. Atrakcyjność gier komputerowych polega na tym, że gracz może uczestniczyć w najbardziej wymyślnych przygodach, które ogranicza jedynie wyobraźnia programistów. Większość gier jest konstruowana na podstawie scenariuszy pełnych przemocy, w których jest wszystko to, co złe, a silna kumulacja agresji, przemocy i niemoralności prowadzi do pozbawienia ich wszelkich wartości. Spreparowana rzeczywistość w grach prowadzi młodego człowieka w świat nierzeczywisty, w którym liczą się najgorsze instynkty, a świat wartości zredukowany zostaje do minimum.

30 Uczestniczenie w grze stało się bardzo popularnym sposobem spędzania wolnego czasu przez dzieci i młodzież. Niektóre dzieci przyzwyczaiły się do takiego właśnie sposobu odpoczynku i niczym innym się nie interesują. Może to prowadzić do uzależnień podobnych do tych od substancji psychoaktywnych.

Korzystanie z gier komputerowych przez dzieci najczęściej nie jest przez nikogo kontrolowane, gdyż dorośli nie potrafią się nimi posługiwać i często nie wiedzą nawet, na czym te gry polegają.

31 Rodzice zwykle najpierw wyrażają swój zachwyt i dumę z faktu, że dziecko już w tak młodym wieku sprawnie posługuje się komputerem. Potem zaczynają się niepokoić, że coraz więcej czasu poświęca ono na gry komputerowe: spędza przed komputerem wiele godzin, a nawet całe dnie i noce, równocześnie zaniedbując swoje obowiązki, opuszczając się w nauce i stopniowo staje się zupełnie innym człowiekiem niż dotychczas.

32 **POSTRZEGANIE KOMPUTERA PRZEZ GRACZA**

Komputer może być przez użytkownika traktowany jako swego rodzaju partner do gry, „elektroniczny przyjaciel", który z perspektywy gracza ma następujące cechy[14]:

- „jest zawsze gotowy do podjęcia zabawy, nie męczy się nigdy i nie odmawia,
- pozwala wielokrotnie powracać do tych samych miejsc, scenariuszy lub akcji,
- konsekwentnie ocenia błędy, ale równocześnie nie karze za nie – okazywaniem złości i rozczarowania,
- daje poczucie władzy graczowi, który sam decyduje o rozpoczęciu czy zakończeniu gry,
- stanowi ucieczkowy „idealny" świat dla gracza, w którym ma on możliwość realizacji swoich marzeń i pragnień,
- interpretacja przegranej lub wygranej z komputerem może być zawsze pozytywna (przegrałem, ale tylko z maszyną; lub wygrałem aż z maszyną, która nie popełnia błędów),
- daje okazję do aktywności własnej w przeciwieństwie do biernego towarzyszenia akcji przy czytaniu książki czy oglądaniu filmu,
- emocje towarzyszące grze mogą być kontrolowane i stopniowane (poziomy trudności), a ryzyko przeżywane jest w „bezpieczny" sposób,
- płeć nie ma znaczenia, bo sam gracz decyduje, jaką rolę wybiera dla siebie – kobiecą czy męską,
- zapewnia możliwość rozładowania emocji w aktywny sposób bez ponoszenia znaczących konsekwencji swoich czynów,
- umożliwia zaspokajanie różnych popędów i potrzeb (np. agresji, potrzeby więzi, popędu seksualnego) z dowolnie wykreowanym partnerem na ekranie".

33 W ostatnim czasie coraz więcej dzieci jest pacjentami poradni psychologicznych, z rozpoznaniem uzależnienia od komputera. Przede wszystkim to rodzice dzieci uzależnionych od gier komputerowych szukają pomocy u specjalistów tego typu. Uzależnienie zaczyna się zazwyczaj bardzo niewinnie. Najpierw jest ciekawość i zafascynowanie, dziecko spędza wiele czasu przy grach komputerowych. Rodzice z satysfakcją przyglądają się swojemu kilku- czy kilkunastoletniemu dziecku, które sprawnie obsługuje komputer. Przyzwalają na to, aby dziecko spędzało coraz więcej czasu przed komputerem, gdyż są przekonani, że rozwija ono swoje zainteresowania, a równocześnie jest w domu pod ich czujnym okiem. Jednak z czasem, przy próbie oderwania od komputera, syn lub córka reagują wybuchami niekontrolowanej złości i agresji. Rodzice powoli tracą kontakt z dzieckiem, a ono samo zatraca kontakt z rzeczywistością, ponieważ najważniejsza staje się gra i czas spędzany w świecie wirtualnym. Zaniepokojeni opiekunowie szukają pomocy u psychologa, często dopiero wówczas, gdy dzieci są już uzależnione od grania, czego konsekwencją są zaburzenia psychosomatyczne, opuszczanie zajęć szkolnych, zaniedbywanie higieny i racjonalnego odżywiania. Kiedy zostają odizolowane od komputera, pojawia się u nich agresja, rozdrażnienie, bezsenność, reakcje fizjologiczne, depresja, a nawet próby samobójcze.

[14] D. Sikorski, *Uzależnienie od gier komputerowych*, www.sop.sds.pl, data dostępu 10.02.2008.

DOBRE PRAKTYKI

34 DOBRE PRAKTYKI – SYSTEM KLASYFIKACJI PEGI

Definicja

PEGI to tzw. **system ratingu wiekowego** opracowany w celu „udzielenia rodzicom pomocy w podejmowaniu świadomych decyzji o zakupie gier komputerowych”[15].

35 Twórcą i właścicielem Ogólnoeuropejskiego Systemu Klasyfikacji Gier jest Europejska Federacja Oprogramowania Interaktywnego (ISFE) z siedzibą w Belgii. We wrześniu 2009 roku system ten uznany został przez pełnomocnika rządu ds. równego traktowania za oficjalny system ratingu wiekowego obowiązujący w Polsce. System PEGI stosowany jest oficjalnie w trzydziestu krajach europejskich. Wspierają go najwięksi producenci konsol do gry – Microsoft, Nintendo, Sony oraz twórcy interaktywnych gier, a także ich wydawcy w całej Europie.

Na system PEGI składają się dwie części – pierwsza dotyczy klasyfikacji wiekowej, druga zaś – opisu treści. Znaki ratingu wskazujące kategorie wiekowe (3, 7, 12, 16, 18 lat) umieszczone są z przodu i z tyłu opakowania zawierającego grę. Znaki te dostarczają rzetelnych informacji o przeznaczeniu danej gry, ale nie uwzględniają niezbędnych umiejętności gracza oraz poziomu jej trudności.

36 Poniżej zestawiono **opisy poszczególnych kategorii wiekowych** według Ogólnoeuropejskiego Systemu Klasyfikacji Gier:

Treść gry odpowiednia dla graczy spośród wszystkich grup wiekowych. Dopuszczalna jest niewielka dawka przemocy, ale w komicznym kontekście. Postacie pojawiające się na ekranie nie powinny być utożsamiane przez dziecko z postaciami rzeczywistymi. W całości natomiast powinny być wytworem jego fantazji.
Gra nie może zawierać obrazów oraz dźwięków, które mogłyby przerazić lub przestraszyć dziecko. Gra oznaczona tym znakiem nie powinna zawierać wulgarnych słów, scen prezentujących nagość czy jakiegokolwiek odwołania do życia seksualnego.

Znakiem tym oznaczone są te gry, które nie zostały zakwalifikowane do grupy PEGI 3, ze względu na występujące w nich sceny lub dźwięki potencjalnie przerażające najmłodszych graczy. Nie są zaś przerażające dla graczy powyżej 7 roku życia. W grach tych dopuszczalne są sceny zawierające częściową nagość, ale nigdy w kontekście seksualnym.

Ten znak widnieje na opakowaniach gier zawierających przemoc o bardziej realistycznym charakterze, „skierowaną przeciwko postaciom fantastycznym i/lub nierealistyczną przemoc wobec postaci ludzkich lub rozpoznawalnych zwierząt”[16].

Gry oznaczone tym znakiem zawierają aktywność seksualną lub przemoc wyglądające realistycznie. Dopuszczalne są sceny zawierające bardziej brutalne wulgaryzmy, pokazujące popełnianie przestępstw oraz stosowanie używek takich jak tytoń czy narkotyki.

15 R. Błaszkiewicz, *Gry komputerowe a zdrowie dziecka w młodszym wieku szkolnym*, „Nauczanie Początkowe”, 1/2010–2011, s. 41.

16 Tamże, s. 41–42.

Ten znak ratingu wiekowego mówi o tym, że gra przeznaczona jest wyłącznie dla dorosłych odbiorców. Gry tego typu przedstawiają sceny przemocy, których widok wywołuje u gracza uczucie odrazy. Ponadto obfitują w sceny ukazujące specyficzne i brutalne rodzaje przemocy.

37 Charakterystyczne dla Ogólnoeuropejskiego Systemu Klasyfikacji Gier PEGI są również **piktogramy** umieszczone z tyłu opakowania zawierającego grę komputerową. **Wskazują one potencjalnie niebezpieczne treści**, które występują w danej grze.

38 Poniżej zamieszczono wspomniane piktogramy oraz krótkie opisy zagrożeń, jakich dotyczą.

Strach – gra może przestraszyć młodsze dzieci.

Przemoc – gra zawierająca elementy przemocy.

Seks – nagość i/lub zachowania seksualne, nawiązania do zachowań o charakterze seksualnym.

Wulgarny język

Narkotyki – nawiązania do narkotyków lub ukazane ich zażywanie.

Dyskryminacja – gra pokazuje przypadki dyskryminacji lub zachęca do niej.

Hazard – gra zachęca do uprawiania hazardu lub wręcz go uczy.

Online – gracz może grać online.

39 Na wielu portalach czy serwisach internetowych udostępniane są użytkownikom gry komputerowe o niewielkich rozmiarach. Tego typu segment rozwija się bardzo szybko i dynamicznie, dlatego w celu jego obsługi stworzono oznaczenie **„PEGI OK”**:

40 Jeśli znak ten widnieje przy danej grze w witrynie lub na portalu internetowym, oznacza to, że mogą grać w nią wszyscy użytkownicy – bez względu na wiek. **„PEGI OK”** oznacza dosłownie – **gra bezpieczna dla wszystkich**.

Gry oznaczone taką ikoną nie mogą zawierać:

- przemocy,
- nagości,
- czynności seksualnych (lub aluzji o charakterze seksualnym),
- wulgaryzmów,
- hazardu (lub jego elementów),
- popularyzacji i/lub zażywania narkotyków,

ĆWICZENIA 18

popularyzacji alkoholu i/lub tytoniu,

przerażających scen[16].

42 **PODSUMOWANIE**

Ogólnoeuropejski System Klasyfikacji Gier PEGI i stosowane w nim oznaczenia w postaci ikonek oraz piktogramów są pewnego rodzaju pomocą i wskazówką dla rodziców dzieci korzystających z gier komputerowych. **Rodzice, wybierając grę, powinni zwracać uwagę nie tylko na jej treść czy charakter. Przede wszystkim powinni mieć na uwadze wiek dziecka, jego rozwój psychiczny oraz możliwości percepcyjne.** Ich rola polega na sprawowaniu kontroli nad tym, w jaki sposób ich dziecko korzysta z gier. Pomocą zatem jest dla nich PEGI, który za pomocą niewielkich ikonek informuje, dla kogo i o czym są gry.

43 Także „instytucje oświatowe powinny być zainteresowane promowaniem szczególnie wartościowych tytułów dostosowanych do odpowiedniego wieku ucznia oraz upowszechnianiem wiedzy na temat ratingu gier i zasad obowiązującego w Europie systemu PEGI”[18].

[17] Por. R. Błaszkiewicz, *Gry komputerowe a zdrowie dziecka w młodszym wieku szkolnym*, „Nauczanie Początkowe”, 1/2010/2011, s. 42.

[18] Z. J. Szeja, *Gry i młodzi gracze. Czy granie w gry komputerowe jest niebezpieczne?*, „Meritum”, 2/2010, s. 10.

BIBLIOGRAFIA:

Andrzejewska A., *Dziecko w cyberprzestrzeni*, Wyd. Pedagogium, Warszawa 2007.

Andrzejewska A., *Uzależnienie od mediów cyfrowych*, w: Pilch T. (red.), *Encyklopedia pedagogiczna XXI w*., *t. 6*, Wyd. Akademickie „Żak”, Warszawa 2007.

Bednarek J., *Zagrożenia w cyberprzestrzeni*, w: Jędrzejko M. (red.), *Patologie społeczne*, Wyższa Szkoła Humanistyczna w Pułtusku, Pułtusk 2006.

Błaszkiewicz R., *Gry komputerowe a zdrowie dziecka w młodszym wieku szkolnym*, „Nauczanie Początkowe”, 1/, 2010/2011.

Chwaszcz J., Pietruszka M., Sikorski D., *Media*, Wyd. KUL, Lublin 2005.

Guerreschi C., *Nowe uzależnienia*, Wyd. Salwator, Kraków 2006.

Kłodecki A., *Przyjaźń z komputerem – korzyść czy zagrożenie,* „Twoje Dziecko”, 06/2000.

Kowalewska K., *Komputerowi mordercy,* „Kultura i Życie”, 7.11.1996.

Łukasz S., *Magia gier wirtualnych*, MIKOM, Warszawa 1998.

Sikorski D., *Uzależnienie od gier komputerowych*, www.sop.sds.pl data dostępu: 10.02.2013).

Skrzypczak J., *Aktualizacje encyklopedyczne*, Wyd. Kurpisz, Poznań 1998.

Szeja Z. J., *Gry i młodzi gracze. Czy granie w gry komputerowe jest niebezpieczne?*, „Meritum”, 2/2010.

INFOHOLIZM

Anna Andrzejewska
Józef Bednarek

OPIS ZJAWISKA

1 WPROWADZENIE

W obecnych czasach rodzi się na naszych oczach nowa generacja uzależnień. „Specjaliści odnotowują lawinowy przyrost niejednoznacznych zaburzeń i dysfunkcji nowej generacji, powodujących niekiedy przejściowe lub trwałe – psychologiczne lub somatyczne inwalidztwo, pojedyncze symptomy, czy syndromy, z którymi nawet specjalistyczny medyczny personel nie daje sobie rady”[1].

2 SKALA I ZASIĘG ZJAWISKA

Zjawisko uzależnienia od mediów cyfrowych pojawiło się w latach 90. XX w. Rozprzestrzenia się ono bardzo dynamicznie, powodując coraz większe zagrożenie nie tylko dla samej jednostki, ale również dla całego społeczeństwa. Staje się w coraz większym stopniu porównywalne z uzależnieniem od używek, takim jak alkoholizm czy narkomania, z tym że bardziej dotkliwe, gdyż obok zmian psychosomatycznych postępuje alienacja jednostki. Mechanizm uzależnienia od mediów, w tym także od komputera i Internetu jest podobny do innych uzależnień. Najpierw jest zainteresowanie i chęć spróbowania czegoś nowego, później stopniowo kontakt z mediami zastępuje inne aktywności, prowadząc do utraty łączności ze światem rzeczywistym. Zaburza się widzenie świata, trudno ocenić, co jest rzeczywiste, a co nie, granica ta zostaje rozmyta. Człowiek daje się wciągnąć do świata wirtualnego, który bardziej go cieszy i satysfakcjonuje niż realny. Tam też odczuwa to, co powinien odczuwać wśród ludzi.

3

W tym miejscu należy zasygnalizować różnicę pomiędzy nadmiernym korzystaniem z komputera i Internetu a uzależnieniem.

Zjawisko nadmiernego i niekontrolowanego korzystania z Internetu jest nazywane w różny sposób. W literaturze przedmiotu i języku potocznym używa się takich określeń, jak: siecioholizm, sieciozależność, cyberzależność, cybernałóg, internetoholizm, netoholizm, zespół uzależnienia od Internetu (ang. *internet addiction syndrome*), uzależnienie internetowe (ang. internet addiction), patologiczne korzystanie z Internetu (ang. *pathological internet use*)[2].

4

Nadmierne korzystanie z komputera i Internetu, a więc nadużywanie mediów interaktywnych, wyraża się w korzystaniu z nich za wszelką cenę, bez kontrolowania czasu. Jest to taki stan, w którym użytkowanie tych mediów może przerodzić się w przymus, a więc w uzależnienie.

5 DEFINICJA

Termin uzależnienie stosowany jest do określenia różnych zaburzeń. Trudno jest mówić o powszechni uznanej naukowej definicji tego terminu. Najczęściej stosuje się to pojęcie w kontekście używania środków psychoaktywnych, zmieniających nastrój oraz zachowanie. Do grupy tych środków należą narkotyki, alkohol, leki oraz inne używki.

W dużym uproszczeniu możemy mówić o uzależnieniu wtedy, gdy występuje nabyta silna potrzeba wykonywania jakiejś czynności lub zażywania jakiejś substan-

[1] L. Szawdyn, *Co to znaczy być uzależnionym od Internetu*, „Magazyn Internetowy WWW”, 2/1999.

[2] K. S. Young, *Caught In The Net*, J. Wiley & Sons, New York 1998; K. S. Young, *Internet Addiction: Symptoms, Evaluation and Treatment*, w: I. Van de Crek, X. Jackson, *Innovations in Clinical a Source Book*, Sarasota FL. Professional Resource Press, 1999; A. *Jakubik, Zespół uzależnienia od Internetu (ZUI) – Internet Addiction Syndrome (IAS)*, http:/// www.psychologia.net.pl; P. Wallace, *Psychologia Internetu*, Dom Wydawniczy REBIS, Poznań 2001; P. Afftab, *Internet a dzieci. Uzależnienia i inne niebezpieczeństwa*, Wyd. Prószyński i S-ka, Warszawa 2003.

cji. Obecnie pojęcie uzależnienia traktuje się dosyć szeroko i zakłada się, iż zawiera ono również *(...) inne wypadki, kiedy ludzie czują się zmuszeni angażować się w ryzykowne, „wymykające się spod kontroli" zachowania (...)*[3].

6 DEFINICJE UZALEŻNIENIA

Dokonując analizy literatury przedmiotu, można spotkać różne definicje uzależnienia.

Według *Encyklopedii zdrowia* uzależnienie to stan psychicznej i fizycznej zależności od jakiegoś środka. Zależność psychiczna przejawia się w przemożnej potrzebie doznawania skutków działania wybranej substancji np. uspokojenia, poprawy samopoczucia, pobudzenia, z czym na ogół wiąże się dążenie do zwiększania dawki i zdobywania, mimo rosnących kosztów materialnych i moralnych"[4].

7 A. Piotrowski definiuje stan uzależnienia w następujący sposób, jest to „stan psychiczny i fizyczny, wynikający z interakcji pomiędzy organizmem a środowiskiem, objawiający się kompulsywnym (przymusowym) przyjmowaniem środka stale lub okresowo, by przeżyć to działanie lub uniknąć złego samopoczucia wynikającego z abstynencji".[5]

8 Z. Zaborowski ujmuje uzależnienie w następujący sposób. Jest to „(…) proces, bądź jego efekt związany z wytwarzaniem się specyficznego związku między jednostką a jej czynnościami, zachowaniem, bądź między jednostką a innymi ludźmi, który charakteryzuje się ograniczeniem pola świadomości, pola decyzyjnego i wyborem często jednej tylko i to w sposób kompulsywny, alternatywy".[6]

9 Według G. Zimbardo nałóg (addiction) formalnie oznacza uzależnienie fizyczne ale też i psychiczne „(…) które jest na tyle poważne, że dane zachowanie stało się przymusowe i jednostka nie ma nad nim wystarczającej dowolnej kontroli".[7] Jest to natrętna potrzeba ciągłego i coraz częstszego przyjmowania substancji lub niepohamowany pociąg do powtarzania czynności, która wywołuje uczucie przyjemności, a tym samym redukuje doznania negatywne. Istotą nałogu jest to, że powstrzymanie się od przyjmowania pewnej substancji czy wykonywania określonej czynności staje się problemem. Podążając dalej za autorem dowiadujemy się, że (…) „uzależnienie (*dependence)* to proces, w którym organizm czy umysł przystosowują się do przyjmowania pewnej substancji i stają się od niej zależne".[8] Autor zwraca uwagę na fakt, że uzależnienie może być rozpatrywane zarówno na poziomie fizjologicznego funkcjonowania organizmu, jak również na płaszczyźnie psychicznej. Uzależnienie fizjologiczne to proces, w którym organizm adaptuje się do danego środka i uzależnia od niego, po części w skutek niedoboru neuroprzekaźników, spowodowanego częstą obecnością tego środka.[9] Uzależnienie psychiczne występuje wtedy, gdy dana osoba uważa zażycie jakiegoś środka za tak pożądane czy przyjemne, że rozwija

[3] P. G. Zimbardo, *Psychologia i życie*, Wyd. Naukowe PWN, Warszawa 1999, s. 31.

[4] *Encyklopedia zdrowia, t .I*, Warszawa 1994, s. 1102–1103.

[5] A. Piotrowski, *Diagnostyczny i statystyczny podręcznik zaburzeń psychicznych,* Warszawa 1996, s. 124.

[6] Z. Zaborowski, *Problemy psychologii życia*, Wyd. Akademickie „Żak", Warszawa 2001, s. 226.

[7] G. Zimbardo, *Psychologia i życie*, PWN, Warszawa 1998, s. 448.

[8] Por. G. Zimbardo, *Psychologia i życie,* PWN, Warszawa 2002, s. 743.

[9] Tamże, s. 743.

się u niej niepohamowane pragnienie.[10] G. Zimbardo traktuje pojęcie uzależnienia szeroko i zakłada, że obejmuje ono nie tylko nadmierną zależność organizmu od alkoholu, nikotyny czy kofeiny, lecz także „(...) inne wypadki, kiedy ludzie czują się zmuszeni angażować się w ryzykowne, »wymykające się spod kontroli« zachowania (...)".[11] Natomiast L. Jampolsky stwierdza, że gdy „znajdujemy się w stanie frustracji, gniewu, gdy jesteśmy nieszczęśliwi, prawdopodobnie nie zdajemy sobie sprawy z tego, że nasz stan może prowadzić do uzależnienia".[12]

10 Uzależnienie objawia się w sferze psychicznej człowieka i jak podaje C. Cekiera: „uzależnienie psychiczne jest to stan psychiczny powstały w wyniku przyjmowania różnych środków uzależniających, przejawiających się różnorodnym stopniem pragnienia przyjmowania tych środków. Stopień ten może przejawiać się zwykłym pragnieniem, dającym się łatwo opanować; może to być także pożądanie posunięte aż do nieopanowanej żądzy i przymusu (...). Duże znaczenie ma zwyczaj, rytuał brania, sposób zażywania, chęć poprawienia sobie komfortu psychicznego lub usunięcia dyskomfortu. Dla uzależnionego człowieka zaabsorbowanie przyjmowanymi środkami staje się dominantą, a jego zachowanie nosi na sobie piętno zachowania nałogowego".[13]

11 Zatem uzależnieniem psychicznym nazywamy psychiczny przymus przyjmowania środka, co czynione jest w celu uzyskania efektów natury emocjonalnej – dla przyjemności bądź uzyskania odprężenia, relaksu, czy złudnego uciekania od codziennych problemów egzystencjalnych. Niemożność zaspokojenia tychże potrzeb prowadzi do podenerwowania, obniżenia nastroju, niepokoju, stanów lękowych, gniewu aż do myśli samobójczych włącznie.[14]

12 Według C. Guerreschi „uzależnienie oznacza zależność fizyczną i chemiczną, okoliczności, w których organizm, aby funkcjonować, domaga się określonej substancji. Słowem *nałóg* określa się ogólny stan, kiedy uzależnienie psychologiczne zmusza do poszukiwania przedmiotu, bez kontaktu z którym egzystencja uzależnionego zdaje się tracić sens".[15]

13 W przytoczonych definicjach uzależnienie odnosi się w większości przypadków do substancji chemicznych. **Niestety w polskiej literaturze naukowej nie można doszukać się określenia definiującego uzależnienie od komputera i Internetu. W przypadku tych urządzeń można mówić o uzależnieniu wówczas, gdy korzystanie z nich zaczyna przeszkadzać w normalnym życiu, w wykonywanej pracy, w kontaktach międzyludzkich, kiedy stanowi swoisty substytut rzeczywistego życia**. Jest to nowe zjawisko rozwijające się bardzo dynamicznie. Przypomnijmy, iż interpretować je można w dwojaki sposób jako uzależnienie od wykonywanych czynności na komputerze i w Internecie oraz uzależnienie od treści z jakich korzysta się za pośrednictwem tych urządzeń. Jest często konsekwencją nie radzenia sobie z problemami zwłaszcza takimi, których ludzie nie są wstanie sobie uświadomić, i nazwać. Największą grupę ryzyka stanowią dzieci i młodzież. To oni znaj-

[10] Tamże, s. 140.

[11] Tamże, s. 31.

[12] J. Jampolsky, *Leczenie uzależnionego umysłu,* Jacek Santorski & CO Agencja Wydawnicza, Warszawa 1992, s. 13.

[13] C. Cekiera, *Psychoprofilaktyka uzależnień oraz terapia i resocjalizacja osób uzależnionych*, Towarzystwo Naukowe KUL, Lublin 1993, s. 17.

[14] A. Nowak, E. Wysocka, *Problemy i zagrożenia społeczne we współczesnym świecie*, „Śląsk", Katowice 2001.

[15] C. Guerreschi, *Nowe uzależnienia*, Wyd. Salwator, Kraków 2006, s. 26.

dując się w tym pędzącym z zawrotnym tempie świecie, szukając dla siebie miejsca. Często właśnie komputer i Internet stanowią odskocznię, są niejako receptą na problemy, jakie je otaczają, na rozterki, jakie je trapią. A wiek ten w takie obfituje.

14 Uzależnienie może dotknąć człowieka na różnych poziomach. Na poziomie behawioralnym ujawnia się poprzez powtarzanie określonych zachowań. Jednocześnie uzależniony jest tak pochłonięty przedmiotem uzależnienia, że nie może się bez niego obejść i zaniedbuje inne sprawy. Negatywne skutki takiej sytuacji wpływają na jego życie i stają się przyczyną cierpienia, również dla osób go otaczających. W ostatnich latach coraz częściej mówi się o uzależniających właściwościach komputera i Sieci. Problem ten staje się coraz poważniejszy i dotyka coraz częściej dzieci i młodzież.[16]

15 **FORMY UZALEŻNIENIA OD KOMPUTERA I INTERNETU**

Jakie są zatem formy uzależnienia od komputera i Internetu? K. S. Young wyróżnia kilka podtypów tego uzależnienia:

- **uzależnienie od sieci internetowej** (*net compulsions*), polega na przymusowym byciu online. Osoby takie przez cały czas są zalogowane do Sieci i bacznie obserwują, co się tam dzieje;
- **przeciążenie informacyjne**, czyli przymus pobierania informacji (*information overload*), np. przebywanie w wielu pokojach rozmów jednocześnie, lub udział w wielu listach dyskusyjnych;
- **socjomanię internetową**, czyli uzależnienie od internetowych kontaktów społecznych (*cyberrelationship ad-diction*), polega na nawiązywaniu kontaktów społecznych tylko poprzez sieć. Dochodzi do zaburzenia relacji pomiędzy ludźmi w kontaktach rzeczywistych. Osoby uzależnione poświęcają swój cały wolny czas na rozmowy z innymi użytkownikami Internetu. Dochodzi u nich do rozchwiania w relacjach człowiek–człowiek. Następuje u nich zanik komunikacji niewerbalnej, nie potrafią prawidłowo odczytywać informacji na tej płaszczyźnie;
- **erotomanię internetową** (*cyberseksual addiction*), która polega na oglądaniu materiałów pornograficznych (filmy, zdjęcia), lub uczestniczeniu w czatach o charakterze erotycznym. Zjawisko to zaczyna być bardzo groźne, gdy na materiały o treści pornograficznej trafiają osoby małoletnie, lub z zaburzeniami w sferze emocjonalnej;
- **uzależnienie od komputera** (*computer addiction*), osoba ma przymus spędzania czasu przy komputerze. Nie jest istotne co robi, ważne jest aby komputer był cały czas włączony, a ona jest przy nim obecna".[17]

16 Autorka dokonała analizy charakterystycznych cech, które ukazują różnicę między normalnym używaniem Internetu, a patologicznym stosowaniem tego narzędzia. W zachowaniu internautów wyróżniła trzy fazy, które przechodzą użytkownicy na swojej drodze prowadzącej ich do uzależnienia[18]:

I Faza – zaangażowania

Ta faza uzależnienia zaczyna się od zapoznania się z Internetem. Człowiek poznaje jego możliwości. Na początku istotną rolę odgrywają uczucia związane z odkrywaniem nowej rzeczywistości po włączeniu komputera. Jest to uczucie zainteresowania i oczekiwania, zafascynowania i uczucie przypływu sił, pożądane zwłaszcza wtedy, gdy ktoś miał trudny dzień i potrzebuje odprężenia. Nawiązanie kontaktu

[16] B. Danowski, A. Krupińska, *Dziecko w sieci*, Wyd. HELION, Gliwice 2007, s. 31.

[17] K. S. Young, *Pathological Internet Use: A Case that Breaks the Stereotype*, Psychological Reports, 1996, s. 899-902.

[18] Tamże.

OPIS ZJAWISKA

ROZPOZNANIE OBJAWY

poprzez Internet powoduje, że znika poczucie osamotnienia, znudzenia. Na początku internauta może odczuwać coś w rodzaju euforii. Po krótkim czasie, w trakcie i tuż po wędrówce po Internecie, może odczuwać spokój. Ludzie często zgłaszali poczucie „braku granic" i poczucie „zjednoczenia z całym światem".

II Faza – zastępowania

Ta faza uzależnienia polega na tym, że te silne odczucia są zastępowane przez zwykłą redukcję dyskomfortu. Internauta czuje potrzebę kontynuowania kontaktów zawartych w sieci dla zachowania poczucia równowagi życiowej, które daje mu ulgę. Zaczyna wchodzić we wspólnotę internetową, rezygnuje z osób, rzeczy, które były dotąd częścią jego życia. Osoby uzależnione wskazywały, że umysł często był zajęty myślami o Internecie, tym, co będą robić, jak tylko się połączą z siecią. Często myśli te towarzyszyły im podczas spotkań z rzeczywistymi znajomymi.

III Faza – ucieczki

Ta faza charakteryzuje się tym, że uzależnienie się pogłębia. Osoba uzależniona chce i potrzebuje coraz większej ilości czasu spędzonego w Internecie. Następuje całkowita ucieczka od świata realnego. Uzależnieni nie traktują Internetu jako narzędzia służącego do komunikacji, zbierania informacji lub rozrywki. Chodzi im bardziej o formę ucieczki przed codziennymi problemami, o których na chwilę zapominają, gdy są *online*. Po wyjściu z sieci, ze zdwojoną siłą wracają ich problemy. Pogłębia się depresja, intensyfikuje się samotność, pojawiają się wyrzuty sumienia z powodu zaniedbywania obowiązków, żony, dzieci.

17 Najbardziej uzależniające są te formy korzystania z sieci, które dotyczą kontaktów interpersonalnych. IRC wirtualne kawiarenki, ICQ usługi, które gromadzą największą liczbę osób niemogących żyć bez sieci. Uzależniony internauta woli wirtualny kontakt z osobami, których nigdy nie widział na oczy, niż z osobami najbliższymi i co ciekawe, siecioholicy spędzają na takim symulowanym kontakcie z bliźnim więcej czasu niż ludzie obcujący ze sobą w tradycyjny sposób. Z jednej strony mamy obawę przed kontaktami międzyludzkimi, z drugiej zaś potrzebę drugiego człowieka. Kolejną usługą pułapką są gry komputerowe, a w szczególności online, uczestnicząc w świecie wykreowanym przez programistów zmierzamy się w tym samym czasie z innymi graczami będącymi po drugiej stronie monitora. Wyższością gier w sieci jest fakt, że jak na razie ludzie są lepsi od elektronicznych przeciwników i gra z drugim człowiekiem jest bardziej pasjonująca.

18 PRZYCZYNY UZALEŻNIENIA

Przyczyn uzależnienia jest oczywiście wiele i zależą one w dużej mierze od osoby, która wpadła w nałóg. Oczywiste jest, że osoby o silnej psychice i zrównoważone emocjonalnie trudniej poddają się destruktywnym wpływom, natomiast te słabsze, o zaniżonej samoocenie, mające problemy z własną tożsamością, są bardziej podatne na wszelkiego rodzaju uzależnienia.

Nadmierne korzystanie z komputera i Internetu zdaniem S. Jaskuły wiąże się z następującymi cechami odbiorcy: „wrażliwość na społeczne odrzucenie (lęk przed odrzuceniem, lęk społeczny) i problemy z otwartą komunikacją interpersonalną, niska inteligencja emocjonalna i kompetencje społeczne oraz powiązane z nimi nieśmiałość i zewnętrznie usytuowane poczucie kontroli. Nałogowi inter-

nauci są osobami skłonnymi do izolacji społecznej, pozostawania w samotności, to niekwestionowani indywidualiści, polegający głównie na sobie, o wysoce rozwiniętym myśleniu abstrakcyjnym. Jednocześnie osoby takie cechuje lękliwość, nadwrażliwość emocjonalna, skłonność do pesymistycznego myślenia i nadmiernego samokrytycyzmu, impulsywność i mała odporność na stres. Na drodze badań potwierdzono również związek uzależnienia z niską samooceną"[19].

Szukając przyczyn uzależnień, można rozpatrywać je w dwóch obszarach, biorąc pod uwagę czynniki:

- **wewnętrzne,**
- **zewnętrzne.**

19 **Do wewnętrznych można zaliczyć problemy dzieci i młodzieży z własną osobowością.** Młodzi ludzie przeżywają poczucie zagubienia w świecie, poszukują sensu istnienia, wartości, które mogliby uznać za swoje. Przeżywają konflikty wewnętrzne w kilku sferach: stosunku do samego siebie, do własnej rodziny, w kontaktach z rówieśnikami. Odczuwają napięcia emocjonalne, bywają nieufni i samotni. Doznania takie mają wszyscy albo prawie wszyscy, nie wszyscy jednak są w stanie konstruktywnie z nimi się zmierzyć. Najłatwiejszą ucieczką od tych problemów jest wirtualna rzeczywistość, po którą sięgają z coraz większą częstotliwością. Na tym tle może rozwinąć się uzależnienie.

20 Uzależnienie stanowi zaskoczenie, kiedy już się rozwinie i ujawni. Zwykle następuje to w dłuższym odstępie czasu od momentu, gdy pierwsze kontakty z czynnikiem uzależniającym nasiliły się w sposób mogący kogokolwiek zaniepokoić. Wyjątkiem jest uzależnienie ludzi bardzo młodych, mogące się rozwinąć zdecydowanie szybciej, już w kilka miesięcy.

21 Szczególnie łatwo popaść w uzależnienie od Internetu. Kiedy mamy problemy, z którymi nie jesteśmy sobie w stanie poradzić, w sieci odnajdziemy osoby o podobnych cechach charakteru, które chętnie poświęcą nam czas i z którymi rozmowa sprawi nam wiele przyjemności. W realnym świecie odnalezienie takich osób jest znacznie trudniejsze. Bywają osoby nieśmiałe o niskim poczuciu wartości, które nie osiągają satysfakcji życiowej, to one są największymi uciekinierami. W Internecie łatwiej jest kogoś poznać i zawrzeć nową przyjaźń. Tu nie trzeba zmagać się z obezwładniającą tremą i obawiać się, czy postępujemy zgodnie z obowiązującymi zasadami.

22 **Głównymi predyspozycjami charakterologicznymi, które mogą sprzyjać uzależnieniu są** m.in.:

- niska samoocena – brak wiary we własne siły,
- brak dojrzałości emocjonalnej – labilność uczuciowa, dominacja negatywnych uczuć i emocji, nieumiejętność budowania relacji społecznych,
- nieumiejętność radzenia sobie ze stresem i cierpieniem,
- negatywny wizerunek samego siebie,
- nieumiejętność nawiązywania kontaktów interpersonalnych.

23 **PRZYCZYNY ZEWNĘTRZNE**

Do czynników zewnętrznych można zaliczyć: wpływy środowiska rodzinnego, szkolnego i rówieśniczego.

19 S. Jaskuła, *Internet jak narkotyk*, „Świat Problemów", 12/2008, s. 12.

24 **Przyczyny uzależnienia mające podłoże w rodzinie**

„Środowisko rodzinne jest podstawowym środowiskiem wychowawczym kształtującym psychikę dziecka, warunkującym jej rozwój, zachowanie dziecka. Z rodziny dziecko czerpie wzorce zachowań, które rzutują na jego późniejszy rozwój i zachowanie”[5].

25 Rodzina oddziałuje na jednostkę od momentu narodzin przez bardzo długi czas. Wychowanie jest procesem, który decyduje o późniejszym funkcjonowaniu człowieka. Odbywa się ono w sytuacjach dnia codziennego i ma charakter socjalizujący. Może prowadzić do rozwoju człowieka lub ten rozwój hamować.

26 Zaburzenia związane z sięganiem przez dzieci po substancję bądź czynnik uzależniający często tkwią w błędach wychowawczych rodziców. Wśród przyczyn leżących po stronie rodziców jest nieumiejętność doboru metod wychowawczych, które powinny uwzględniać predyspozycje dziecka. Zbyt wygórowane, a także sprzeczne wymagania w stosunku do niego mogą powodować napięcia i frustracje. Innym źródłem zaburzeń prowadzącym do popadnięcia w uzależnienie jest zapominanie przez rodziców, że dziecko ma wiele potrzeb psychicznych, do których przede wszystkim można zaliczyć potrzebę bezpieczeństwa i przynależności.

27 Uogólniając, można wskazać na kilka zasadniczych czynników, ze strony rodzinnego środowiska wychowawczego, które mogą stanowić podłoże uzależnienia:

brak więzi emocjonalnych,

brak kontroli ze strony rodziców, opiekunów,

źle zaplanowany czas wolny,

częste awantury i zła atmosfera w domu,

brak poczucia bezpieczeństwa,

niska samoocena pogłębiana przez rodziców itp.

28 **Przyczyny ze strony środowiska szkolnego prowadzące do zachowań destruktywnych (w tym uzależnień)**

„Wychowanie jest procesem, którego istotą są interakcje między wychowawcą a wychowankiem; ich skutkiem jest zasób doświadczeń zdobytych przez wychowanka. Środowiskiem wychowawczym stwarzającym tę możliwość jest szkoła i różnorodność zachodzących w niej relacji”[21].

29 „Prawidłowo zorganizowane środowisko powinno być bogate w bodźce stymulujące rozwój zainteresowań, rozbudzające sferę poznawczą, ruchową i społeczną dziecka (…). Zwraca się uwagę na przeżycia emocjonalne wynikające z jakości relacji zachodzących między dzieckiem a nauczycielem, między samymi dziećmi, jak również na przeżycia związane z rodzajem podejmowanej przez dziecko aktywności i miejscem, w którym dziecko przebywa”[22].

[20] A. Chybowska, J. Szanejko, *Warunki społecznego rozwoju*, „Edukacja i Dialog”, 3/2001, http://www.vulcan.edu.pl/eid/archiwum/2001/03/warunki_rozwoju.html, data dostępu: 20.10.2012.

[21] A. Chybowska, J. Szanejko, *Warunki społecznego rozwoju,* „Edukacja i Dialog”, 3/2001, http://www.vulcan.edu.pl/eid/archiwum/1998/01/szkola.html data dostępu: 23.10.2012.

[22] Tamże.

30 Do przyczyn tkwiących w środowisku szkolnym, a sprzyjających uzależnieniom można zaliczyć:

- upadek autorytetów moralnych,
- nadmierne obciążenie lekcjami (obszerne programy nieodpowiadające poziomowi intelektualnemu dzieci i młodzieży),
- słaba więź ze szkołą,
- brak nauczycieli szczególnie obdarzonych powołaniem,
- poczucie „inności", „niższości",
- brak w programach oświatowo-wychowawczych treści uwzględniających problematykę uzależnień od mediów.

31 **Przyczyny prowadzące do uzależnień ze strony środowiska rówieśniczego**

Na rozwój dziecka ma również wpływ środowisko rówieśnicze. Dzięki relacjom z rówieśnikami, dzieci i młodzież nabywają umiejętności w relacjach społecznych. Zgodnie z poglądem Z. Gasia, relacje te dotyczą przede wszystkim „poczucia pewności siebie wśród innych ludzi, poczucia bycia akceptowanym przez innych, sprawności w kontaktach z ludźmi oraz samodzielności i tolerancji społecznej"[23].

32 Spośród wielu przyczyn destruktywnych zachowań dzieci i młodzieży, ogromny wpływ odgrywa oddziaływanie grup rówieśniczych, w których spędzają wolny czas. W zależności od środowiska, z jakiego pochodzą rówieśnicy, kształtuje się ich obopólny światopogląd, poprzez wzajemne oddziaływanie na siebie.

33 Do przyczyn tkwiących w środowisku rówieśniczym, które mogą wpływać na uzależnienie od mediów można zaliczyć:

- nieprawidłowe relacje pomiędzy rówieśnikami,
- niepewność własnej atrakcyjności,
- nieumiejętność komunikowania się, w tym z płcią przeciwną,
- trudność określenia swego miejsca w środowisku rówieśniczym.

34 Zaburzenia pojawiające się w wyżej wymienionych płaszczyznach mogą prowadzić do ucieczki w wirtualny świat, gdzie wszystko jest przyjemne i proste.

35 **SYMPTOMY PROBLEMU**

K. Kaliszewska, klasyfikując skutki uzależnienia od komputera i Internetu wskazuje następujące zjawiska:

- „zanik więzi rodzinnych, utrata przyjaciół, wyizolowanie społeczne,
- utrata zainteresowań, osłabienie siły i woli osobowości, utrata kontroli nad zachowaniem,

[23] W. Poleszak, *Diagnoza relacji rówieśniczych*, w: Z. Gaś, *Badanie zapotrzebowania na profilaktykę w szkole,* Wyd. MENIS, Warszawa 2004, s. 156.

ĆWICZENIA 19

zaniedbywanie obowiązków szkolnych i domowych, co może wiązać się z niezdaniem do następnej klasy,

zaniedbywanie zdrowia (nieprawidłowe odżywianie, brak ruchu, nieregularny sen, problemy z kręgosłupem, bóle głowy, zmęczenie, zaniedbywanie higieny osobistej[24].

36 W analizie przebiegu uzależnienia przedstawionego na przykładzie Internetu wyróżnić można **następujące fazy, w których podano najważniejsze symptomy problemu**:

I. Faza początkowa

1. Przebywanie w sieci sprawia przyjemność.
2. Wzrost ochoty na coraz częstsze przebywanie w sieci.

W fazie tej następuje utrata poczucia czasu.

II. Faza ostrzegawcza

1. Szukanie okazji do jak najczęstszego przebywania w sieci.
2. Rozładowanie napięcia poprzez sieć.
3. Próby korzystania z sieci w ukryciu.
4. Korzystanie z sieci przynosi ulgę.

Charakteryzuje ją brak chęci powrotu do rzeczywistości.

III. Faza krytyczna

1. Spadek innych zainteresowań niezwiązanych z siecią.
2. Zaniedbywanie wyglądu zewnętrznego.
3. Zaniedbywanie snu.
4. Nieregularne odżywianie się.
5. Silna potrzeba przebywania w sieci.
6. Stałe myślenie o tym, co dzieje się w sieci, o tym, co ostatnio robiliśmy podczas sesji.
7. Potrzeba zwiększania ilości czasu spędzanego w sieci.
8. Podejmowanie nieudanych prób ograniczenia czasu spędzanego w sieci.
9. Poczucie rozdrażnienia, poirytowania, złości, gdy coś lub ktoś zmusza nas do skrócenia czasu uczestnictwa w sieci lub uniemożliwia korzystanie z niej.
10. Zaniedbywanie nauki, pracy, rezygnacja ze spotkań towarzyskich, odkładanie na później pilnych zadań na rzecz korzystania z sieci.
11. Okłamywanie innych odnośnie ilości czasu spędzanego w sieci (zaniżanie faktycznej ilości godzin spędzanych przy komputerze).
12. Pojawienie się konfliktów rodzinnych w związku z komputerem.
13. Przeznaczanie coraz większej ilości pieniędzy na zakup sprzętu komputerowego, oprogramowania, akcesoriów czy książek i czasopism o tematyce komputerowej.

Następuje w niej utrata kontroli nad własnym zachowaniem.

IV. Faza przewlekła

1. Okresy długotrwałego przebywania w sieci.
2. Przebywanie w sieci w celu przeżywania silnych emocji.
3. Świat wirtualny staje się jedynym światem w życiu.
4. Rozpad więzi rodzinnych.
5. Degradacja zawodowa i społeczna.
6. Choroby somatyczne.
7. Lęki, psychozy.
8. Sięganie po inne środki zmieniające nastrój (alkohol, leki).
9. Poczucie bezsensu życia w świecie realnym.

Skrajne wyczerpanie organizmu.

Jej cechą jest właściwe uzależnienie.

37 **DYLEMATY Z WYZNACZANIEM GRANIC**

Od pierwszych doniesień wskazujących na problemy pojawiające się u osób nadmiernie korzystających z komputera lub Internetu minęło kilkanaście lat. Mimo

[24] K. Kaliszewska, Nadmierne używanie Internetu. Charakterystyka psychologiczna. Wyd. Naukowe UAM, Poznań, s. 38–39.

coraz większego zainteresowania tą kwestią przez wiele środowisk, **jak do tej pory nie udało się wypracować spójnej i klarownej koncepcji teoretycznej, która ujmowałaby etiologię, mechanizm powstawania oraz bliskie i odległe konsekwencje nadmiernego używania komputera i Internetu, co więcej nie ma jasnych kryteriów diagnostycznych pozwalających na rozpoznanie tego problemu** – co dla opisania specyfiki zjawiska wydaje się kwestią kluczową.

38 Istnieją spory wokół diagnozy. Nie ma zgody badaczy w sprawie stworzenia nowej kategorii diagnostycznej dla zdefiniowania patologicznego korzystania z komputera i Internetu. Są także tacy naukowcy, którzy kwestionują uznanie nadmiernego korzystania z sieci za uzależnienie. Należy do nich m.in. amerykański psychiatra J. Grohol. „Nie rozumiem, dlaczego tyle uwagi poświęca się tzw. mrocznej stronie Internetu – mówi ten badacz. Ludzie spędzają całe dnie na pielęgnacji ogródka, grze w brydża czy czytaniu gazet, a nikt z tego powodu nie trąbi na alarm”[25]. I. Goldberg, psychiatra z Uniwersytetu Columbia, dodaje: „Gdyby 100 lat temu psychiatria zajmowała taką pozycję, jak dziś, powstawałyby kluby Anonimowych Czytelników Powieści”[26]. Ich adwersarze przypominają, że podobnie wyglądała sytuacja, kiedy R. Custer w 1980 r. przedstawił badania wskazujące na podobieństwo między zamiłowaniem do hazardu i alkoholizmem. Też spotkał się wówczas z ogromną krytyką środowiska psychologicznego i psychiatrycznego. Musiało upłynąć kilkanaście lat od wspomnianego wydarzenia, aby termin „uzależnienie od hazardu” został wpisany do leksykonów medycznych. Dziś niemal każdy ośrodek odwykowy ma oddział dla kompulsywnych graczy.

39 Podobnie wygląda sytuacja z Internetem. Nie można przyjąć jednej określonej terminologii związanej z nadmiernym niekontrolowanym użytkowaniem tych narzędzi. Negatywne konsekwencje opisywane w literaturze trudno uznać za kryteria, są one jedynie zbiorczą listą objawów obserwowanych u poszczególnych pacjentów. **W literaturze przedmiotu odnaleźć można następujące terminy przyjęte na określenie tego zjawiska:**

- problematyczne używanie Internetu,
- zależność od Internetu,
- patologiczne używanie Internetu,
- zaburzenie polegające na uzależnieniu od Internetu (Internet Addicion Disorder)
- uzależnienie od Internetu[27]
- zespół uzależnienia od Internetu[28]

Dlatego podstawowym i naglącym problemem do rozwiązania przez naukowców na drodze kolejnych badań empirycznych w obszarze negatywnego oddziaływania Internetu i jego konsekwencji jest:

1. Ustalenie granicy pomiędzy zdrowym, a patologicznym używaniem Internetu.
2. Wyznaczenie kryteriów diagnostycznych, które mimo niskiej wiedzy o tym zjawisku byłyby na tyle precyzyjne, że umożliwiałyby swobodne prowadzenie badań uwzględniających specy-

[25] P. Dębek, L. Szawdyn, *Złapani w sieć,* „Chip Online”, http://www2.chip.pl/archiwum/article_14286.html, data dostępu: 10.02.2012.

[26] Tamże.

[27] K. Kaliszewska, *Zjawisko nadmiernego używania Internetu w Poznawczo-Behawioralnym Modelu Davi,* „Forum Oświatowe” 2005, s. 139.

[28] A. Jakubik, *Zespół uzależnienia od Internetu (ZUI),* http://www..psychologia.edu.pl data dostępu: 16.01.2012.

ficzne problemy ludzi związane z nadmiernym i jednocześnie szkodliwym korzystaniem z Internetu.
3. Opisanie zjawiska nadmiernego używania Internetu w jasny sposób w podstawach teoretycznych[29].

40 W Stanach Zjednoczonych, gdzie zjawisko uzależnienia od Internetu występuje już od ponad 10 lat, pierwszą osobą prowadzącą badania w tym zakresie była wspomniana psychiatra z Pittsburga dr Kimberly S. Young. Jest ona najbardziej znanym ekspertem badającym zjawisko uzależnienia od Internetu, członkiem Amerykańskiego Towarzystwa Psychologicznego, w Pensylwanii Psychological Association, a także członkiem-założycielem Międzynarodowego Towarzystwa Zdrowia Psychicznego *online*. K. S. Young również nie podaje wiążącej definicji uzależnienia. Stwierdza natomiast, że uzależnienie od Internetu może być definiowane jako zaburzenie kontroli impulsów niepowodujące intoksykacji[30].

41 **DIAGNOZA**

Diagnoza jest procesem poszukiwania danych potrzebnych do podjęcia działań zmierzających do zmiany aktualnego stanu psychospołecznego ludzi.

42 Aby określić, czy dane zachowanie przejawia charakter uzależnienia, M. D. Griffiths zaproponował następujące **kryteria kliniczne tego zjawiska**:

1. **Wyrazistość emocjonalnego podporządkowania** – konkretne zachowanie się jest motywem przewodnim w życiu uzależnionego, przejmuje kontrolę nad jego myśleniem, uczuciami, zachowaniem.
2. **Zmiana nastroju** – to subiektywne doświadczenie, które przez osoby uzależnione uznawane jest za konsekwencję ich działań. Może być postrzegane jako sposób radzenia sobie z emocjami, ucieczki lub odseparowania się od otaczającej rzeczywistości.
3. **Tolerancja dawkowania** – w miarę upływu czasu, aby osiągnąć te same rezultaty emocjonalne potrzebna jest coraz większa „dawka" danego zachowania.
4. **Objawy odstawienia** – przerwanie bądź nagłe ograniczenie pożądanej aktywności wywołuje nieprzyjemne uczucia i objawy fizjologiczne.
5. **Konflikt** – może on występować pomiędzy najbliższym otoczeniem, a osobą uzależnioną, bądź też może to być dyskonflikt wewnętrzny, podczas którego uzależniony traci poczucie kontroli nad samym sobą.
6. **Nawrót** – tendencja powracania do negatywnych wzorców postępowania, nawet po wielu latach abstynencji i kontroli[31].

43 Jak przyznaje J. Grohol, osoby spędzające zbyt dużo czasu w sieci mogą być narażone na występowanie poważnych problemów, jednak nie należy każdego potencjalnego niebezpieczeństwa nawyku czynić nową kategorią diagnostyczną. Według niego nadmierne korzystanie z Internetu stanowić może jedną z form ucieczki od problemów, zaburzeń zdrowia, takich samych jak praca, czytanie książek czy oglądanie telewizji. Tego rodzaju postawy mogą doprowadzić do kompulsywnego korzystania z Internetu i telewizji czy jakiegokolwiek innego. **Zachowania kompulsywne, inaczej natręctwa, są jednak włączone w ogólniejsze kategorie diagnostyczne**

[29] K. Kaliszewska, *Zagubieni w sieci – czyli o nadmiernym użytkowaniu zasobów i możliwości Internetu*, w: L. Cierpiałkowska (red.), *Oblicza współczesnych uzależnień*, Wyd. Naukowe UAM, Poznań 2006, s. 112–113.

[30] K.S. Young, *Caugh in the Net*, John Wiley & Sons, New York 1998.

[31] M. Griffiths, *Gry i hazard. Uzależnienia dzieci w okresie dorastania*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2004, s. 11–12.

i w odniesieniu do nich jest już sprawdzona w praktyce metoda terapeutyczna zakładająca, iż technologia nie odpowiada za powstawanie natręctw czy uzależnień[32].

W roku 1999 J. Grohol opracował **III fazy rozwoju patologicznego nawyku korzystania z Internetu**:

I Faza – fascynacja.

II Faza – rozczarowanie (oderwanie się od sieci, która traci na atrakcyjności z chwilą, gdy przestaje być nowością, która kusi).

III Faza – równowaga (odpowiedzialne i właściwe podejście do korzystania z sieci).

44 Opisując te fazy autor pokazuje, że patologiczne korzystanie z Internetu jest związane z I fazą zetknięcia się z nowym światem, który przyciąga z nieodpartą siłą. Osoby, które przechodzą do kolejnych faz, nie podlegają zaburzeniom[33]. Nasuwa się tu jednak pytanie, co z osobami, którym nie uda się z niej wyjść?

45 Innym kryterium diagnostycznym siecioholizmu może być **klasyfikacja DSM-IV** (*Diagnostic and Statistical Manual of Mental Disorders*). Jest to system diagnozy nozologicznej Amerykańskiego Towarzystwa Psychiatrycznego. Stanowi narzędzie dla lekarzy rodzinnych, psychiatrów, psychologów i psychoterapeutów. Zgodnie z tym kryterium uzależnienie można rozpatrywać, jeśli w ciągu 12 miesięcy przynajmniej trzy objawy występują równocześnie.

Tymi objawami mogą być:
„I. **Tolerancja**, która może się ujawniać w dwojaki sposób:

A. Zwiększenie czasu korzystania z Internetu dla osiągnięcia tej samej satysfakcji.
B. Wyraźny spadek satysfakcji przy korzystaniu z Internetu przez taki sam czas.

II. **Zespół abstynencyjny**.
A. Objawy typowe dla zespołu abstynencyjnego:
1. Nieudane próby zaprzestania lub zredukowania czasu korzystania z Internetu.
2. Co najmniej dwa z wymienionych kryteriów pojawiające się w ciągu kilku dni do miesiąca od zaprzestania lub zredukowania czasu korzystania z komputera:
   a. pobudzenie psychoruchowe,
   b. lęk,
   c. obsesyjne myślenie o tym, co dzieje się w Internecie,
   d. fantazje i marzenia senne o Internecie,
   e. dowolne lub mimowolne naśladowanie ruchów palców na klawiaturze.
3. Wymienione objawy powodują zaburzenia w funkcjonowaniu społecznym, zawodowym i innych ważnych sferach życia.

B. Korzystanie z Internetu w celu uniknięcia zespołu abstynencyjnego.

III. **Częstotliwość i czas korzystania z Internetu większe od zamierzonych**.

IV. **Uporczywe pragnienie zaprzestania lub ograniczenia korzystania z Internetu**.

V. **Większość zajęć koncentrowana na czynnościach związanych z Internetem** (np. porządkowanie plików, kupowanie książek o sieci, poznawanie no-

[32] J. Grohol, *Internet addiction guide*, http://psychcentral.com.netaddiction data dostępu: 15.09.2012.

[33] Tamże.

wych wyszukiwarek, ściąganie nowych plików).

VI. **Ograniczenie lub rezygnacja z czynności i zainteresowań** (społecznych, zawodowych, rekreacyjnych) istniejących przed uzależnieniem na rzecz korzystania z Internetu.

VII. **Korzystanie z Internetu pogłębia się mimo świadomości szkodliwych następstw fizycznych, społecznych lub psychologicznych** (np. ograniczenia snu, problemów rodzinnych, spóźniania się, zaniedbywania obowiązków, rezygnacji z innych form aktywności)

46 TEST K. S. YOUNG

K. S. Young podaje inną klasyfikację kryteriów diagnostycznych uzależnienia od Internetu. Opracowała **test diagnostyczny**, który po przeprowadzeniu **pozwala stwierdzić możliwość uzależnienia**. Pięć pozytywnych odpowiedzi na poniższe pytania daje wynik pozytywny:

1. Czy czujesz się zaabsorbowany Internetem do tego stopnia, że ciągle rozmyślasz o odbytych sesjach internetowych i/lub nie możesz doczekać się kolejnych sesji?
2. Czy odczuwasz potrzebę zwiększenia ilości czasu spędzanego w Internecie, aby uzyskać większe zadowolenie (mieć więcej satysfakcji)?
3. Czy podejmowałeś wielokrotnie nieudane próby kontrolowania, ograniczania lub zaprzestania korzystania z Internetu?
4. Czy odczuwałeś wewnętrzny niepokój, miałeś nastrój depresyjny albo byłeś rozdrażniony wówczas, kiedy próbowałeś ograniczać lub przerwać korzystanie z Internetu?
5. Czy zdarza Ci się spędzać w Internecie więcej czasu niż pierwotnie zaplanowałeś?
6. Czy kiedykolwiek ryzykowałeś utratę bliskiej osoby, ważnych relacji z innymi ludźmi, pracy, nauki albo kariery zawodowej w związku ze spędzaniem zbyt dużej ilości czasu w Internecie?
7. Czy kiedykolwiek skłamałeś swoim bliskim, terapeutom albo komuś innemu, w celu ukrycia własnego nadmiernego zainteresowania Internetem?
8. Czy używasz Internetu w celu ucieczki od problemów albo w celu uniknięcia nieprzyjemnych uczuć (np. poczucia bezradności, poczucia winy, niepokoju lub depresji)?[35].

Należy jednak stwierdzić, iż test ten przygotowany w połowie lat 90. ubiegłego stulecia zawiera kategoryczne i jednoznaczne pytania, stąd rozstrzygnięcia są bardzo uogólnione.

47 PODSUMOWANIE

Celem korzystania z komputera i internetu jest poprawa nastroju, odprężenie, uzyskanie satysfakcji, ucieczka od problemów, chęć zapomnienia o kłopotach. Nadmierne użytkowanie jest konsekwencją nieradzenia sobie z problemami, zwłaszcza takimi, których ludzie nie są w stanie sobie uświadomić i nazwać. Ogarnia coraz szersze grono ludzi i wymaga dalszych analiz.

BIBLIOGRAFIA:

Afftab P., *Internet a dzieci. Uzależnienia i inne niebezpieczeństwa*, Wyd. Prószyń-

[34] I. Pospiszyl, *Patologie społeczne. Resocjalizacja,* Wyd. Naukowe PWN, Warszawa 2008, s. 189.

[35] Por. K. S. Young, *Caught In The Net*, J. Wiley & Sons, New York 1998; http://www.netaddiction.com/ data dostępu: 10.02.2013.

ski i S-ka, Warszawa 2003.

Cekiera C., *Psychoprofilaktyka uzależnień oraz terapia i resocjalizacja osób uzależnionych*, Towarzystwo Naukowe KUL, Lublin 1993.

Chybowska A., Szanejko J., *Warunki społecznego rozwoju,* „Edukacja i Dialog", 3/2001, http://www.vulcan.edu.pl/eid/archiwum/2001/03/warunki_rozwoju.html, data dostępu: 20.10.2012.

Danowski B., Krupińska A., *Dziecko w sieci*, Wyd. HELION, Gliwice 2007.

Dębek P., Szawdyn L., *Złapani w sieć,* „Chip Online", http://www2.chip.pl/archiwum/article 14286.html, data dostępu: 10.02.2012).

Encyklopedia zdrowia, t .I, Warszawa 1994.

Filipiak M., *Homo Communicans wprowadzenie do teorii masowego komunikowania,* Wyd. Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2003.

Griffiths M., *Gry i hazard. Uzależnienia dzieci w okresie dorastania*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2004.

Grohol J., *Internet addiction guide*, http://psychcentral.com.netaddiction, data dostępu: 15.09.2012.

Guerreschi C., *Nowe uzależnienia*, Wyd. Salwator, Kraków 2006.

Jakubik A., *Zespół uzależnienia od Internetu (ZUI) – Internet Addiction Syndrome (IAS),* http:///www.psychologia.net.pl, data dostępu: 16.01.2012.

Jampolsky J., *Leczenie uzależnionego umysłu,* Jacek Santorski & CO Agencja Wydawnicza, Warszawa 1992.

Jaskuła S., *Internet jak narkotyk*, „Świat Problemów", 12/2008.

Kaliszewska K., *Nadmierne używanie Internetu. Charakterystyka psychologiczna*. Wyd. Naukowe UAM, Poznań 2010.

Kaliszewska K., *Zagubieni w sieci – czyli o nadmiernym użytkowaniu zasobów i możliwości Internetu*, w: Cierpiałkowska L. (red.), *Oblicza współczesnych uzależnień*, Wyd. Naukowe UAM, Poznań 2006.

Kaliszewska K., *Zjawisko nadmiernego używania Internetu w Poznawczo-Behawioralnym Modelu Davi,* „Forum Oświatowe" 2005 .

Nowak A., Wysocka E., *Problemy i zagrożenia społeczne we współczesnym świecie*, „Śląsk", Katowice 2001.

Piotrowski A., *Diagnostyczny i statystyczny podręcznik zaburzeń psychicznych,* Warszawa 1996.

Poleszak W., *Diagnoza relacji rówieśniczych*, w: Gaś Z., *Badanie zapotrzebowania na profilaktykę w szkole,* Wyd. MENIS, Warszawa 2004.

Pospiszyl I., *Patologie społeczne*. *Resocjalizacja,* Wyd. Naukowe PWN, Warszawa 2008.

Szawdyn L., *Co to znaczy być uzależnionym od Internetu*, „Magazyn Internetowy WWW, 2/1999.

Wallach P., *Psychologia Internetu,* Dom Wydawniczy REBIS, Poznań 2001.

Young K. S., *Caught In The Net*, J. Wiley & Sons, New York 1998.

Young K. S., *Internet Addiction: Symptoms, Evaluation and Treatment*, w: Van de Crek I., Jackson X., *Innovations in Clinical a Source Book,* Sarasota FL. Pro-

fessional Resource Press, 1999.

Young K. S., *Pathological Internet Use: A Case that Breaks the Stereotype*, "Psychological Reports", 1996 .

Zaborowski Z., *Problemy psychologii życia*, Wyd. Akademickie „Żak", Warszawa 2001.

Zimbardo P. G., *Psychologia i życie*, Wyd. Naukowe PWN, Warszawa 1999.

SZCZEGÓŁOWY
PROGRAM SZKOLENIA

Józef Bednarek

PROGRAM SZKOLENIA - ZAGROŻENIA ZWIĄZANE Z UZALEŻNIENIAMI	
Sposób realizacji	Warsztat
Materiały	**Materiały dydaktyczne dla uczestników szkolenia:** materiały szkoleniowe (finalna wersja produktu); b) inne materiały poglądowe i dokumenty innych specjalistycznych instytucji szkoleniowych i profilaktycznych; c) analiza systemowa i procesualna uzależnień i gier komputerowych. _
Treści merytoryczne	**blok tematyczny: (8h dydaktycznych)** 1. Podstawy teoretyczne (definicje, wyniki badań, skala i zasięg zagrożeń uzależnień i zagrożeń gier komputerowych. 2. Przyczyny uzależnień i grania w gry komputerowe. 3. Przebieg uzależnień i grania w gry komputerowe. 4. Objawy uzależnień i grania w gry komputerowe. 5. Skutki uzależnień i grania w gry komputerowe. 6. Dobre praktyki (działania) związane z uzależnieniami i graniem w gry komputerowe. 7. Nowe kompetencje społeczno-wychowawcze pracownika socjalnego w zakresie uzależnień i grania w gry komputerowe.
Obszary	Efekty kształcenia
Wiedza zdobyta w czasie zajęć	W wyniku przeprowadzonych zajęć, Uczestnik powinien być w stanie: • wymienić ogólne podstawy teoretyczne uzależnień i zagrożeń grania w gry komputerowe; • rozumieć uwarunkowania, prawidłowości oraz mechanizmy uzależnień i grania w gry komputerowe; • posiadać orientację stanu i zasięgu uzależnień i zagrożeń.
Umiejętności zdobyte w czasie zajęć	Umiejętności w zakresie: • diagnozowania przyczyn, przebiegu, objawów, skutków uzależnień i zagrożeń; • umieć przeciwdziałać i realizować profilaktykę w zakresie uzależnień o zagrożeń: • doskonalić niezbędne kompetencje społeczno-wychowawcze w zakresie uzależnień i grania w gry komputerowe.
Forma zajęć	Zajęcia grupowe, analiza realizowanych zadań w zespołach, studia indywidualnych przypadków uzależnień i ich konsekwencji.
Metody prowadzenia zajęć	Wykład, ćwiczenia aktywizujące, grupowe, inscenizacja uzależnień i zagrożeń, burza mózgów, dyskusja, wymiana poglądów.
Zalecane ćwiczenia	Ćwiczenia 15-18 znajdujące się w module *Kształcenie*
Sprawdzenie efektów szkolenia	Ankiety, testy kompetencyjne, aktywny udział w dyskusji, odpowiedzi na pytania.

ZAGROŻENIA
DLA PIENIĘDZY

Marcin Bochenek, Piotr Bisialski,
Martyna Różycka, Anna Rywczyńska,
Krzysztof Silicki, Agnieszka Wrońska

OPIS ZJAWISKA

1 WPROWADZENIE

Obecnie wykorzystywane są w coraz szerszym zakresie usługi internetowe czy mobilne, które angażują w świecie wirtualnym rzeczywiste pieniądze. Według badań firmy Gemius za rok 2011 70% internautów dokonuje zakupów w sieci. Zaś Związek Banków Polskich podaje, iż w pierwszym kwartale 2012 r. liczba klientów aktywnie korzystających z usług bankowości internetowej wyniosła 10,5 mln i rośnie ona w tempie ok. 12% rocznie[1]. Przelewy bankowe, zakupy przez Internet, aukcje elektroniczne są ważnymi usługami online, angażującymi nasz portfel. Niektóre usługi, z pozoru darmowe, także mogą w efekcie okazać się płatnymi. Dlatego ważne jest by coraz lepiej rozumieć, jak bezpiecznie posługiwać się finansami przy korzystaniu z nowoczesnych technologii.

2 Celem dydaktycznym opracowania jest przybliżenie użytkownikowi kwestii zagrożeń dla osobistych finansów przy nieumiejętnym korzystaniu z usług internetowych czy mobilnych. W tej części skoncentrowano się na takich aspektach jak: bezpieczne zakupy przez Internet, bankowość elektroniczna czy aukcje internetowe. W tym kontekście zostało opisanych kilka pojęć, takich jak szyfrowanie czy zjawisko „phishingu", których właściwe zrozumienie odgrywa dużą rolę w rozwijaniu odporności użytkownika na zagrożenia cyberprzestrzeni.

3 Ważne jest by zwrócić uwagę także na takie usługi, które z pozoru nie stanowią zagrożenia dla portfela, ale po uważniejszym przyjrzeniu się im – okazują się zawoalowaną formą wymuszania płatności.

[1] Raport Związku Banków Polskich: *NetB@nk – bankowość Internetowa i płatności bezgotówkowe – podsumowanie – 1 kw. 2012 r.*

BEZPIECZNE ZAKUPY PRZEZ INTERNET

Lista pojęć:
Najważniejsze pojęcia związane z tą kwestią to: zakupy online, bankowość elektroniczna, protokół SSL, sklepy internetowe, bezpieczne przelewy, metody płatności, porównywarki cen, aukcje internetowe, mikropłatności

4 Celem artykułu jest omówienie problematyki zakupów dokonywanych za pośrednictwem Internetu w tym:

- przedstawienie statystyki dotyczącej zjawiska,
- omówienie zagrożeń związanych z zakupami online,
- wskazanie zasad bezpiecznego kupowania w sieci.

5 OPIS ZJAWISKA

Zakupy przez Internet to nie tylko dokonywanie inwestycji finansowych poprzez kupowanie produktów, ale również dokonywanie rezerwacji zakwaterowania, udział w loteriach i zakładach, aukcje internetowe, a także usługi informatyczne, za które bezpośrednio płaci się elektronicznie. W 2010 roku towary lub usługi w Europie zamówiło przez Internet, do użytku prywatnego, 40% osób fizycznych[2]. O wymiarze zjawiska handlu elektronicznego świadczy fakt, że 80% światowych marek posiada katalog produktów online. W Polsce najpopularniejsze sklepy internetowe to m.in.[3]: Euro.com.pl, Zalando.pl, Merlin.pl, Doz.pl, BonPrix.pl, Amazon.

6 Zakupy online stały się ogromnym ułatwieniem dla globalnego konsumenta, jednakże związane są z nimi zagrożenia, które mogą doprowadzić do poniesienia szkody finansowej czy też otrzymania produktu niezgodnego z zamówieniem.

[2] European Commission, Eurostat, Information society statistics.

[3] Megapanel Gemius 11/2012.

Zakupy elektroniczne są też coraz częściej dokonywane przez osoby niepełnoletnie. Młodzi użytkownicy sieci stają się coraz aktywniejszymi konsumentami. 12 proc. użytkowników internetowej porównywarki cen Ceneo.pl to osoby poniżej 18 roku życia[4]. 15 proc. nastolatków posiada konto w serwisie aukcyjnym, poprzez które trzy razy częściej kupuje produkty, niż je sprzedaje. Młodzi klienci najchętniej kupują online gry, telefony komórkowe i ubrania. Dzieci dokonują w Internecie drobnych transakcji. Za to na dużą skalę. Przykładowo, w grach online ukryte jest wiele tzw. mikropłatności. Na zakup gry może wystarczy 20 zł, ale za to jej ciągłe uatrakcyjnianie czy też gadżety potrzebne, by kontynuować grę, mogą kosztować krocie. Towary i usługi są często promowane w sieci za pośrednictwem spamu, który może zachęcać internautów, szczególnie dzieci i młodzież, do dokonania wpłat finansowych.

7 ROZPOZNANIE PROBLEMU OBJAWY

Dokonując zakupów online bez zachowania szczególnej ostrożności, można narazić się na poważne konsekwencje finansowe. Podstawowym problemem związanym z zakupami przez Internet jest niewystarczające sprawdzenie sprzedającego, brak pełnego i jasnego opisu przedmiotu bądź usługi, która ma się stać celem zakupu oraz korzystanie z zakupów przez witryny internetowe niezapewniające bezpiecznego wykonania przelewu. Ponadto co czwarte dziecko przyznało, że korzysta z kont albo kart kredytowych rodziców bez ich wiedzy, a jedynie 17% rodziców deklaruje, że wie o internetowych zakupach swoich dzieci[5]. Temat bezpieczeństwa podczas zakupów internetowych oraz zagadnienia związane z właściwym dbaniem o bezpieczeństwo dziecka podczas kupowania mu sprzętu elektronicznego były tematem kampanii edukacyjnej „Zakup kontrolowany" realizowanej jesienią 2012 roku przez Polskie Centrum Programu Safer Internet tworzone przez NASK i Fundację Dzieci Niczyje[6].

DIAGNOZA – narzędzia, metody

Podstawowe oznaki świadczące o nieprawidłowościach związanych z zakupami przez Internet:

Płatność okazuje się większa niż zakładano/informował sprzedawca (odbiorca mógł paść ofiarą fałszywej promocji – cena towaru obniżona przy np. równocześnie zawyżonej cenie dostawy);

Odbiorca nie otrzymał zamówionego towaru bądź dostał go w innym stanie niż zakładał;

Ktoś włamał się na konto bankowe kupujcego, bądź użytkownik odnotował podejrzane obciążenia na karcie kredytowej (dodatkowe informacje w części poświęconej phisingowi, bankowości elektronicznej i szyfrowaniu).

[4] Raport *Młodzi kupują w sieci*, Ceneo.pl, 2011.

[5] Raport *Online Family 2011*, Horton 2011.

[6] http://saferinternet.pl/zakup_kontrolowany/o_akcji.html

DOBRE PRAKTYKI

ĆWICZENIA 20

9 DOBRE PRAKTYKI

Zalecenia, których warto przestrzegać:

- Nauczyć dzieci rozsądnego dokonywania zakupów i kontroluj ich wydatki.
- Zawsze sprawdzać opinie o sprzedawcy.
- Pamiętać, iż sklep internetowy musi zrealizować zamówienie w terminie 30 dni, chyba że strony ustaliły inaczej. Od umowy takiej konsument może odstąpić w ciągu 10 dni od otrzymania towaru lub rozpoczęcia świadczenia usługi, bez obowiązku podawania przyczyny.
- Sprawdzać regulamin i zasady zwrotów konkretnych towarów.
- Upewnić się, czy transmisja danych odbywa się w bezpiecznym połączeniu (protokół SSL). W przeglądarce na początku adresu witryny powinno pojawić się „https" zamiast „http".
- Sprawdzać wybór różnych metod płatności.
- Czytać dokładnie ofertę wystawców na serwisach aukcyjnych i ogłoszeniowych.
- Po zakończonej transakcji warto napisać swój komentarz, pozytywne opinie lub ostrzeżenia będą cenne dla innych kupujących.
- Kiedy realizacja usługi przebiega niezgodnie z warunkami umowy – złożyć reklamację. Jeśli nie przyniesie ona skutku, należy skontaktować się z instytucją chroniącą konsumentów. Ich lista dostępna jest na stronie www.uokik.gov.pl. Ze standardami prawnymi w Unii Europejskiej w zakresie ochrony konsumentów można zapoznać się na stronie Europejskiego Centrum Konsumenckiego[7].

[7] www.konsument.gov.pl

ROZUMIENIE SZYFROWANIA

Kluczowe pojęcia:
Szyfrowanie, certyfikat cyfrowy, podpis elektroniczny (cyfrowy)

DEFINICJA:
Szyfrowanie[8] to pojęcie znane z matematyki czy pracy wywiadów, które określa takie przetworzenie danych porcji informacji, aby były one trudne lub niemożliwe do odczytania dla postronnych, niepowołanych osób. W komunikacji elektronicznej szyfrowanie ma ogromne znaczenie przy przesyłaniu wartościowych informacji, których nikt inny oprócz nadawcy i odbiorcy nie powinien móc odczytać ani ich zmienić. Warto poznać przykłady stosowania szyfrowania, zalecenia w jakich przypadkach należy posłużyć się szyfrowaniem oraz jak w praktyce stosować te mechanizmy przy zawieraniu transakcji przez Internet lub sieć komórkową. Mechanizmy szyfrowania, w połączeniu z metodami identyfikacji komunikujących się stron (certyfikaty cyfrowe[9], loginy, hasła) tworzą kompletny sposób bezpiecznej komunikacji, która pozwala

[8] Szyfrowanie – metody zabezpieczania komunikacji pomiędzy użytkownikami lub użytkownika z serwisem internetowym lub mobilnym poprzez bezpieczne zakodowanie przesyłanych treści (takich jak: hasła, dane osobowe, numery rachunków, kwoty, umowy), aby nie mogły być odczytane przez osoby postronne (np. cyberprzestepców). Szyfrowanie w komunikacji www stosuje się w połączeniu z cyfrowymi certyfikatami, które pozwalają komputerowi czy smartfonowi użytkownika rozpoznać, czy łączy się z właściwym serwerem (np. serwerem usługi bankowości elektronicznej naszego banku). Bezpieczne, szyfrowane połączenie objawia się np. poprzez pojawienie się ikonki zamkniętej kłódeczki w przeglądarce.

[9] Certyfikaty cyfrowe – jest to rodzaj elektronicznej pieczątki wystawianej przez zaufane urzędy certyfikatów, potwierdzającej, że dany serwis jest tym, za kogo się podaje. Jeśli certyfikaty się nie zgadzają, np. chcesz połączyć się z serwisem aukcyjnym i dokonać zakupu a pojawi się okienko, w którym dowiesz się, że twoja przeglądarka wykryje, że pieczątka jest nieważna albo należy do kogoś zupełnie innego – czym prędzej się rozłącz.

zachować poufność informacji, pewność, że nikt jej po drodze nie zmieni na inną oraz że strony, które sobie coś przesyłają, są tymi, za które się podają.

11 **OPIS ZJAWISKA**

W komunikacji internetowej wszystko, co jest wysyłane może być w łatwy sposób dostępne dla innych. Pisząc do kogoś e-mail warto by użytkownicy zdawali sobie sprawę, że jego treść w łatwy sposób może być dostępna dla innych użytkowników niż adresat wiadomości – np. cyberprzestepców. To tak jakby napisać kartkę pocztową i wrzucić na stertę innych kartek, które przewożone w otwartych ciężarówkach docierałyby do adresatów. Po drodze, w zasadzie każdy, kto zada sobie trochę trudu, może taką korespondencję przeczytać.

12 Czy to może być groźne dla finansów? Zależy to od informacji, które są przesyłane. Jeśli są to życzenia świąteczne, to oczywiście nie, ale jeśli ktoś przesyła pocztą elektroniczną numery i PIN-y kart kredytowych – to o kłopot nie trudno. Użytkownicy rzadko wysyłają takie treści e-mailem, więc skala problemu nie musi być duża. Warto jednak zastanawiać się, co jest wysyłane, mając świadomość, że może to zostać odczytane przez niepowołane osoby. Istnieją bowiem metody szyfrowania korespondencji, więc jeśli e-mailem jest wysyłane coś ważnego, powinno się tę treść zaszyfrować.

13 Zupełnie jednak inna skala zjawiska występuje przy robieniu przez Internet zakupów czy korzystaniu z bankowości elektronicznej. Przykładowo liczba internautów korzystających z usług bankowości internetowej w Polsce jest obecnie na poziomie ponad 10 mln i rośnie w tempie 12% rocznie. Gdyby więc korzystanie z takich usług nie było zabezpieczone, cyberprzestępcy szybko i na dużą skalę staliby się właścicielami pieniędzy i zakupionych przez internautów towarów. Stałoby się tak dlatego, że bez stosowania takich mechanizmów jak szyfrowanie, mogliby łatwo przechwycić wrażliwe informacje takie jak: numer konta, login do konta w banku, hasło, stan konta itp. Mogliby też łatwo dokonać „w czyimś imieniu" operacji, których dana osoba nie chciała (np. przelać pieniądze na swoje konto). Podobnie bowiem, jak w wypadku poczty elektronicznej, jeśli nie stosuje się szyfrowania, operacje w Internecie mogą być widoczne praktycznie dla każdego. To tak jakby wywiesić nazwę użytkownika i hasło do np. serwisu Allegro – na szybie w oknie swojego domu.

14 **CO TO WŁAŚCIWIE JEST TO SZYFROWANIE I GDZIE W PRAKTYCE MOŻNA SIĘ Z NIM ZETKNĄĆ?**

15 Poprzez **szyfrowanie** określa się metody zabezpieczania komunikacji pomiędzy użytkownikami lub użytkownika z serwisem internetowym lub mobilnym poprzez bezpieczne zakodowanie przesyłanych treści (takich jak: hasła, dane osobowe, numery rachunków, kwoty, umowy), aby nie mogły być odczytane przez osoby postronne (np. cyberprzestepców). Szyfrowanie w komunikacji WWW (czyli w czasie używania przeglądarki internetowej) stosuje się w połączeniu z cyfrowymi certyfikatami, które pozwalają komputerowi czy smartfonowi użytkownika rozpoznać, czy łączy się z właściwym serwerem (np. serwerem usługi bankowości elektronicznej naszego banku). Bezpieczne, szyfrowane połączenie objawia się np. poprzez pojawienie się ikonki zamkniętej kłódeczki w przeglądarce.

16 Powyżej zostało przywołane pojęcie certyfikatu cyfrowego, czy też inaczej zwanego elektronicznym, warto poznać także to pojęcie. **Certyfikat cyfrowy** jest to nic innego jak rodzaj elektronicznej pieczęt-

OPIS ZJAWISKA

DOBRE PRAKTYKI

ROZPOZNANIE OBJAWY

ĆWICZENIA 21

DIAGNOZA

ki wystawianej przez tzw. zaufane urzędy certyfikatów, potwierdzające, że dany serwis internetowy jest tym, za kogo się podaje. Jeśli certyfikaty się nie zgadzają, np. chce połączyć się z serwisem aukcyjnym i dokonać zakupu, a pojawi się okienko, w którym użytkownik dowie się, że jego przeglądarka wykryła, iż pieczątka jest nieważna albo należy do kogoś zupełnie innego – czym prędzej należy się rozłączyć.

17 **ROZPOZNANIE PROBLEMU OBJAWY**

Osoby, które nie mają świadomości stosowania mechanizmów ochronnych (szyfrowania) mogły być w przeszłości ofiarami nadużyć ze strony cyberprzestępców. Mogły stracić pieniądze w transakcjach elektronicznych, ich numery kart kredytowych mogły zostać wykradzione i w konsekwencji na ich rachunkach bankowych mogły pojawić się straty. Warto rozmawiać z tymi osobami, czy zdarzyły im się przypadki niewyjaśnionych strat finansowych związanych z kartami debetowymi, kredytowymi lub korzystaniem z Internetu.

18 Może te osoby otrzymują mnóstwo niezamówionej korespondencji (pocztą elektroniczną i zwykłą) i zastanawiają się, skąd ktoś znał ich imię, nazwisko, adres zamieszkania i inne dane osobowe? Całkiem możliwe, że użytkownicy sami kiedyś podali te dane na stronach internetowych, które nie dbają o ochronę zbieranych danych, bo nie stosują szyfrowania. Na przykład jakiś czas temu dokonano przeglądu stron internetowych przeznaczonych dla osób poszukujących pracy i okazało się, że większość z nich nie stosuje certyfikatów i szyfrowania.

19 **DIAGNOZA – narzędzia, metody**

Rozmawiając z osobami, które odważnie dokonują zakupów w Internecie, warto zapytać, czy wiedzą, czym różni się komunikacja bezpieczna od niezabezpieczonej i jak to rozpoznać na ekranie komputera czy smartfona. Należy pamiętać by wypełniając formularze internetowe, w których podaje się swoje poufne dane (np. dane osobowe), zwraca uwagę na zielone kłódeczki pojawiające się w pasku adresowym przeglądarki – świadczące o tym, że dana transmisja jest bezpieczna.

20 **DOBRE PRAKTYKI**

Aby w praktyce poznać stosowanie szyfrowania opartego na certyfikatach cyfrowych, najlepiej przeprowadzić ćwiczenie: Szyfrowanie, dzięki któremu można w praktyce zobaczyć, że konkretne połączenie z witryną jest bezpieczne. Na przykładzie serwisu allegro.pl widać bowiem, że po wejściu na stronę główną w paseczku nawigacyjnym przeglądarki jest po prostu adres allegro.pl – czarną czcionką, ale po przejściu na podstronę *moje allegro,* gdzie podaje się już nazwę użytkownika i hasło, w pasku nawigacyjnym pojawia się zielona kłódeczka świadcząca o tym, że:

nasza przeglądarka rozpoznała serwer Allegro,

certyfikat tego serwera jest ważny,

od tej pory, wszystko co zostanie wpisane z klawiatury i co wyświetli się na naszym ekranie – jest zaszyfrowane, więc nikt, kto nie stoi za plecami korzystającego z komputera i nie zagląda mu przez ramię, nie będzie widział np. co kupuje bądź sprzedaje.

21 Kiedy strefa witryny związana z angażowaniem pieniędzy zostanie opuszczona i użytkownik przejdzie na podstrony informacyjne, zielona kłódeczka najprawdopodobniej zniknie, bo zwykłe surfowanie w Internecie (przeglądanie stron internetowych) najczęściej nie jest szyfrowane.

22 Warto zainteresować się także możliwościami szyfrowania poczty elektronicznej, zwłaszcza jeśli przesyłane bedą wiadomości, których treść ma pozostać znana tylko dla nadawcy i odbiorcy. Jednym z rozwiązań jest standard OpenPGP[10,11], ale także większość programów pocztowych pozwala na stosowanie szyfrowania.

ZJAWISKO PHISHINGU

Lista pojęć: phishing, wyłudzanie, spam, bankowość elektroniczna (internetowa), transakcje online

23 Zjawisko phishingu[12], czyli wyłudzania poufnych danych użytkowników Internetu w celu np. zaatakowania przeprowadzanych przez nich transakcji finansowych online i kradzież środków finansowych staje się coraz większym zagrożeniem dla naszego portfela. W tej części przedstawiono opis zjawiska, skalę zagrożenia, przykłady występowania a także porady, jak się chronić przed zostaniem ofiarą phishingu, jako że zagrożenie to jest skierowane wprost na użytkownika komputera czy smartfona przy wykorzystaniu metod socjotechnicznych – stąd odporność na to zagrożenie jest zależna od stopnia świadomości internauty.

24 **DEFINICJA**

Phishigiem określa się wyłudzanie osobistych informacji od użytkowników sieci (nazwy użytkownika, haseł, PIN-ów, numerów kart kredytowych itp.) poprzez podszywanie się pod znaną użytkownikowi z nazwy instytucję (np. bank, w którym konto) lub osobę, w celu późniejszego wykorzystania tych informacji do nieuprawnionych działań (np. kradzież pieniędzy z bankowego konta).

25 Skala tego zjawiska jest coraz większa, szczególnie wraz z dynamicznym wzrostem wykorzystania bankowości elektronicznej i mobilnej oraz zakupów w sieci.

26 Najbardziej rozpowszechnionym scenariusz phishingu stosowany przez cyberprzestępców jest następujący:

- atakujący wysyła spam, czyli dużą liczbę wiadomości przy pomocy poczty elektronicznej lub portali społecznościowych do wielu internautów, w celu skłonienia ich do odwiedzenia konkretnej strony internetowej lub podania osobistych danych (np. loginu i hasła do serwisu aukcyjnego czy konta bankowego);
- spamer często podszywa się pod znaną instytucję, np. bank, uzasadnia konieczność zweryfikowania danych do konta internetowego np. procedurami bankowymi lub zablokowaniem konta, a link do strony internetowej bardzo przypomina adres http konkretnego banku;
- ofiara, w zależności od treści e-maila, podaje swoje poufne dane lub wchodzi na spreparowaną przez cyberprzestępcę stronę, która do złudzenia przypomina znaną mu witrynę;
- na spreparowanej stronie ofiara loguje się, myśląc, że ma do czynienia z autentyczną witryną swojego banku albo serwisu aukcyjnego i jej dane poufne zostają przechwycone przez intruza;

OPIS ZJAWISKA

[10] http://www.ci.ue.katowice.pl/faq/content/1/11/pl/jak-mog%C4%99-szyfrowa%C4%87-swoj%C4%85-poczt%C4%99-elektroniczn%C4%85-jak-bezpiecznie-przesy%C5%82a%C4%87-poczt%C4%99-bezpieczna-poczta-czyli-pgp-w-kilku-krokach.html

[11] http://www.openpgp.org/

[12] **Phishing** – jest to pojęcie określające „łowienie" użytkowników Internetu i usług mobilnych przez grupy przestępcze (podziemie internetowe), np. poprzez podstawienie fałszywej strony internetowej, przypominającej stronę twojego banku w celu wyłudzenia poufnych danych, takich jak hasła, numery kart kredytowych zainfekowania komputera lub smartfona a następnie dokonywania przez intruza transakcji finansowych bez wiedzy użytkownika (np. przelewów z konta bankowego).

ROZPOZNANIE OBJAWY

DIAGNOZA

- dodatkowo, komputer bądź smatrfon użytkownika zostaje zarażony tzw. złośliwym oprogramowaniem (ang. malware), takim jak wirusy czy konie trojańskie i dołącza do armii komputerów na całym świecie, które są pod kontrolą podziemia internetowego (tzw. botnety);
- od tej pory intruz jest w stanie kontrolować wszystko, co robi na komputerze jego właściciel, jest w stanie dokonywać nieuprawnionych transakcji w sposób niezauważalny dla użytkownika – co jest bezpośrednim zagrożeniem dla portfela internauty.

27 Jak podaje zespół CERT Polska[13], w praktyce zanotowano wiele sposobów działania złośliwego oprogramowania, które może rozpanoszyć się na komputerze bądź smartfonie, po skutecznym ataku phishingowym. W czasie operacji bankowości elektronicznej może więc nastąpić:

podmiana numeru konta docelowego oraz kwoty tuż przed zatwierdzeniem przelewu;

podmiana aktualnego stanu konta;

modyfikacja danych na liście wykonywanych operacji;

żądanie podania kodów jednorazowych w celu aktywacji/sprawdzenia funkcji bezpieczeństwa;

prośba o podanie numeru telefonu oraz wybraniu modelu aparatu (atak ZitMo/2011);

monit proszący o zwrot środków pochodzących z błędnego/podejrzanego przelewu;

monit proszący o wykonanie testowego przelewu w ramach aktywacji/sprawdzenia nowych funkcji bezpieczeństwa.

Wszystkie te „operacje" oraz żądania spowodują z pewnością uszczuplenie zawartości konta w banku osoby zaatakowanej.

28 **ROZPOZNANIE PROBLEMU OBJAWY**

Osoby, które nie mają świadomości występowania zjawiska phishingu, mogły być w przeszłości ofiarami nadużyć ze strony cyberprzestępców. Mogły stracić pieniądze w transakcjach elektronicznych; ich PIN-y, identyfikatory, numery kart kredytowych mogły zostać wykradzione i w konsekwencji na ich rachunkach bankowych mogły pojawić się straty. Warto rozmawiać z tymi osobami, czy zdarzyły im się przypadki niewyjaśnionych strat finansowych związanych z kartami debetowymi, kredytowymi lub korzystaniem z Internetu. Także osoby, które otrzymują dużo niezamówionej korespondencji (spam) są narażone na próby wyłudzenia poufnych informacji rozmaitymi metodami (socjotechnika), które przy braku świadomości zagrożenia wyglądają na ważne wiadomości, polecenia, które należy wykonać.

29 **DIAGNOZA – narzędzia, metody**

Kiedy prowadzi się rozmowy z osobami, które korzystają z bankowości elektronicznej, czy aukcji elektronicznych, należy zapytać, czy jakikolwiek serwis internetowy zażądał od nich przy użyciu poczty elektronicznej bądź serwisu społecznościowego, aby podały swoje poufne informacje, takie jak numer klienta, hasło, PIN. Należy ustalić, czy zdarzyło im się paść ofiarą oszustów i stracili pieniądze bądź ponieśli jakieś inne straty.

30 Należy podkreślić, czy te osoby wiedzą, czym różni się komunika-

[13] (http://www.cert.pl/news/6142

cja bezpieczna od niezabezpieczonej i jak to rozpoznać na ekranie komputera czy smartfona. Warto również ustalić, czy podając swoje identyfikatory i hasła (np. przy sprawdzaniu stanu swojego konta przez Internet) zwracają uwagę na zielone kłódeczki w pasku adresowym przeglądarki?

31 Należy zweryfikować, czy otrzymują dużo spamu i czy zdarza im się dostawać prośby o kliknięcie na adres, który jest w treści wiadomości e-mail. Czy klikają i przenoszą się na strony internetowe, które są im sugerowane? Jeśli tak, jest bardzo duże prawdopodobieństwo, że komputery tych osób już są zarażone.

32 Standardowe pytanie dotyczy także korzystania przez użytkowników z programów antywirusowych i świadomości włączania zapór osobistych w komputerach. Jeśli nie stosują systemów antywirusowych i nie mają włączonych zapór (ang. firewall) jest prawie pewne, że ich komputery są zarażone i nie powinno się z nich wykonywać jakichkolwiek transakcji związanych z finansami.

33 **DOBRE PRAKTYKI**

Aby bronić się przed zagrożeniem phishingu, należy pamiętać o kilku zasadach:

- serwisy internetowe, a już na pewno banki, nie wysyłają do swoich klientów wiadomości pocztą elektroniczną ani poprzez serwisy społecznościowe z prośbą o zalogowanie się i podanie nazw użytkowników, haseł czy innych poufnych informacji;
- nie należy klikać w linki przysłane pocztą elektroniczną ani w załączniki – jeśli nie ma się pewności, kto i w jakim celu przysłał wiadomość, szczególnie, jeśli jej nie była oczekiwana. Jest to obecnie najbardziej rozpowszechniony sposób zarażania komputerów ofiar wirusami, koniami trojańskimi, oprogramowaniem szpiegującym;
- banki, serwisy aukcyjne, sklepy internetowe używają bezpiecznych połączeń wykorzystujących certyfikaty cyfrowe i szyfrowanie, także jeśli zwraca się uwagę, czy w trakcie komunikacji – np. z bankiem – w pasku adresowym przeglądarki pojawia się zielona kłódeczka, po kliknięciu na którą otworzy się okienko potwierdzające, że mamy do czynienia z tą witryną, z którą chcieliśmy się połączyć – nie grozi użytkownikowi, że ulegniemy atakowi phishingowemu;
- każdy bank prowadzący usługę bankowości elektronicznej ma na swojej stronie porady dla swoich użytkowników, jak bezpiecznie korzystać z usług online, np.: http://www.pekao.com.pl/indywidualni/bankowosc_elektroniczna/Bezpieczenstwo
- oprócz powyższych zasad, należy stosować aktualne oprogramowanie na swoim komputerze (w szczególności aktualną wersję przeglądarki), bowiem metody ataków stale się zmieniają, a producenci oprogramowania starają się za tym nadążać i publikują nowsze wersje (np. przeglądarek), które bronią się przed znanymi atakami;
- warto też pamiętać, że danych poufnych nie należy nigdy podawać w treści wiadomości wysyłanych pocztą elektroniczną, bo łatwo mogą wpaść w ręce osób niepowołanych.

BANKOWOŚĆ ELEKTRONICZNA

34 **Lista pojęć**

Bankowość elektroniczna, bankowość internetowa, telefoniczna, terminalowa, phishing, pharming, skimming, vishing

35 **DEFINICJE**

Nowoczesne technologie są obecne w każdej dziedzinie życia. Zostały wykorzystane również do potrzeb bankowości. **Bankowość elektroniczna (ang. e-banking) jest**

ĆWICZENIA 22

DOBRE PRAKTYKI

OPIS ZJAWISKA

ROZPOZNANIE OBJAWY

formą usług oferowanych przez banki, która polega na umożliwieniu klientowi banku dostępu do jego rachunku za pomocą urządzenia elektronicznego (np. komputera, bankomatu, terminalu POS, telefonu) i łącza telekomunikacyjnego (np. linii telefonicznej). Istnieje wiele korzyści płynących z bankowości elektronicznej. Są nimi wygodna komunikacja i dostępność wirtualnych usług bankowych przez 24 godziny na dobę 7 dni w tygodniu z dowolnego miejsca bez konieczności fizycznej obecności w placówce banku; duży zakres produktów i usług; niższe koszty przeprowadzanych operacji oraz możliwość sprawowania bieżącej kontroli nad własnym rachunkiem, sprawdzenia salda; dokonywanie transakcji bezgotówkowych, co daje poczucie bezpieczeństwa i jest formą nadzoru sytuacji finansowej. Istnieją różne formy bankowości elektronicznej. Są nimi bankowość internetowa, telefoniczna oraz terminalowa.

36 **Bankowość internetowa**

Bankowość internetowa to komunikacja z bankiem za pośrednictwem Internetu (przeglądarki internetowej) poprzez witrynę internetową banku umożliwiającą dokonywanie online różnorodnych operacji lub za pomocą oprogramowania dedykowanego do komunikacji z bankiem. Najważniejszą cechą bankowości internetowej jest wirtualna obsługa klienta, tj. włączenie klienta jako fizycznego użytkownika do skomputeryzowanego systemu bankowego.

37 **Bankowość telefoniczna**

Phone banking i mobile banking to usługi bankowe dostępne za pośrednictwem telefonu (bankowość telefoniczna/phone banking) oraz urządzeń przenośnych, w tym telefonów komórkowych (bankowości mobilna /mobile banking). Operacje bankowe mogą być realizowane na kilka sposobów: poprzez kontakt z operatorem (call center) lub automatyczny serwis telefoniczny IVR oraz przy użyciu telefonu komórkowego za pomocą SMS lub technologii WAP.

38 **Bankowość terminalowa**

Polega na dokonywaniu transakcji bankowych z wykorzystaniem urządzeń elektronicznych tj. bankomatów i terminali do akceptowania kart płatniczych (POS). Jest to najczęściej wykorzystywana forma bankowości elektronicznej, realizowana poprzez karty płatnicze. Ze względu na sposób rozliczenia transakcji karty można podzielić na debetowe, kredytowe oraz obciążeniowe.

39 **ROZPOZNANIE PROBLEMU OBJAWY**

Warunkiem bezpiecznego wykonywania transakcji bankowych drogą elektroniczną jest świadomość występowania zagrożeń i stosowanie zasad bezpieczeństwa. Zagrożenia można w różny sposób skatalogować. Mogą wynikać z nieodpowiedniego lub błędnego działania systemu, niskich kompetencji lub nieostrożności osób korzystających z tej formy bankowości, mogą być związane z nielegalną działalnością, w tym z wykorzystywaniem szkodliwego oprogramowania. Zagrożenia bezpieczeństwa danych w systemach informatycznych związane są z ich przetwarzaniem i przechowywaniem. **Można je podzielić na następujące grupy** [14]:

- **zagrożenia wspólne dla klienta i serwera,**
- **zagrożenia serwera,**
- **zagrożenia klienta.**

40 Pierwszy typ zagrożeń, **czyli zagrożenia wspólne dla serwera i klienta, wiąże się z procesem przesyłania danych**. Do typowych zagrożeń

[14] P. Laskowski, *Bezpieczeństwo elektronicznych operacji bankowych*, „Scientific Bulletin of Chełm Section of Mathematics and Computer Science", 1/2008 za: *Bankowość elektroniczna*, red. A. Gospodarowicz, Warszawa 2005.

tego rodzaju zalicza się m.in.:

- snifing – podsłuchiwanie sieci umożliwiające poznanie treści przekazu;
- spoofing – polegający na podszywaniu się pod inny komputer należący do danej sieci, przy przejęciu dzięki temu sesji użytkownika wraz z maszyną;
- network snooping – różne metody szpiegowania, np. badanie parametrów sieci, ze szczególnym uwzględnieniem rozpoznania słabości stosowanych zabezpieczeń;
- ataki man-in-the-middle – polegające na monitorowaniu połączenia przez niepowołaną osobę pośredniczącą w transmisji danych pomiędzy klientem i serwerem;
- różne przejawy komputerowego sabotażu i cyberterroryzmu.

41 Do zagrożeń serwera, prowadzących do przejęcia lub też zniszczenia jego zasobów, zalicza się:

- ataki z użyciem szeregu szkodliwych programów (ang. malware) ingerujących w systemy informatyczne. Programy wykorzystywane do ataków są określane w literaturze różnymi pojęciami, przypominającymi zagrożenia ze świata rzeczywistego:
  - wirusy,
  - tzw. bakterie powielające się ustawicznie w celu zablokowania systemu,
  - robaki komputerowe przenoszące się na system w sieci i pozostawiające po sobie bakterie i wirusy,
  - konie trojańskie będące programami naruszającymi bezpieczeństwo systemu poprzez np. wykradanie haseł, udające przeprowadzenie w tym samym czasie bezpiecznych operacji lub otwierające tajne furtki dla atakujących system komputerowy,
  - bomby logiczne, czyli ukryte fragmenty programów uruchamianych w ustalonym czasie lub po zajściu określonego zdarzenia,
- nieautoryzowany dostęp do systemu poprzez tzw. furtki, czyli wejścia pozwalające omijać zabezpieczenia, ataki na zasoby baz danych, a także sabotaż i cyberterroryzm, np. przy użyciu bomb elektromagnetycznych niszczących zasoby baz danych;
- błędy i przeoczenia obsługujących system, zagrożenia losowe i środowiskowe, błędne funkcjonowanie serwera oraz działania nieuczciwych pracowników.

42 **Na zagrożenia związane z klientem składają się problemy związane z logowaniem i pracą w systemie.** Do głównych zagrożeń z tej grupy należy:

- kompromitacja zabezpieczeń dostępu do systemu, czyli ujawnienie loginu, hasła, hasła jednorazowego, jak również kodu PIN do tokena;
- phishing (łowienie haseł), czyli wyłudzanie poufnych informacji osobistych (np. haseł lub szczegółów dot. karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne (więcej nt. phishingu w części: „Zjawisko phisingu") – manipulowanie systemem i sprzętem, pozwalające na dokonanie zmian niewidocznych dla użytkowników;
- zbyt słabe zabezpieczenia pełnego dostępu do rachunku, np. tylko na podstawie identyfkatora;
- błędy w standardowych oprogramowaniach, jak również błędne zastosowanie technologii np. Active X, czyli programów wczytywanych z Internetu i uruchamianych na komputerze użytkownika, zapewniających niepowołany dostęp do wszystkich zasobów komputera, łącznie z zawartością dysku.

Czym jest phishing, pharming, skimming, vishing ?

Phishing – metoda podstępnego uzyskiwania haseł dostępu do internetowych kont bankowych użytkownika za pośrednictwem np. e-maili, w tym wyłudzanie poufnych informacji osobistych (np. haseł lub szczegółów dot. karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję.

Pharming – bardziej niebezpieczna dla użytkownika oraz trudniejsza do wykrycia forma phishingu. Charakterystyczne dla pharmingu jest to, że nawet po wpisaniu prawidłowego adresu strony www, ofiara zostanie przekierowana na fałszywą (choć mogącą wyglądać tak samo) stronę www. Ma to na celu przejęcie wpisywanych przez użytkownika do zaufanych witryn haseł, numerów kart kredytowych i innych poufnych danych.

Skimming – nielegalne kopiowanie zawartości paska magnetycznego karty bankowej bez wiedzy jej posiadacza, w celu wykonywania nieuprawnionych transakcji.

Vishing – metoda oszustwa, mająca swoje podstawy w phisingu i metodach socjotechnicznych, polegająca na tym, że oszuści wykorzystując telefonię internetową podszywają się pod instytucje finansowe.

ĆWICZENIA 23

DIAGNOZA

43 DIAGNOZA

Jednym z problemów bankowości elektronicznej są systemy bezpieczeństwa. Obecnie stosowane rozwiązania techniczne zapewniają niezbędny poziom bezpieczeństwa, jednak konieczna jest ciągła praca nad doskonaleniem zabezpieczeń systemów i coraz większa świadomość użytkowników.

DOBRE PRAKTYKI

44

Cztery główne metody zapewniające bezpieczeństwo to:

szyfrowana transmisja danych – realizowana za pośrednictwem protokołu SSL,

proste uwierzytelnianie – (identyfikator, hasło, PIN),

silne uwierzytelnianie – (np. token, certyfikat użytkownika, klucz prywatny),

podpis elektroniczny.

Oferując usługi bankowości elektronicznej, bank musi przestrzegać jednej z podstawowych zasad bankowości: obowiązku zapewnienia bezpieczeństwa środków pieniężnych gromadzonych na rachunkach bankowych jego klientów. Obsługa operacji dokonywanych przez Internet podlega przepisom wynikającym z ustawy o elektronicznych instrumentach płatniczych. Obowiązkiem banku jest m.in. „zapewnienia posiadaczowi bezpieczeństwa dokonywania operacji, z zachowaniem należytej staranności oraz przy wykorzystaniu właściwych rozwiązań technicznych”[15]. Korzystając z usług bankowości elektronicznej należy jednak pamiętać, że zapewnienie bezpieczeństwa jest procesem ciągłym, i że w dużym stopniu zależy od wiedzy i umiejętności użytkowników. Mogą oni w znacznym stopniu ograniczyć wpływ różnego rodzaju zagrożeń pochodzących z sieci Internet, zachowując ostrożność i rozwagę w działaniu, a także aktualizując swoje przeglądarki internetowe oraz stosując zabezpieczenia sprzętowe i programowe (więcej nt. zabezpieczeń w dziale Komputer).

45 DOBRE PRAKTYKI

Korzystając z bankowości elektronicznej, warto pamiętać o podstawowych zasadach bezpieczeństwa.

[15] Art. 31 ust. 1 Ustawy o elektronicznych instrumentach płatniczych.

Zalecenia – jak postępować i czego unikać?

- używać własnego komputera podczas korzystania z usług bankowości elektronicznej (np. nie korzystać z komputerów w kafejkach internetowych do tego celu);
- dbać o bezpieczeństwo własnego komputera, korzystając z legalnego oprogramowania oraz stosując konieczne aktualizacje, w tym aktualizowany na bieżąco program antywirusowy;
- nie udostępniać osobom trzecim numeru klienta, haseł, karty kodów jednorazowych itp. (także nie przesyłać takich danych e-mailem), nie podawać tego typu danych na stronach internetowych, które nie stosują szyfrowania i certyfikatu cyfrowego;
- nie odpowiadać na e-maile z prośbą o ujawnienie czy zweryfikowanie danych osobowych, informacji dotyczących numeru konta czy karty kredytowej. Bank nigdy nie wysyła e-maili z prośbą o podanie takich danych. W wypadku otrzymania takiego e-maila należy od razu skontaktować się z bankiem;
- nie zapisywać haseł ani numerów PIN, tylko je zapamiętać;
- regularnie monitorować rachunek bankowy, wyciągi bankowe;
- upewnić się, czy połączenie jest szyfrowane (czy adres strony w oknie przeglądarki rozpoczyna się od https://, bo zwykłej zaczyna się od http://) oraz czy na pasku u dołu lub u góry ekranu pojawia się ikona z zamkniętą kłódką;
- wylogowywać się po zakończeniu działań na rachunku;
- ręcznie wpisywać adres strony banku i/lub stworzyć do niego zakładkę w przeglądarce, nie korzystać z „podpowiadaczy" i linków.

AUKCJE INTERNETOWE - SUPER PROMOCJE - FAŁSZYWE STRONY

Lista pojęć: sklep internetowy, aukcja internetowa, oszustwa internetowe, SMS premium, szyfrowana transakcja, spam, fałszywe strony, phishing, „słup"

OPIS ZJAWISKA

46 OPIS ZJAWISKA

Jedną z głównych zalet zakupów online jest bardzo szybka i łatwa możliwość znalezienia produktów lub usług po niższych cenach niż w tradycyjnych sklepach. Oszuści dobrze o tym wiedzą i doskonale odnajdują się w wirtualnym handlu, wykorzystując chęć użytkowników do znalezienia dobrej okazji w Internecie. Do tego celu wykorzystują spreparowane sklepy internetowe np. z elektroniką, czy markową odzieżą, które wyglądają zupełnie legalnie lub wykorzystują do tego aukcje internetowe, np. na Allegro, kusząc klientów okazjonalną ofertą cenową. W rzeczywistości sprzedawane są na nich towary podrobione, niezgodne z rzeczywistością lub co gorsza po zapłacie nie są wcale dostarczane do kupującego. Oszuści kuszą łatwymi pieniędzmi, które rzekomo dana osoba wygrała w loterii a „jedynym" warunkiem odebrania pieniędzy jest wypełnienie wniosku i wniesienie opłaty.

47 Innym bardzo niebezpiecznym w skutkach prawnych dla użytkownika zjawiskiem jest podejmowanie kuszących ofert pracy, często z możliwością wykonywania jej w domu za stosunkowo dużą stawkę. Użytkownik otrzymuje wiadomość e-mail od zagranicznej firmy poszukującej agentów finansowych w jego kraju. Jest to kusząca oferta łatwej pracy, którą można wykonywać w domu i pozwalającej zarobić kilka razy więcej niż średnia krajowa, w obcej walucie (dolary, euro), gdy poświęca się na to 3–4 godziny dziennie. Jeśli ofiara się zgodzi, zostaje poproszona o dane swojego konta bankowego. W rzeczywistości użytkownik jest wykorzy-

DIAGNOZA

ROZPOZNANIE OBJAWY

ĆWICZENIA 24

stywany w ramach procederu kradzieży pieniędzy z kont bankowych osób, których dane zostały wcześniej skradzione przez cyberprzestępców (np. wykorzystujących techniki phishingu). Pieniądze są przelewane bezpośrednio na konto użytkownika-ofiary, którego zadaniem jest z kolei przesłanie sumy, która wpłynęła na jego konto dalej za pośrednictwem firm umożliwiających szybkie przekazywanie gotówki np: Western Union. Ofiara w tym momencie staje się tzw. „słupem", a w policyjnym śledztwie w sprawie kradzieży uznawana jest za współsprawcę kradzieży pieniędzy.

48 Oszuści kuszą często łatwymi pieniędzmi, które rzekomo zostały wygrane np. w loterii, a jedynym warunkiem odebrania pieniędzy jest wypełnienie wniosku i wniesienie opłaty przelewem lub za pomocą bardzo popularnych krótkich wiadomości SMS zwanych SMS Premium. Numery te wykorzystywane są w wielu konkursach i teleturniejach, jak również przy opłacie np. za bilety komunikacji miejskiej. Niestety, często podana informacja o koszcie SMS jest nieprawdziwa. Zdarzają się również sytuacje, w których opłata za wiadomość jest pobierana, chociaż system informuje o braku możliwości realizacji usługi z przyczyn technicznych. W wielu przypadkach o poniesionych kosztach możemy dowiedzieć się dopiero z chwilą otrzymania rachunku za telefon, gdyż usługodawca celowo ukrył informację o prawdziwej cenie wysłania wiadomości.

49 **ROZPOZNANIE PROBLEMU OBJAWY**

Oszustwa internetowe istniały niemal od początku Internetu. Każdego roku cyberprzestępcy wymyślają nowe techniki i taktyki mające na celu oszukanie użytkowników. Rozpoznanie problemu zależy tylko od czujności użytkownika. Gdy ona zawiedzie, skutkiem jest najczęściej strata finansowa.

50 Dlatego też ważne jest by omawiać czy, użytkownik miał do czynienia z ofertami pozornie łatwego zarobku, jak opisany powyżej proceder „słupów" internetowych lub też czy słyszał, bądź był ofiarą jakichś oszustw przy zakupach internetowych (fałszywy sklep, niedostarczone towary itp.). Należy zweryfikować czy i jak korzysta z okazji, które otrzymuje np. pocztą elektroniczną (najczęściej w postaci spamu).

51 **DIAGNOZA**

Należy kierować się zdrowym rozsądkiem. To najlepszy sojusznik w obronie przed wyłudzeniami. Nikt nie rozdaje niczego za darmo!

Zawsze należy zapoznać się z regulaminem zamieszczanym przez sprzedającego oraz uważnie sprawdzać wszelkiego rodzaju ukryte koszty. W przypadku SMS Premium możesz zawsze sprawdzić koszt esemesa w Internecie w rejestrze numerów wykorzystywanych przez dostawców usług o podwyższonej opłacie.

Starać się zawsze sprawdzić wiarygodność Sprzedającego lub np. Pracodawcy. W Internecie często można znaleźć informacje od innych użytkowników np. na forach internetowych.

52 Rozmawiając z osobą dokonującą zakupów w sieci warto się zorientować, czy i ile spamu dostaje na swoją skrzynkę poczty elektronicznej. Jeśli otrzymuje dużo spamu (liczba niezamówionych ofert otrzymywanych w ciągu doby jest większa od ilości zwykłej korespondencji, lub jest mniejsza, ale stanowi więcej niż 10% otrzymywanych listów elektronicznych) to należy zbadać, czy ten użytkownik używa programu antywirusowego i czy ten program jest na bieżąco aktualizowany. Istnieje bowiem ścisły związek między ilością spamu a poziomem zagrożenia,

że padnie się ofiarą jakiegoś mniej lub bardziej wymyślnego oszustwa.

53 Pomocne mogą być pytania: Skąd użytkownik zyskuje pewność, że sklep jest godny zaufania? Czy sprawdza, czy istnieje stacjonarny telefon kontaktowy, na który można zadzwonić? Czy zwraca uwagę na bezpieczne połączenie z serwerem w czasie transakcji (czy certyfikat strony internetowej sklepu należy do tego podmiotu, który zajmuje się sprzedażą?). Czy stosuje się do wszystkich lub wybranych zasad podanych w części DOBRE PRAKTYKI?

54 **DOBRE PRAKTYKI**

Aby chronić się przed oszustwami w sieci, należy przestrzegać kilku podstawowych zasad:

1. Jeśli cena wydaje się zbyt atrakcyjna, należy podchodzić do transakcji bardziej podejrzliwie.

2. Warto zadzwonić na numer obsługi Klienta, jeśli nie ma żadnego numeru kontaktowego, to powinno wzbudzić podejrzliwość uytkownika.

3. W przypadku usług „krypto płatnych" np.: SMS Premium lub infolinii premium, należy sprawdzić czy podawany koszt jest rzeczywisty. Informacji o kosztach można szukać na stronach UOKIK, KRRiT, oraz UKE.

4. Należy sprawdzić, czy sklep internetowy posiada szyfrowanie treści w procesie zakupu (por. część „Rozumienie szyfrowania" oraz „Bezpieczne zakupy przez Internet").

5. W przypadku płatności kartą kredytową, pierwszym warunkiem koniecznym jest szyfrowana transakcja w sklepie (punkt 3).

6. Warto sprawdzić komentarze wystawiane przez innych kupujących. Wyszukać nazwę sklepu internetowego, właściciela sklepu, sprawdzić, czy ktoś inny nie opublikował żadnych skarg na daną stronę internetową lub aukcję.

7. Należy zwracać uwagę na poprawność gramatyczną treści korespondencji od sprzedającego. Często przestępcy instalując fałszywe strony czy aukcje nie mówią w języku polskim, a wszelkiego rodzaju korespondencja e-mail jest tłumaczona za pośrednictwem słowników internetowych.

8. Istotne, by zwrócić uwagę z jakiej domeny przychodzi korespondencja od sprzedającego. Czy jest taka sama jak strony internetowej (np. strona: www.twojsklep.pl i e-mail: biuro@twojsklep.pl).

9. Jeśli pojawiają się wątpliwości przy stwierdzeniu, czy dana oferta jest wiarygodna czy nie, lepiej z niej nie korzystać.

10. Jeśli padnie się ofiarą oszustwa internetowego, należy zgłosić sprawę na policję. Ponadto, jeżeli ofiara korzystała z karty kredytowej, bezzwłocznie powinna ją zablokować w banku.

DOBRE PRAKTYKI

BIBLIOGRAFIA:

Gospodarowicz A., *Bankowość elektroniczna*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2004.

E-mail i ataki phishingowe, „OUCH!", Biuletyn bezpieczeństwa komputerowego SANS Institute i CERT Polska, 2/2013 (http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_po.pdf).

Laskowski P., *Bezpieczeństwo elektronicznych operacji bankowych*, „Scientific Bulletin of Chełm Section of Mathematics and Computer Science", 1/2008.

Schneier B.: *Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C*, Wydawnictwa Naukowo -Techniczne, Warszawa 2002.

Bankowość internetowa – nowe zagrożenia, artykuł z http://www.chip.pl/artykuly/porady.

Szwajkowska G., Kwaśniewski P., Leżoń K., Woźniczka F., *Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia*, Urząd Komisji Nadzoru Finansowego, Warszawa 2010.

ZAGROŻENIA
DLA KOMPUTERA I INNEGO SPRZĘTU

Marcin Bochenek, Piotr Bisialski,
Martyna Różycka, Anna Rywczyńska,
Krzysztof Silicki, Agnieszka Wrońska

OPIS ZJAWISKA

WPROWADZENIE

1 W przeszłości komputerom zagrażały głównie wirusy i robaki. Chociaż podstawowym celem tych programów tworzonych przez hakerów było rozprzestrzenianie się, a tylko niektóre z nich były tworzone z myślą o uszkodzeniu plików i komputerów, określane były one jako „cyberwandalizm". Obecnie największym zagrożeniem dla komputerów jest oprogramowanie typu crimeware. Są to szkodliwe programy tworzone przez cyberprzestępców po to, aby w nielegalny sposób zarobić pieniądze. Crimeware może przybierać postać wirusów, robaków, trojanów, skryptów lub innych szkodliwych programów, rozpowszechnianych różnymi kanałami jak poczta elektroniczna, przenośne pamięci, czy też zainfekowane strony www. Jednocześnie należy pamiętać, że zagrożenia te odnoszą się dzisiaj do wszystkich zaawansowanych urządzeń, z których korzystamy na co dzień jak tablety, smartfony, konsole do gier czy też telewizory.

2 Celem dydaktycznym artukułu jest zobrazowanie użytkownikom zagrożeń związanych z codziennym korzystaniem z komputera i innych urządzeń mobilnych. W tej części publikacji skoncentrowano się na zagrożeniach związanych z codzienną pracą, m.in.: korzystaniem z poczty elektronicznej, zewnętrznych przenośnych pamięci danych, jak również opisaniem skutków wynikających z infekcji. W kolejnych punktach opisane zostały podstawowe środki ochrony, które w znaczący sposób mogą zmniejszyć ryzyko zarówno utraty danych jak i strat finansowych.

ZŁOŚLIWE OPROGRAMOWANIE/SPAM

Lista pojęć

Złośliwe oprogramowanie (malware), spam

Celem tej czści artykułu jest omówienie

3 zagrożeń związanych z korzystaniem z poczty elektronicznej i poznanie m.in.:

- w jaki sposób e-mail przyczynia się do propagacji złośliwego oprogramowania,
- czym jest spam i jak go uniknąć

OPIS ZJAWISKA

4 E-mail na przełomie wieku XX i XXI stał się jedną z najbardziej rozpowszechnionych form komunikacji zarówno w życiu osobistym, jak i zawodowym. Do podstawowych zagrożeń związanych z korzystaniem z usług poczty e-mail należą: spam, złośliwe oprogramowanie i phishing (który bliżej został omówiony w artykule poprzednim). Każde z tych zagrożeń występuje na masową skalę, narażając użytkowników na potencjalne niebezpieczeństwo oraz powodując ogólną utratę zaufania do korzystania z poczty elektronicznej.

SPAM

5 Spam to w skrócie wiadomość e-mailowa z niechcianą reklamą wysłaną do tysięcy, a czasem nawet do wielu milionów adresatów. Według raportu Symanteca **szacuje się, że w 2011 roku rozsyłanych było około 42 miliardów wiadomości dziennie, co oznacza że około 70% wiadomości jest spamem**. Badając wpływ wiadomości SPAM na użytkowników, przy założeniu, iż jedna wiadomość spamowa na 1000 jest czytana i wywiera wpływ/przynosi skutek, biorąc pod uwagę liczbę wiadomości wysyłanych każdego dnia na świecie, widoczne jest, że efekt jest ogromny i daje wymierne korzyści finansowe hakerom. Treść, jaką głównie wypełnione są wiadomości spam, to reklamy/informacje: farmaceutyczne, randki/sex, biżuteria/zegarki, kasyna/gry/zakłady bukmacherskie, środki dietetyczne, promocje i super okazje. Szacuje się, że aż 87% złośliwego opro-

ZŁOŚLIWE OPROGRAMOWANIE

gramowania trafia na nasze komputery drogą e-mailową. Praktycznie każdy rodzaj złośliwego oprogramowania, jak wirusy, robaki czy konie trojańskie, rozpowszechniany jest dzisiaj drogą e-mailową. Do infekcji komputera może dojść za pomocą załączników w poczcie e-mail, które po otwarciu mogą próbować uszkodzić system operacyjny, wykraść dane, przejąć kontrolę nad komputerem lub śledzić wpisywane przez użytkowników teksty. W ten sposób hakerzy mogą uzyskać dostęp do prywatnych danych i haseł np: logowania do banku, poczty czy serwisów społecznościowych. Złośliwe oprogramowanie nie zawsze musi być załącznikiem do e-maila. Równie często spotyka się preparowane wiadomości, w których umieszczone są linki prowadzące do stron zawierających złośliwy skrypt, które bez wiedzy użytkownika mogą zainstalować się na komputerze. Wiadomości te tworzone są tak, aby użytkownik zainteresował się i uwierzył w ich treść, a następnie kliknął w link/baner, który przeniesie go do szczegółów zamieszczonych na stronie WWW.

ROZPOZNANIE PROBLEMU

OBJAWY

6

Wiadomości ze spamem często można rozpoznać już po nadawcy oraz temacie, takim jak np.: **Twoje zgłoszenie** albo **Gratulacje, wygrałeś!**. System antyspamowy zainstalowany w komputerze może znaczącą większość tych wiadomości automatycznie oznaczać jako niechciane i przenieść do folderu SPAM. W wypadku zarażenia złośliwym oprogramowaniem powinno ono zostać wykryte przez system antywirusowy. Jednak najlepiej jest dbać o to, aby nie odczytywać wiadomości nieznanego pochodzenia oraz nie wchodzić na strony internetowe, co do których legalności i wiarygodności nie jest się pewnym. Należy również pamiętać, aby nie instalować na komputerze zbędnego oprogramowania. Jeśli użytkownik nie jest pewien, do czego służy dany program, nie powinien go instalować. Kupując lub pobierając programy, należy korzystać tylko ze sprawdzonych, bezpiecznych źródeł. Korzystanie z programów pirackich jest nie tylko łamaniem prawa, ale także niesie ze sobą ryzyko zarażenia systemu komputerowego złośliwym oprogramowaniem.

DIAGNOZA

7

W celu ograniczenia ryzyka infekcji należy korzystać przede wszystkim program antywirusowy wraz z filtrem antyspamowym. Niestety ich posiadanie nie daje nam gwarancji, że cała poczta zostanie wyfiltrowana, a otrzymane wiadomości w skrzynce nie będą spamem, wiadomościami typu phishing czy też nie będą zawierały złośliwego oprogramowania w załącznikach. Niezbędnym elementem jest również

Najlepszym sposobem, aby zapobiec zagrożeniom propagującym się za pomocą poczty e-mail jest zwolnić na chwilę, pomyśleć i sprawdzić, czy chce się odczytać wiadomość, obejrzeć załącznik, odpowiedzieć na niego lub kliknąć na przesłany w wiadomości link WWW.

8 dbanie o regularną aktualizację wszystkich zainstalowanych na komputerze programów oraz systemu antywirusowego.

DOBRE PRAKTYKI

9 Przy czytaniu poczty bardzo ważny jest zdrowy rozsądek i racjonalna doza podejrzliwości. Przede wszystkim nie należy otwierać załączników w e-mailach docierających od nieznanych nadawców, opatrzonych dość ogólnym tytułem. Należy również zastanowić się zawsze przed kliknięciem w zamieszczone w wiadomościach lub Internecie odsyłacze (linki).

OPIS ZJAWISKA

Warto również zwrócić uwagę na rozszerzenia plików w załączniku. Najniebezpieczniejsze, często zawierające złośliwe oprogramowanie, są pliki tzw. wykonywalne, które instalują się na komputerach często bez wiedzy i pozwolenia użytkownika, np: .exe, .bat, .vbs, .scr, .lnk.

Aby zidentyfikować zagrożenie, warto 10 odpowiedzieć na kilka prostych pytań, które pomogą każdemu użytkownikowi w rozpoznaniu niebezpiecznych wiadomości e-mail:

Czy znacz nadawcę wiadomości?

Czy otrzymałeś już inne wiadomości od tego nadawcy?

Czy spodziewałeś się otrzymać tę wiadomość?

Czy tytuł wiadomości, nazwa załącznika oraz treść wiadomości mają sens?

Czy wiadomość nie zawiera złośliwego oprogramowania – a więc jaki jest wynik skanowania antywirusowego?

ROZPOZNANIE OBJAWY

DYSKI ZEWNĘTRZNE USB

Lista pojęć

Pendrive, szyfrowanie danych, firewall, antywirus

11 Celem tej części jest omówienie zagrożeń związanych z korzystaniem z zewnętrznych dysków i pamięci przenośnych:

- w jaki sposób e-mail przyczynia się do propagacji złośliwego oprogramowania,
- czym jest spam i jak go uniknąć.

ĆWICZENIA 26

12 **OPIS ZJAWISKA**

Dane to często najcenniejsza rzecz, jaka jest gromadzona w komputerach. W razie kradzieży, sprzęt można szybko odtworzyć, danych najczęściej już nie, warto więc zadbać o bezpieczeństwo danych. Dzisiaj aktywność szkodliwego oprogramowania propagującego się za pomocą popularnych nośników pamięci jak: pendrive'y, karty pamięci, zewnętrzne dyski twarde jest powszechnym problemem. Dodatkowo w dobie powszechnej mobilności urządzeń: laptopy, netbooki, smartfony często zsynchronizowane są ze sobą, przechowywane są wrażliwe dane podobnie jak numery kart kredytowych, ważną korespondencję czy urzędowe dokumenty – bez żadnego zabezpieczenia. Niestety odpowiedniego bezpieczeństwa nie zapewni im ani program antywirusowy, ani firewall. Właściwą ochroną jest **szyfrowanie danych,** zastosowanie odpowiednich narzędzi zabezpieczających gwarantujące, że szyfru nie da się praktycznie złamać a dane nie zostaną odczytane przez osoby trzecie, które zdobyły np. nielegalnie dostęp do określonego sprzętu.

13 **ROZPOZNANIE PROBLEMU/ OBJAWY**

Zainfekowana pamięć po podpięciu do komputera natychmiast infekuje dyski twarde. Szkodliwy kod jest automatycznie uruchamiany i kopiuje pliki z pamięci na dysk twardy, instalując również inne złośliwe programy. Posiadając zainstalowany i zaktualizowany system antywirusowy, są duże szanse, że wykryje on złośliwe oprogramowanie i uniemożliwi jego propagację na komputerze. W celu ochrony danych przed osobami trzecimi, należy zadbać o odpowiednie ich zaszyfrowanie. Na rynku dostępnych jest szereg programów szyfrujących, w tym również darmowych, które pozwolą użytkownikom na zabezpieczenie kluczowych dla nich danych. Należy również

pamiętać, że jeśli hasło do rozszyfrowania zostanie utracone, to razem z nim stracone zostaną też i dane.

Nasze dane będą bezpieczne dopiero wtedy, kiedy zaszyfrujemy je tak, aby nikt oprócz nas nie mógł z nich skorzystać.

14 **DIAGNOZA**

Należy zwróć uwagę na podłączane do komputera urządzenia przenośne, w szczególności pendrive'y lub dyski USB. Mogą one bardzo łatwo przenosić wirusy – wystarczy, że były wcześniej podłączone do zainfekowanego komputera. Aby sprawdzić, czy podłączane do naszego komputera dyski zewnętrzne nie są zainfekowane, należy wykonać pełne ich skanowanie zaktualizowanym programem antywirusowym i upewnić się, że system firewall na naszym komputerze jest włączony. Jeśli program antywirusowy wykryje jakiekolwiek zainfekowane pliki, należy postępować zgodnie z zaleceniami generowanymi przez program antywirusowy. W celu ochrony wrażliwych danych należy zidentyfikować je i wykorzystać do ich szyfrowania odpowiednie programy szyfrujące, jednocześnie pamiętając o skonstruowaniu bezpiecznego silnego hasła.

15 **DOBRE PRAKTYKI**

Zalecenia:

Należy zainstalować program antywirusowy z aktualnymi sygnaturami wirusów.

Warto skanować programem antywirusowym wszystkie zewnętrzne nośniki danych podłączane do komputera. (Nie wolno podłączać pamięci USB nieznanego pochodzenia do komputera).

Dobrze jest zidentyfikować ważne dane i zadbać o odpowiednie ich zaszyfrowanie, pamiętając również o sporządzaniu cyklicznie kopii zapasowych.

BOTNETY

Lista pojęć

Botnet, złośliwe oprogramowanie, spam, firewall, antywirus

16 Celem tego fragmentu jest omówienie zagrożenia związanego z nieumiejętnym korzystaniem z Internetu i poznaniem m.in., czym jest botnet oraz jakie zagrożenia wynikają z przynależności do niego.

17 **OPIS ZJAWISKA**

Botnety to sieci komputerów zainfekowane szkodliwym oprogramowaniem. Komputery należące do takich sieci nazywane są komputerami zombie i pozostają do całkowitej dyspozycji właściciela botnetu. Pierwsze botnety zostały stworzone w latach 90. Największe grupy komputerów zombie składają się z kilkuset tysięcy do ponad miliona jednostek (botów), a skala zagrożenia dotyczy znacznej część (25%-40%) komputerów używanych w gospodarstwach domowych. Komputer staje się częścią botnetu w momencie zainfekowania szkodliwym oprogramowaniem zmieniającym go w tzw. „boty", które są trudne do wykrycia, a tym samym szczególnie niebezpieczne. Haker ma często dostęp do wszystkich zasobów komputera i całkowicie kontroluje zainfekowany sprzęt. Proces infekcji komputera może mieć różny przebieg np.: za pomocą kliknięcia linku otrzymanego pocztą e-mail (por. SPAM). Komputery należące do botnetu mogą być wykorzystywane przez hakerów do prowadzenia nielegalnej działalności przynoszącej im często profity finansowe. Najczęściej sieci botnetowe wykorzystywane są do:

- podejmowania działań o charakterze przestępczym, skierowanych przeciwko innym komputerom i ich użytkownikom,
- rozsyłania spamu,

ROZPOZNANIE OBJAWY

DOBRE PRAKTYKI

ĆWICZENIA 26

- szpiegowania danych komputera, na którym zainstalowany jest bot,
- paraliżowania serwerów i witryn internetowych w wyniku powtarzających się zapytań wysyłanych ze wszystkich komputerów botnetu.

18 ROZPOZNANIE PROBLEMU /OBJAWY

Nawet jeśli nieświadomi użytkownicy oceniają zagrożenie infekcją i podłączeniem do botnetu swojego komputera jako znikome, to jednak należy mieć świadomość konsekwencji wynikających z kontrolowania komputera przez niepowołane osoby postronne. Należy zdawać sobie sprawę, że oprogramowanie zainstalowane na komputerach może w każdej chwili zostać zaktualizowane przez hakerów i wyposażone w nowe funkcje i możliwości, jeśli zleceniodawca uzna taką operację za opłacalną i wskazaną. Przykłady tego, co może spowodować osoba zarządzająca siecią botnetową to:

Zablokowanie twardego dysku i urządzeń zewnętrznych (myszy, klawiatury, etc.) i umożliwienie dostępu do nich dopiero po dokonaniu wpłaty określonej kwoty.

Wykradanie danych dostępowych do e-banku, poczty elektronicznej, portali społecznościowych i innych usług, z których korzystamy za pośrednictwem Internetu.

Dokonywanie w imieniu użytkownika nielegalnych pobrań na jego komputer.

Wykorzystywanie komputera ofiary do przechowywania nielegalnych informacji.

19 DIAGNOZA

W celu ochrony osobistych danych, optymalnej i wydajnej pracy komputera oraz uniknięcia nieświadomego uczestnictwa w działaniach o charakterze przestępczym, należy stosować kilka prostych zasad. Przede wszystkim zacząć od przeprowadzenia kontroli, która wykryje słabe strony (podatności) w systemie – takie systemy dostępne są online w Internecie (np.: Secunia) – a następnie należy włączyć pełne skanowanie komputera programem antywirusowym. Jeżeli urządzenie nie może zostać zabezpieczone przez oprogramowanie antywirusowe lub gdy chcemy się upewnić, że w pełni odzyskamy nad nim kontrolę, należy rozważyć ponownie zainstalowanie systemu operacyjnego lub wykonanie pełnego resetu fabrycznego, zainstalowanie najnowszej wersji antywirusa oraz odzyskiwanie danych z kopii zapasowej (por. część o kopiach zapasowych).

Jeśli coś niepokoi użytkownika, nie powinien działać pochopnie. W wypadku, gdy ma trudności z diagnozowaniem przyczyn, powinien zwrócić się o pomoc do kogoś, kto się na tym zna.

20 DOBRE PRAKTYKI

Zainstalowanie programu antywirusowego i regularne dokonywanie jego aktualizacji.

Nie wyłączanie Firewalla systemowego.

Należy aktualizować programy, takie jak system operacyjny, przeglądarka internetowa, antywirus.

Zachować ostrożność w odniesieniu do wiadomości e-mail (spam).

Jeśli coś wydaje się dziwne – nie należy panikować. Jeśli coś jest niepokojące, nie należy działać pochopnie. Jeśli są trudności z diagnozowaniem przyczyn, należy zwróć się o pomoc do kogoś, kto się na tym zna.

Żadne z opisanych powyżej działań nie stanowi samo w sobie skutecznego zabezpieczenia, ale połączenie wszystkich wymienionych środków bezpieczeństwa znacząco podwyższa bezpieczeństwo danego komputera.

SIECI BEZPRZEWODOWE I INNY SPRZĘT W DOMU, PRACY I SZKOLE

Lista pojęć

Punkt dostępowy, sieć Wi-Fi, SSID, WPA2

21 OPIS ZJAWISKA

Dzisiaj posiadamy szereg urządzeń, które mają możliwość dostępu do Internetu. Oprócz komputera PC i laptopów dostęp do sieci umożliwiają również telefony komórkowe, smartpfony, tablety, konsole do gier, jak również nowoczesne telewizory. Najczęściej dostęp do Internetu w tych urządzeniach realizowany jest za pomocą bezprzewodowych sieci Wi-Fi, technologia ta z uwagi na wygodę użytkowania stała się dzisiaj standardem. Sieć Wi-Fi sprawia, że użytkownicy nie muszą zawracać sobie głowy wierceniem dziur i przeciąganiem kabli przez ściany. Wadą jednak sieci bezprzewodowych jest możliwość występowania problemów z bezpieczeństwem. Sieć bezprzewodowa jest kontrolowana przez tzw. Punkt dostępowy (z ang. WiFi access point). Jest to urządzenie, które obecnie najczęściej występuje jako element w tzw. bezprzewodowym routerze. To on jest odpowiedzialny za podłączanie urządzeń do sieci domowej i umożliwianie im dostępu do Internetu. Dlatego też należy zadbać o odpowiednie zabezpieczenie zarówno samych urządzeń mobilnych, jak również punktów dostępowych sieci.

22 ROZPOZNANIE PROBLEMU OBJAWY

Brak lub nieodpowiednie zabezpieczenie urządzeń mobilnych posiadających dostęp do Internetu naraża użytkownika na wszystkie cyberzagrożenia tak samo jak w przypadku stacjonarnego komputera PC. Jednocześnie w wypadku korzystania z bezprzewodowej sieci Wi-Fi, nieodpowiednie jej zabezpieczenie może skutkować nieautoryzowanym dostępem do sieci dla postronnych osób będących w jej zasięgu. Należy pamiętać również, że każdy właściciel odpowiada prawnie za wszelkie działania w sieci, które realizowane są przez jego punkt dostępowy. Jeśli użytkownik nie zadba o odpowiednią konfigurację zabezpieczeń domowej sieci Wi-Fi, musimy liczyć się z tym, że inne osoby mogą korzystać z jego łącza internetowego, znacząco obniżając jego przepustowość, wykorzystując je np. do ściągania nielegalnych treści lub podsłuchiwać i przechwytywać przesyłane przez niego dane.

23 DIAGNOZA

Najlepszym sposobem na sprawdzenie bezpieczeństwa sieci bezprzewodowej jest przeprowadzenie próby włamania się do niej. Do tego jednak potrzebne są odpowiednie narzędzia i wiedza. W celu odpowiedniego zabezpieczenia domowej bezprzewodowej sieci Wi-Fi należy zastosować kilka podstawowych zasad:

- jednym z pierwszych kroków w celu poprawienia bezpieczeństwa sieci WiFi jest ograniczenie liczby osób oraz sposobów pozwalających uzyskać dostęp do panelu administracyjnego, który pozwala na zmianę konfiguracji sieci. Należy pamiętać o zastosowaniu odpowiednio silnego hasła (por. część „Silne hasła”);
- kolejnym krokiem jest zapewnienie dostępu do sieci bezprzewodowej tylko użytkownikom i ich urządzeniom,

ROZPOZNANIE OBJAWY

OPIS ZJAWISKA

DIAGNOZA

DOBRE PRAKTYKI

ĆWICZENIA 27

ĆWICZENIA 28

które są znane. Bezprzewodowy router należy skonfigurować w taki sposób, aby inne nieuprawnione osoby, które będą odbierały sygnał radiowy sieci, nie były w stanie się podłączyć ani podsłuchiwać ruchu. Obecnie jedną z najpowszechniej zalecanych metod szyfrowania ruchu w sieci bezprzewodowej jest algorytm WPA2. Uruchomienie go wiąże się z zabezpieczeniem dostępu do sieci odpowiednio silnym hasłem;

- należy zadbać o zmianę nazwy sieci bezprzewodowej (SSID), która wyświetla się po wykryciu dostępnych sieci w danym obszarze. Nazwa nie powinna mieć związku ani z fizycznym położeniem (nie powinna zawierać np. nazwiska lub adresu), ani z nazwą producenta routera. Każda dodatkowa informacja jest prezentem dla potencjalnego intruza – po co dawać mu znać, którą sieć lub markę routera powinien brać na celownik?
- należy pamiętać, aby hasło, które będzie wykorzystywane do podłączania sieci (WPA2), było inne niż hasło do panelu administracyjnego punktu dostępowego;
- urządzenia mobilne jak tablety, smartfony, konsole do gier czy nawet telewizory, które są podłączone do sieci zapamiętają hasła dostępu do sieci. Należy jednak co jakiś czas (np. co 3–6 miesięcy) zmieniać hasła dostępowe, szczególnie gdy gościom została udostpniona;
- w momencie, gdy zabezpieczenia punktu dostępowego są już w pełni skonfigurowane, jednym z ostatnich kroków jest ustawienie serwerów DNS, które mają być używane w sieci domowej. DNS to usługa, która jest niezbędna do prawidłowego funkcjonowania sieci Internet. Zalecamy, aby ustawić serwery usługi OpenDNS jako podstawowe (primary DNS) w konfiguracji punktu dostępowego. OpenDNS to darmowa usługa, która zapewnia, że witryny, do których się łączymy są bezpieczne (nie dokonują ataków na użytkownika). Dodatkowo OpenDNS umożliwia administratorowi domowej sieci łatwe zarządzanie listą stron, do których domownicy mają mieć zapewniony dostęp oraz tych, do których dostęp powinien zostać ograniczony (np. filtrowanie treści dostępnych dla najmłodszych użytkowników Internetu).

24 DOBRE PRAKTYKI

Gdy użytkownik próbuje łączyć się z innymi użytkownikami sieci bezprzewodowych z urządzeń mobilnych np. na wakacjach wskazane jest, aby uzyskiwać połączenie tylko z sieciami bezprzewodowymi wymagającymi klucza zabezpieczeń sieciowych lub mającymi inne formy zabezpieczeń, takie jak certyfikat. Przed podłączeniem do sieci Wi-Fi takiej jak sieć publiczna w kawiarence czy na lotnisku, należy dokładnie zapoznać się z oświadczeniem o zasadach zachowania poufności i dowiedzieć się, które pliki, o ile w ogóle jakieś, są zachowywane na komputerze oraz jakie informacje usługodawca pobiera z komputera. Należy pamiętać również, aby przy logowaniu się do poczty, banku lub innego serwisu używać połączenia szyfrowanego (por. ochrona urządzeń mobilnych).

25 W wypadku podłączenia do sieci bez zabezpieczeń należy zachować ostrożność, ponieważ osoba z odpowiednimi narzędziami może zobaczyć wszystkie wykonywane czynności, takie jak odwiedzane witryny sieci Web, używane dokumenty oraz nazwy użytkownika i hasła.

Należy również pamiętać o instalacji programów antywirusowych na wszystkich urządzeniach, na których można je stosować (PC, laptop, tablet, smartfone).

ANTYWIRUS/FIREWALL/FILTR RODZICIELSKI

Lista pojęć

Antywirus, firewall, filtr rodzicielski, wirus, robak, trojan

OPIS ZJAWISKA

26 OPIS ZJAWISKA

Obecnie standardem jest, że komputery i inne urządzenia mobilne jak smartfony czy tablety posiadają stały dostęp do Internetu. Należy zadbać o skuteczną ochronę przed wirusami i programami szpiegującymi, zabezpieczając te urządzenia tak, aby nikt nie mógł przechwycić haseł, które są wpisywane na stronach internetowych ani zdalnie używać cudzego komputera. Wirusy, robaki, konie trojańskie są złośliwym oprogramowaniem (ang: malware) tworzonym przez hakerów, które propaguje się za pośrednictwem Internetu. Inne nośniki, jak np.: przenośne pamięci (pendrivy) zarażają komputery podatne na atak. Wirusy i robaki mogą propagować się automatycznie, przechodząc z komputera na komputer w ramach np. sieci domowej, podczas gdy konie trojańskie dostają się do komputera, ukrywając się wewnątrz pozornie wiarygodnego programu, na przykład wygaszacza ekranu. Złośliwe oprogramowanie tworzone jest w większości przypadków na zamówienie i może mieć różne zastosowanie dające hakerom określone profity.

Innym ważnym aspektem, na który również należy zwracać szczególną uwagę, jest ochrona dzieci, a więc najmłodszych użytkowników komputerów w domu, przez treściami nielegalnymi, wulgarnymi i pornograficznymi dostępnymi w Internecie. Do tego celu służą specjalne programy filtrujące treści dostępne w Internecie.

27 Programy antywirusowe

Oprogramowanie antywirusowe może pomóc chronić komputer przed wirusami, robakami i innymi zagrożeniami bezpieczeństwa. Oprogramowanie antyszpiegowskie zaś może pomóc chronić komputer przed oprogramowaniem szpiegowskim i innymi niechcianymi programami. Ponieważ codziennie pojawiają się nowe wirusy, ważne jest, aby wybrać program antywirusowy z funkcją automatycznej aktualizacji. Podczas aktualizowania oprogramowania antywirusowego nowe wirusy są dodawane do listy wyszukiwanych wirusów, co pomaga chronić komputer przed nowymi atakami. Jeśli lista wirusów jest nieaktualna, komputer jest narażony na nowe zagrożenia. Korzystanie z aktualizacji wymaga zwykle wniesienia rocznej opłaty aktualizacyjnej. Aby otrzymywać regularne aktualizacje, należy zadbać o jej ważność.

28 Firewall

Określany jest jako zapora sieciowa, która chroni komputer przed złośliwym oprogramowaniem i hakerami próbującymi uzyskać dostęp do komputera. Zapora blokuje informacje lub zezwala na ich przesłanie do komputera w zależności od jej ustawień. Każdy system operacyjny Windows posiada wbudowany personalny Firewall, który standardowo jest zawsze uruchomiony.

29 Filtr rodzinny

Wobec niedostatecznej ochrony dziecka przed nieodpowiednimi treściami, szereg firm działa na rzecz podniesienia bezpieczeństwa. Dostępne są moduły kontroli rodzicielskiej. Są to programy lub usługi np. u dostawcy Internetu, chroniące dzieci przed dostępem do materiałów pornograficznych i przemocy w Internecie. Komputer przeznaczony dla dziecka powinien być wyposażony w program filtru-

DIAGNOZA

ROZPOZNANIE OBJAWY

jący, pozwalający na uchronienie dziecka przed kontaktem ze szkodliwymi treściami. Programy kontroli rodzicielskiej dysponują też możliwościami ograniczania aktywności dziecka – takimi jak wypełnianie formularzy online, korzystanie z komunikatorów, mogą również monitorować czas, który dziecko spędza przed komputerem.

30 **ROZPOZNANIE PROBLEMU OBJAWY**

Przykładowymi objawami infekcji złośliwym oprogramowaniem mogą być m.in. utrata informacji z dysku twardego, całkowite uniemożliwienie pracy urządzenia lub znaczące pogorszenie wydajności i stabilności komputera. Innym znacznie gorszym w wykryciu szkodliwym oprogramowaniem są programy śledzące działania użytkownika i wykradające m.in. hasła do kont bankowych i innych serwisów. Przykłady objawów zainfekowania to między innymi:

- komputer zabiera użytkownika na strony internetowe, na które nie chce się udać,
- komputer uruchamia programy, które nigdy nie były zainstalowane,
- oprogramowanie antywirusowe zgłasza zainfekowane pliki,
- aktualizacje antywirusa i systemy kończą się niepowodzeniem,
- komputer znacząco wolniej pracuje i się zawiesza.

Internet zawiera zarówno treści wartościowe, jak i szkodliwe dla dziecka. Gdy dziecko szuka np. serwisów z dziecięcymi grami komputerowymi online, może się zdarzyć, iż wpisując nazwę portalu zrobi literówkę i wówczas trafi na stronę zawierającą nieodpowiednie dla niego materiały. Na takie strony dziecko może trafić, wybierając nieodpowiedni link znajdujący się w wynikach przeglądarki czy klikając na link umieszczony na forum lub przesłany na skrzynkę pocztową czy znajdujący się w komunikatorze.

31 **DIAGNOZA**

Aby sprawdzić, czy komputer nie jest zainfekowany, należy wykonać pełne skanowanie zaktualizowanym programem antywirusowym i upewnić się, że system firewall na komputerze jest włączony. Jeśli program antywirusowy wykryje jakiekolwiek zainfekowane pliki, należy wykonać zalecane kroki. Można uruchomić dodatkowe skanowanie zabezpieczeń przez skanery online dostępne w Internecie. Jeżeli urządzenie nie może zostać zabezpieczone przez oprogramowanie lub gdy chcemy się upewnić, że w pełni należy odzyskać nad nim kontrolę, należy rozważyć ponowne zainstalowanie systemu operacyjnego lub wykonanie pełnego resetu fabrycznego, zainstalowanie najnowszej wersji antywirusa oraz odzyskiwanie danych z kopii zapasowej (por. fragment o kopiach zapasowych).

„Im wcześniej użytkownik zorientuje się, że padł ofiarą ataku, tym szybciej będzie mógł zareagować i zminimalizować szkody".

32 Z raportu badań „EU Kids Online" wynika, że ponad połowa rodziców w UE obawia się kontaktu dziecka z treściami pornograficznymi, związanymi z przemocą, uwodzeniem dziecka przez nieznajomych w sieci. Jednocześnie z badań wynika, że jedynie połowa rodziców w Polsce zainstalowała na domowym komputerze program filtrujący lub monitorujący aktywność dziecka w sieci. Podstawowym elementem do sprawdzenia aktywności dziecka w sieci, jeżeli nie mamy jeszcze filtru rodzinnego, jest przejrzenie historii odwiedzanych stron dostępnych w przeglądarkach internetowych. Ważne jest również dbanie o odpowiednią konfigurację komputera. Nawet jeśli komputer ma służyć wyłącznie dziecku, należy zastanowić się, kto będzie posiadał uprawnienia administracyjne, pozwalające m.in. na instalowanie nowego oprogramowania lub zmianę kluczowych ustawień bezpieczeństwa. W wy-

padku najmłodszych użytkowników zaleca się, by takie uprawnienia posiadała osoba dorosła, a dziecko miało tylko wydzielony profil z ograniczonymi prawami.

33 **DOBRE PRAKTYKI**

Należy pamiętać o:

1. Zainstalowaniu programu antywirusowego i pamiętaniu o jego cyklicznym aktualizowaniu.
2. Regularnym aktualizowaniu Windows i innych programów zainstalowanych na komputerze.
3. Nie podłączaniu pamięci USB, płyt CD, DVD nieznanego pochodzenia.
4. Nie otwieraniu wiadomości e-mail nieznanego pochodzenia.
5. Nie „klikaniu" w linki www, które wyglądają podejrzanie.
6. Nie instalowaniu oprogramowania nieznanego pochodzenia.
7. Nie wyłączaniu Firewalla systemowego.
8. Ochronie dzieci przed treściami nielegalnymi i pornograficznymi przez instalację oprogramowania filtrującego treści w Internecie lub zakup usługi u operatora.

Żadne z opisanych powyżej działań nie stanowi samo w sobie skutecznego zabezpieczenia, ale połączenie wszystkich wymienionych środków bezpieczeństwa znacząco podwyższa bezpieczeństwo twojego komputera.

AKTUALIZACJE

Ze względu na dużą dynamikę pojawiania się nowych zagrożeń bezpieczeństwa w cyberprzestrzeni oprogramowanie komputerów, smartfonów, tabletów i innych urządzeń korzystających z sieci, powinno być systematycznie aktualizowane.

34 Poniżej przedstawiono opis zjawiska występowania luk bezpieczeństwa w powszechnie używanym oprogramowaniu i zagrożeń, jakie mogą być efektem wykorzystania tych luk przez cyberprzestępców czy też hakerów lub terrorystów. Zostanie wyjaśnione, dlaczego przeprowadzanie aktualizacji oprogramowania systemowego i aplikacji jest jednym z kluczowych elementów obrony przez cyberzagrożeniami, a także w jaki sposób takie aktualizacje są przeprowadzane oraz jaką rolę w tym procesie pełni właściciel komputera, tabletu, czy smartfona.

35 **OPIS ZJAWISKA**

Aktualizacjami czy inaczej: uaktualnieniami oprogramowania nazywamy każdą czynność wymiany części tego oprogramowania na nowszą wersję, poprawioną lub wyposażoną w nowe funkcjonalności. Ze względu na tematykę cyberzagrożeń interesujące są aktualizacje bezpieczeństwa, czyli takie czynności wymiany oprogramowania, które likwidują pewne luki bezpieczeństwa ujawnione przez organizacje czy firmy zajmujące się tematyką zabezpieczeń.

36 We współczesnym świecie technologii komputerowych aktualizacje systemów operacyjnych (takich jak Windows, Android, Linux, IOS) czy konkretnych aplikacji, takich jak przeglądarki internetowe (Internet Explorer, Firefox, Chrome, Opera) następują w sposób automatyczny, czy raczej półautomatyczny – zwykle za wiedzą i zgodą właściciela telefonu, tabletu, smartfona, konsoli do gier. Dzieje się tak, kiedy dane urządzenie jest podłączone do Internetu. Na ekranie komputera, laptopa czy telefonu pojawia się komunikat, że dostępna jest nowa wersja oprogramowania – czasem towarzyszy temu informacja, że jest to ważne uaktualnienie ze względu na zachowanie bezpieczeństwa. Wystarczy zaakceptować instalację i system operacyjny bądź dana aplikacja (np. Acrobat Reader) au-

DOBRE PRAKTYKI

ĆWICZENIA 29

OPIS ZJAWISKA

ROZPOZNANIE OBJAWY

tomatycznie dokonuje uaktualnienia wersji oprogramowania. Zwykle towarzyszy temu komunikat, iż po instalacji należy zrestartować urządzenie, żeby nowa wersja mogła poprawnie pracować.

37 Jeśli by nie dokonano aktualizacji, bądź nie pozwalałoby się aby producenci oprogramowania zdalnie je wykonywali, bardzo szybko komputery i inne urządzenia mające kontakt z Internetem stałyby się łatwym łupem cyberprzestepców. Stosują oni bowiem metody skanowania przestrzeni Internetu w poszukiwaniu źle zabezpieczonych komputerów, a następnie zarażają te komputery złośliwym oprogramowaniem, które potrafi wykorzystać wszystkie znalezione w urządzeniu luki bezpieczeństwa. Wtedy nasz komputer, tablet, smartfon czy nawet konsola do gier podłączona do sieci, tak naprawdę pracuje na rzecz kogoś innego (podziemia internetowego) i bez wiedzy właściciela może rozsyłać spam, może być częścią botnetu atakującego rządowe witryny, a dodatkowo wszystkie informacje, które są na komputerze użytkownika lub zostały wpisane w przeglądarce (np. dane poufne) padają łupem intruzów.

38 Dosyć ważne są także aktualizacje systemów antywirusowych i innych systemów bezpieczeństwa (zapora – firewall, antymalware). Skuteczność tych systemów wręcz opiera się na ich aktualności. Systemy antywirusowe zawierają bazy znanych wirusów i szkodliwego oprogramowania, która jest aktualizowana przez ich twórców codziennie a nawet (w sytuacji podwyższonego zagrożenia) – kilka razy na dzień. Jeśli więc np. skończy się licencja programu albo z jakichś względów bazy wirusów nie są aktualizowane przez kilka dni – bezpieczeństwo (w szczególności przy transakcjach online, w których dysponujemy własnym portfelem) jest po prostu niskie.

ĆWICZENIA 30

39 Należy więc dbać o to, by wersje systemów operacyjnych, aplikacji, systemów zabezpieczeń były zawsze najaktualniejsze. Ale skąd można wiedzieć, czy programy, których codziennie używamy są uaktualnione i nie zawierają znanych luk czy błędów? Najlepiej zapoznać się i przeprowadzić
Ćwiczenie: Czy jesteś aktualny?

40 **ROZPOZNANIE PROBLEMU OBJAWY**

Osoby, które używają starszych, nieaktualnych wersji systemów operacyjnych czy aplikacji zwykle mają problemy z prawidłowym działaniem swoich urządzeń. Ich komputery PC, laptopy, tablety czy smartfony działają wolno, często się zawieszają lub towarzyszą temu jakieś nieoczekiwane efekty (pauzy w działaniu czy dziwne komunikaty na ekranie – np. o błędach).

41 Może to być oczywiście spowodowane awarią urządzenia, ale częściej mamy do czynienia z zawirusowaniem czy też ogólniej zakażeniem komputera szkodliwym oprogramowaniem.

UWAGA: Coraz częściej zawirusowane urządzenie samo informuje użytkownika o tym, że jest problem z bezpieczeństwem i poprzez wyskakujące komunikaty „namawia" do kupienia jakiegoś cudownego oprogramowania (np. antywirusowego), które wyleczy komputer. To także są próby oszustwa. Nigdy nie powinno się ulegać takim sugestiom, nie należy ściągć i kupować programów z niesprawdzonych źródeł – zamiast wybawić z opresji, jeszcze bardziej zakażą system.

42 Zdarza się także, że zawirusowany komputer pada łupem szantażystów, którzy straszą użytkownika poprzez wyskakujące okienka, że jeśli nie prześle określonej sumy (zwykle w dolarach) na wskazane konto, to dane na dysku zosta-

ną zniszczone. Wtedy także nie powinno się płacić, należy wezwać znanego dobrego fachowca-komputerowca, bo każdy niewłaściwy ruch może spowodować pogorszenie sytuacji (uszkodzenie danych).

43 **DIAGNOZA**

Ta część poświcona jest zagadnieniom, jak być „aktualnym". Aby sprawdzić, czy nasze oprogramowanie jest rzeczywiście aktualne, należy przeprowadzić analizę – taką jak w Ćwiczeniu: Czy jesteś aktualny?
Następnie, jeśli się okaże, że z jakiegoś powodu system operacyjny czy któraś z używanych aplikacji mają zablokowaną możliwość przeprowadzania aktualizacji – należy to odblokować.

Jeśli zostaną zauważone takie objawy, jak opisane w punkcie 30., jak najszybciej należy uruchomić oprogramowanie antywirusowe. Wcześniej dobrze jest sprawdzić, czy jest ono aktualne i czy ma aktualną bazę wzorców wirusów (patrz Ćwiczenie: Czy jesteś aktualny?)

Jeśli się to nie udaje – należy zasięgnąć porady specjalisty od komputerów.

44 **DOBRE PRAKTYKI**

Zanim źle działające urządzenie zostanie zaniesione do naprawy, warto sprawdzić, czy użytkowane oprogramowanie jest aktualne – a jeśli nie – natychmiast sprawdzić, dlaczego tak jest (samemu, lub z pomocą specjalisty) oraz uruchomić **aktualny** program antywirusowy.

45 Oprócz tego warto też sprawdzić inne ustawienia komputera czy tabletu, które chronią ich bezpieczeństwo, takie jak np. zapora (włączona czy wyłączona?).

KOPIE ZAPASOWE

Wykonywanie kopii zapasowych jest koniecznością ze względu na awaryjność sprzętu i oprogramowania, a także ze względu na zagrożenie ataków niszczących ze strony cyberprzestępców bądź innych osób dokonujących nadużyć w cyberprzestrzeni.

46 W dziale przedstawiono, czym są kopie bezpieczeństwa, dlaczego i jak je tworzyć, a także w jaki sposób korzystać z utworzonych wcześniej kopii, jeśli dojdzie do zniszczenia danych na dysku bądź na karcie pamięci.

47 **OPIS ZJAWISKA**

Dane znajdujące się na dysku komputera lub w pamięci smartfona czy tabletu mogą zostać całkowicie zniszczone lub utracone z powodu kradzieży, awarii sprzętu, oprogramowania bądź w związku z atakiem cyberprzestępców. W tym ostatnim przypadku, często się zdarza szantaż: jeśli użytkownik nie zapłaci, zniszczone zostaną dane na dysku. Nie wchodząc w tym miejscu w powody utraty danych, można zauważyć dwie rzeczy:

- istnieją wyspecjalizowane firmy, które w wielu przypadkach potrafią odzyskać stracone dane – zwykle takie usługi sporo kosztują,
- o wiele rozsądniej jest zawczasu przygotować kopie bezpieczeństwa naszych danych (tzw. backup), aby w sytuacji awaryjnej móc po nie sięgnąć.

48 Kopią bezpieczeństwa nazywamy zestaw naszych danych przeniesiony na nośnik poza urządzeniem, na którym się one normalnie znajdują, w postaci takiej, że jest możliwe ich odczytanie, szczególnie w sytuacji, kiedy podstawowe urządzenie ulegnie awarii bądź kradzieży. Istnieją generalnie dwa podejścia do tworzenia kopii bezpieczeństwa:

DIAGNOZA

- archiwizowanie jedynie tych danych, które uważamy za ważne (których nie sposób inaczej odtworzyć), takich jak dokumenty, zdjęcia, filmy;
- archiwizowanie całej zawartości dysków czy pamięci urządzeń (łącznie z systemem operacyjnym i aplikacjami), co przyśpiesza powrót do normalnego działania przy całkowitej awarii np. dysku twardego.

49 Na komputerach z systemami Windows, Linux czy MAC OS istnieją narzędzia tworzenia kopii, np. w Windows 7 jest to Microsoft Backup and Restore. Wtedy wystarczy zaplanować częstotliwość tworzenia kopii zapasowych i miejsce, gdzie będą one automatycznie tworzone.

DOBRE PRAKTYKI

50 Ale nawet jak użytkownik nie ma do dyspozycji żadnego programu do tworzenia kopii, w ostateczności może po prostu przekopiować ważną zawartość dysku (np. określony katalog) na zewnętrzny nośnik (np. płytę CD, zewnętrzny dysk, pamięć USB). Oczywiście będzie miał na głowie pamiętanie o kolejnych kopiach, dane bowiem szybko się dezaktualizują i kopia, którą wykonał pół roku temu nie zabezpiecza go przed utratą wszystkich ważnych danych.

51 Wykonane kopie należy czytelnie oznaczyć, a także co pewien czas (nawet jeśli nic się nie zdarzyło z danymi podstawowymi) skopiowane dane należy spróbować odtworzyć. Zdarza się bowiem, że użytkownik sądził, iż kopie wykonały się prawidłowo, a jak przychodzi co do czego, okazuje się, że nie dają się odtworzyć.

ROZPOZNANIE OBJAWY

52 **ROZPOZNANIE PROBLEMU OBJAWY**

Niestosowanie kopii zapasowych ujawnia się boleśnie, kiedy następuje kradzież lub awaria tabletu, laptopa czy smartfona lub gdy staniemy się przedmiotem cyberataku, który zniszczy nasze dane. Zdarza się, że w tym ostatnim wypadku jest to sposób na

ĆWICZENIA 31

53 zacieranie śladów przez intruzów.

DIAGNOZA

Użytkownicy zwykle nie stosują kopii bezpieczeństwa z braku świadomości, braku czasu lub umiejętności.

54 Jednak większości użytkowników zdarzyła się, lub zdarzy się w przyszłości, jakaś utrata danych np. w wyniku awarii. Dla diagnozy, z jaką sytuacją mamy do czynienia wystarczy zadanie dwóch pytań:

1) co się stanie lub co uczyni użytkownik w wypadku awarii dysku bądź innego urządzenia napełnionego jego danymi?
2) czy zdarzył się już taki wypadek w przeszłości?

55 **DOBRE PRAKTYKI**

Istnieje kilka podstawowych zasad przy

- należy starać się by proces tworzenia kopii zapasowych jak najbardziej automatyzować, aby wykonywały się niejako same, aby nie trzeba było o tym pamiętać;
- ważne jest właściwe ustalenie częstotliwości tworzenia kopii w zależności od tempa zmian danych (co tydzień, co miesiąc a może codziennie);
- należy unikać tworzenia kopii na tym samym urządzeniu – raczej poszukaje się metody tworzenia kopii na nośnikach, które można przechowywać oddzielnie (można nawet zamknąć je w podręcznym sejfie albo wywieźć do innej lokalizacji);
- coraz częściej spotykamy się z usługą „backupu w chmurze" co oznacza, że dane będą składowane „gdzieś w Internecie". Warto w takich przypadkach dokładnie zapoznać się z regulaminem takiej usługi (np. czy dane są szyfrowane?) i odpowiedzialnością za utratę danych;
- regularnie należy sprawdzać, czy udaje się odtworzyć dane z kopii zapasowej, aby była pewność, że będzie

można skorzystać z kopii bezpieczeństwa w kryzysowej sytuacji,
- jeśli kopiowany jest cały dysk, łącznie z systemem operacyjnym i aplikacjami, to warto mieć świadomość, że po odtworzeniu komputer cofnął się o ileś dni, tak więc w tym czasie mogły się pojawić jakieś ważne aktualizacje bezpieczeństwa, należy je niezwłocznie doinstalować;
- dla szczególnie ważnych danych warto wykonać więcej niż jedną kopię bezpieczeństwa – najlepiej na różnych nośnikach;
- generalnie, pracując nad wszelkimi dokumentami należy cyklicznie zapamiętywać treść, aby w wypadku awarii czy cyberataku nie stracić aktualnej wersji dokumentu.

tworzeniu kopii bezpieczeństwa:

SILNE HASŁA

Hasła to podstawa bezpieczeństwa korzystania z komputera czy rozmaitych serwisów internetowych (społecznościowych, aukcyjnych, bankowości elektronicznej). Wiedza, jakich haseł używać, aby rzeczywiście były wystarczająco silne oraz jak to zrobić, żeby sprawiało to nam jak najmniej trudności, jest bardzo przydatna w obronie przed rozmaitymi zagrożeniami cyberprzestrzeni. W niniejszym rozdziale przedstawiono, jakie hasła można traktować jako wystarczająco silne, jak je tworzyć, jak zapamiętać, jak chronić, aby nie wpadły w niepowołane ręce a także podano szereg zaleceń co do stosowania haseł przy korzystaniu z wielu serwisów online, które wymagają rejestracji i podania hasła.

56 OPIS ZJAWISKA

Hasło wraz z nazwą użytkownika tworzy zestaw informacji, który jest najpopularniejszym sposobem uwierzytelniania, czyli weryfikacji tegoż użytkownika przy logowaniu się do komputera czy do serwisu internetowego. Hasło jest więc ważnym elementem bezpieczeństwa i warto zdać sobie sprawę, że łatwe do odgadnięcia hasło (np. „12345” lub imię kota) takim zabezpieczeniem nie jest. Często użytkownicy nie doceniają roli haseł i stosują słabe hasła, które są:
- krótkie – łatwe do zaatakowania „na ślepo” (hasło poddane zostaje wielu próbom odgadnięcia – im krótsze hasło, tym łatwiej je złamać);
- łatwe do odgadnięcia poprzez ataki tzw. słownikowe (hasło jest wyrazem znajdującym się w słownikach) – atakujący wykorzystuje programy pozwalające próbować słowa z różnych istniejących słowników.

Łatwo sobie wyobrazić, czym może skończyć się złamanie przez intruza (osobę lub szkodliwy program) hasła do poczty elektronicznej, konta bankowego czy pliku zawierającego poufne dane. Można stracić poufne dane, a nawet gotówkę.

Dlatego też powinno się pamiętać o kilku zasadach, które na pozór wydają się trudne do spełnienia, ale, jak się okaże, łatwo można sobie z tym poradzić:

a. należy stosować hasła odpowiednio długie. Niektóre serwisy wymuszają odpowiednią długość haseł (np. 8 znaków, 10 znaków i więcej). Uważa się, że hasła silne nie powinny mieć mniej niż 12 znaków;
b. w haśle powinny się znajdować różne typy znaków: cyfry, duże litery, znaki specjalne (np. $, !, *).

57

Tak więc wyobraźmy sobie hasło spełniające powyższy warunek: **Ct jh,kwn10l?.** To jest silne hasło, spełnia powyższe reguły, ale z drugiej strony jest trudne do zapamiętania. Często więc użytkownicy zapisują trudne do zapamiętania hasła w miejscach łatwo dostępnych (np. na karteczkach blisko komputera) bądź

OPIS ZJAWISKA

w miejscach łatwych do przewidzenia (notesy, telefony itp.). To powoduje, że hasła łatwo mogą wpaść w niepowołane ręce. Haseł nie należy przekazywać bowiem nikomu pod żadnym pozorem, ani na karteczce, ani e-mailem, ani słownie, ani w żaden inny sposób. Hasło najbezpieczniejsze jest w naszej głowie. Ale jak zapamiętać tak upiorne hasło jak **Ct jh,kwn12m?,** może ktoś zapytać? O tym w części: DOBRE PRAKTYKI.

58 Hasła, o których mowa była do tej pory, niezależnie czy silne czy słabe, są tzw. hasłami statycznymi, wielokrotnego użytku. Hasła statyczne, nawet te najsilniejsze, mogą zostać przechwycone przez szkodliwe oprogramowanie (np. tzw. keylogeery), podsłuchane (np. przez programy monitorujące przepływ pakietów w sieci), bądź podpatrzone. Może stać się to w sposób niezauważony dla użytkownika i od tej pory ktoś inny może posługiwać się naszym identyfikatorem i hasłem.

59 Dlatego też, do bardziej zaawansowanych zastosowań, np. logowania zdalnego do sieci firmowej bądź do konta bankowości elektronicznej używa się haseł dynamicznych – tzw. **haseł jednorazowych**.

60 Hasło jednorazowe (czy też kod jednorazowego użytku), jest to hasło, które traci swą ważność po jednokrotnym zastosowaniu, a więc jego podsłuchanie nic nie daje osobom postronnym. W bankowości elektronicznej stosuje się hasła jednorazowe w postaci np.:

- tzw. kart zdrapek, gdzie do zatwierdzania każdej kolejnej transakcji używa się kolejnego kodu znajdującego się na specjalnej karcie wydawanej przez bank;
- tzw. tokenów, czyli specjalnych urządzeń elektronicznych, wyświetlających kolejne kody, którymi należy się posłużyć w trakcie dokonywania transakcji.

61 Częstokroć bankowcy stosują także metodę „pytanie-odpowiedź" i użytkownik konta bankowości elektronicznej otrzymuje w trakcie operacji bankowej esemesem na swój telefon kod, którym powinien się posłużyć dla autoryzacji transakcji.

62 Metody haseł statycznych i dynamicznych są niejednokrotnie stosowane łącznie, np. żeby zalogować się do serwisu bankowego jesteśmy proszeni o podanie identyfikatora i hasła statycznego (względnie określonych pozycji w haśle, np. trzeciej, piątej, szóstej, ósmej i dziewiątej) a do zatwierdzania transakcji używany jest kod jednorazowy (np. otrzymywany esemesem).

63 Metody uwierzytelniania (czyli weryfikacji użytkownika za pomocą identyfikatora i hasła) cały czas są rozwijane i cały czas podlegają coraz to nowym, wymyślnym atakom, takim jak ZeuS czy ZITMO[1].

64 **ROZPOZNANIE PROBLEMU OBJAWY**

Zwykle użytkownik nie ma świadomości, że hasła znalazły się w posiadaniu osób postronnych. Może się zorientować po wystąpieniu niepożądanych konsekwencji, takich jak podejrzana (nie jego) aktywność na danym koncie lub wymierne straty, jeśli mówimy o hasłach do serwisów zakupowych czy bankowych. Czasem jednak może zauważyć pierwsze symptomy podejrzanej aktywności. Na przykład, kiedy jest się pewnym, że podane zostało prawidłowe hasło do serwisu, z którego często korzystano a jednak okazuje się, że jest ono nieprawidłowe i użytkownik musi zastosować procedurę ustalenia nowego hasła, może to oznaczać, że osoba niepowołana była zdolna wcześniej przechwycić hasło i nawet zmienić je na inne. To może oznaczać, że został

[1] http://www.cert.pl/news/3193

ROZPOZNANIE OBJAWY

ĆWICZENIA 32

zawirusowany komputer lub też metoda uwierzytelniania do serwisu nie jest bezpieczna (np. nie ma włączonego szyfrowania).

65 **DIAGNOZA**

Diagnoza polega na przeprowadzeniu wywiadu z osobą posługującą się komputerem czy innym urządzeniem komunikującym się z siecią i poproszeniu o podanie jakiegoś przykładowego hasła, którego używa. Następnie należy zapytać, czy dana osoba używa tego samego hasła do wielu komputerów, programów, serwisów internetowych. Jeśli okaże się, że podane przykładowe hasło jest słabe wg opisu z tego działu oraz osoba ta używa tych samych haseł do wielu serwisów, można postawić diagnozę, że jest ona narażona na utratę swoich danych czy pieniędzy. Należy następnie spytać, czy spotkała się z określeniem: słabe hasła oraz czy zna zasady i metody konstruowania silnych haseł. W rozmowie należy też spytać, czy korzysta z bankowości elektronicznej i w jaki sposób odbywa się uwierzytelnienie i autoryzacja transakcji – czy użytkownik rozumie istotę tego procesu i jakie czyhają tu zagrożenia.

66 **DOBRE PRAKTYKI**

Wróćmy do przykładowego hasła:

Ct jh,kwn12m?

Wiemy już, że nie należy haseł nigdzie zapisywać, a więc pozostaje pytanie, czy silne hasła są zapamiętywalne? Oczywiście, jeśli takie hasło stworzy automatyczny generator, szansa jego zapamiętania jest niewielka. Ale można takie hasła konstruować inaczej. Jeśli zdamy sobie sprawę, że nasze przykładowe hasło powstało ze zdania:

Czy **t**o **j**est **h**asło**, k**tóre **w**ytrzyma **n**astępne **12 m**iesięcy**?**

67 to kwestia jego zapamiętanie wyda się od razu znacznie łatwiejsza. Są to tzw. metody mnemotechniczne pozwalające tworzyć silne hasła, które jednocześnie nie są trudne do zapamiętania, bo autor może je skojarzyć np. z jakimś znanym mu zdaniem.

68 Jakie są inne zalecenia i dobre praktyki związane ze stosowaniem haseł?

Oto kilka z nich:

a. Jeśli użytkownik ma (a zwykle ma) wiele kont w serwisach internetowych, to nie powinien stosować tego samego hasła do wszystkich serwisów. Szczególnie, jeśli są to konta o różnej ważności (np. konto w serwisie społecznościowym i konto w bankowości elektronicznej). Zaatakowanie jednego serwisu i przejęcie haseł użytkowników narazi wszystkie ich aktywności online na poważne zagrożenie. Jeśli użytkownik chce sobie ułatwić zarządzanie kilkoma hasłami (zapisać, jakie hasło służy do jakiego serwisu), może stosować dodatkowe oprogramowanie[2], które będzie przechowywało nazwy i hasła w formie zaszyfrowanej – a użytkownikowi pozostanie zapamiętać jedno jedyne hasło główne;
b. Nie należy korzystać z opcji zapamiętania hasła, którą oferują serwisy „dla naszej wygody". Po jakimś czasie, nawet jeśli nikt nie przechwyci hasła, użytkownik nie będzie wiedział, jakiego używa, bo przyzwyczai się do wchodzenia na dany serwis bez podawania hasła (zrobi to za niego oprogramowanie);
c. Nawet silne hasło trzeba kiedyś zmienić na nowe. Systemy operacyjne, takie jak Windows, wymuszają cykliczną zmianę haseł (np. co pół roku), ale nawet jeśli nie ma przymusu – warto hasła zmieniać. Dlaczego? Nigdy nie wiadomo, czy nie zostało ono podsłu-

[2] np. opensource'owy program KeePass Pasword Safe

chane, podpatrzone i czy nie zostanie wykorzystane bez wiedzy właściciela;

d. Jeśli użytkownik zapomni hasła, wiele serwisów oferuje opcje podpowiedzi bądź wysyła na skrzynkę e-mail link do strony WWW, na której można ustalić nowe hasło. Jeśli chodzi o podpowiedzi, starajmy się, aby nie były łatwe do odgadnięcia (np. imię kota babci), natomiast ustalając nowe hasło poprzez logowanie do specjalnej strony www danego serwisu, należy zwrócić uwagę czy połączenie jest bezpieczne (szyfrowanie SSL – ikonka zamkniętej kłódeczki oraz certyfikat należący do właściciela serwisu);
e. Na koniec porady uniwersalne:

należy posiadać aktualne oprogramowanie antywirusowe, bo to minimalizuje zagrożenie, że hasła zostaną przechwycone przez cyberprzestepców,

nie należy logować się do ważnych serwisów z kafejek internetowych, bo nie wiemy, czy publiczne komputery nie są zawirusowane i czy nie przechwycą danych uwierzytelniających,

również korzystając z własnego sprzętu, ale za pomocą publicznych sieci WiFi powinno się mieć ograniczone zaufanie do bezpieczeństwa, bo prawdopodobieństwo, że ktoś podsłuchuje naszą transmisję jest całkiem spore.

BIBLIOGRAFIA:

Aktualizowanie oprogramowania, „OUCH!”, Biuletyn bezpieczeństwa komputerowego SANS Institute i CERT Polska – 8/2011 (http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201108_po.pdf)

Backup i przywracanie danych,„OUCH!”, Biuletyn bezpieczeństwa komputerowego SANS Institute i CERT Polska, 10/2011 (http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201110_po.pdf)

Bezpieczne i silne hasła, „OUCH!”, Biuletyn bezpieczeństwa komputerowego SANS Institute i CERT Polska – 5/2011 (http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201105_po.pdf)

Bezpieczny komputer w siedmiu krokach, „OUCH!” 12/2012, http://www.securingthehuman.org

E-mail kilka prostych porad, „OUCH!”, 3/2012, http://www.securingthehuman.org

Ludwig-Maximilians-Universität München, http://www.fak11.lmu.de/it/it_sicherheit/botnets/botnets_pl.html#Polski

Microsoft support: http://windows.microsoft.com/pl-pl/windows-vista/how-do-i-know-if-a-wireless-network-is-secure

Raport Dyżurnet – *Rozwiązania filtrujące niepożądane treści w Internecie*, Warszawa 2009

Stecko K., *Przewodnik po bezpieczeństwie e-mail – przegląd popularnych zagrożeń*, „Haking” 1/2011

Zabezpieczenia domowej sieci bezprzewodowej, „OUCH!”, 1/2012 http://www.securingthehuman.org

ZAGROŻENIA DLA
PRYWATNOŚCI

Marcin Bochenek, Piotr Bisialski,
Martyna Różycka, Anna Rywczyńska,
Krzysztof Silicki, Agnieszka Wrońska

OPIS ZJAWISKA

1 **WPROWADZENIE**

Problematyka ochrony prywatności należy do najważniejszych aspektów związanych z bezpieczeństwem użytkowników Internetu. Od tego, w jaki sposób będzie zarządzać swoją tożsamością online zależy, czy bardziej użytkownik narażony będzie na cyberprzemoc, czy nie grozi mu utrata danych osobowych, czy nie padnie ofiarą oszustw finansowych oraz czy w przyszłości jego wizerunek w sieci nie zaprzepaści szans na karierę, dostęp do edukacji, udane życie rodzinne. Umiejętna ochrona prywatności powinna stanowić podstawę w edukacji zarówno najmłodszych, jak również dorosłych użytkowników Internetu. W dobie niezwykłej popularności portali społecznościowych i, co za tym idzie, przenoszenia wielu aspektów codziennego życia do sieci szczególnie ważne jest umiejętne tworzenie swoich profili sieciowych, zaznajamianie się z regulaminami poszczególnych serwisów, świadome korzystanie z ustawień prywatności i kontrolowanie danych i informacji, które pojawiają się o nas w Internecie. Szczególnie ważna jest też troska o bezpieczną obecność dziecka online. W poniższym dziale przedstawiono zagrożenia związane z niewłaściwym zarządzaniem swoją prywatnością, omówiono problem cyberprzemocy oraz narzędzia i zasady, dzięki którym użytkownicy mogą być bezpieczniejsi w sieci.

SERWISY SPOŁECZNOŚCIOWE

(bezpieczny profil, spam, cyberprzemoc, ujawnianie informacji)

2 **Lista pojęć**

Portal społecznościowy, Facebook, nk.pl, Nasza klasa, profil, fanpage, cyberprzemoc, aplikacje internetowe, posty

3 Celem tej części artykułu jest omówienie problematyki związanej z bezpiecznym korzystaniem z serwisów społecznościowych:

- przedstawienie zjawiska;
- omówienie zagrożeń związanych z korzystaniem z serwisów społecznościowych;
- wskazanie zasad ochrony prywatności online.

4 **OPIS ZJAWISKA**

Jednym z ostatnich fenomenów sieci jest niezwykła popularność portali społecznościowych. W Polsce korzysta z sieci społecznościowych już prawie 70% dzieci i młodzieży. W grupie wiekowej 15–16 lat odsetek ten jest jeszcze wyższy. Największą popularność w ostatnich latach zdobył Facebook, z którego obecnie korzysta ponad 900 mln internautów na całym świecie. W Polsce od kilku lat bardzo powszechny jest również portal Nasza klasa. Ideą tego rodzaju serwisów jest przekazanie internautom platformy, za pośrednictwem której mogą dzielić się swoimi codziennymi doświadczeniami, zdjęciami czy też ciekawostkami, mogą budować sieci znajomych, utrzymywać stałe kontakty z ludźmi z całego świata oraz odnawiać kontakty z przyjaciółmi z przeszłości. Efektem niezwykłej popularności portali społecznościowych stała się powszechna na nich obecność firm, instytucji pozarządowych oraz innych organizacji prowadzących za pośrednictwem tzw. fanpage'ów kampanie swoich inicjatyw czy też budujące swoją markę.

5 **ROZPOZNANIE PROBLEMU OBJAWY**

Największym ryzykiem związanym z korzystaniem z portali społecznościowych jest brak umiejętności ochrony własnej prywatności. Nieumiejętne tworzenie profilu oraz zbyt wiele informacji publikowanych na profilach publicznych może stać się przyczyną dostania się danych w niepowołane ręce. Co więcej, z serwisu Facebook korzysta ponad połowa dzieci w wieku 9–12 lat, mimo iż jego regulamin zezwala na założenie konta dopiero po ukończeniu 13. roku życia. Jednym z zagrożeń związanych z brakiem ochrony prywatności w sieci może być cyberprzemoc – inaczej przemoc z użyciem mediów elektronicznych[1] – przede wszystkim Internetu i telefonów komórkowych. Przypomnijmy, do działań określanych jako cyberprzemoc zalicza się m.in.: wyzywanie, straszenie, poniżanie kogoś w Internecie lub przy użyciu telefonu, robienie komuś zdjęć lub rejestrowanie filmów bez jego zgody, publikowanie w Internecie lub rozsyłanie telefonem zdjęć, filmów lub tekstów, które kogoś obrażają czy ośmieszają lub podszywanie się pod kogoś w sieci.

6 Portale społecznościowe to również coraz częściej środowisko dla spamu, profile użytkowników pozwalają na wyjątkowo precyzyjne ukierunkowanie oferty komercyjnej, na którą podatni mogą być zwłaszcza niepełnoletni użytkownicy portali. Potencjalnym zagrożeniem jest również narażenie się na straty finansowe w postaci m.in. kradzieży związanej z publikowaniem adresu, informacji o posiadanym majątku, zwłaszcza w połączeniu z zapowiedzią dłuższego urlopu.

7 Szczególną ostrożność trzeba też stosować przy korzystaniu z aplikacji internetowych. Zwłaszcza aplikacje stworzone poza Unią Europejską mogą nie chronić w odpowiedni sposób umieszczanych w nich danych osobowych. Nie warto korzystać z aplikacji nieznanego pochodzenia, ponieważ oprócz dostępu do skreślonych danych mogą również z konta użytkownika zdalnie rozsyłać się w sieci kontaktów.

Należy pamiętać, że Internet z łatwością zapamiętuje tzw. ścieżki (sposób poruszania si, miejsca, strony, po których porusza się użytkownik przyp. red.). Publikowane na różnych portalach i w rożnych kontekstach informacje mogą posłużyć komuś w celu zdobycia o użytkowniku szczegółowych danych i wykorzystania ich przeciwko niemu – na przykład w celu stworzenia fałszywego profilu, podszycia się pod daną osobę, doprowadzenia do oszustw bankowych itp.

8 **DIAGNOZA**

Mając na uwadze zagrożenia związane z korzystaniem z portali społecznościowych, należy zachować w Internecie szczególną dbałość o swoją prywatność, a przede wszystkim o informacje pozwalające na zidentyfikowanie konkretnej osoby: imię, nazwisko, wiek, adres, nazwa szkoły, zdjęcia. Publikując dane osobiste, należy trzymać się prostej zasady – umieszczać tylko takie informacje, które byłoby się w stanie powierzyć nieznajomemu. Budując profil oraz akceptując osoby do sieci kontaktów, warto korzystać ze zróżnicowanych uprawnień jakie można do danego kontaktu przypisać. Szczegółowe informacje można znaleźć np. w sekcji „Ustawienia i narzędzia prywatności" na portalu Facebook. Należy pamiętać też o tym, że informacja raz zamieszczona w Internecie pozostanie w nim na zawsze, a dostęp do niej może mieć praktycznie każdy, również za kilka, kilkanaście lat. Zamykanie starych, nieużywanych kont w serwisach społecznościowych oraz używanie różnych

ROZPOZNANIE OBJAWY

DIAGNOZA

[1] więcej na ten temat w module II

DOBRE PRAKTYKI

ĆWICZENIA 34

loginów i haseł w poszczególnych portalach to jedne z kluczowych działań, które można podjąć, mając na uwadze ochronę prywatności online.

9 **DOBRE PRAKTYKI**

Chcąc właściwie dbać o swoją prywatność warto pamiętać[2]:

- o sprawdzeniu, w jaki sposób działa portal zanim utworzy się na nim swój profil. Przede wszystkim zainteresować się, jaki poziom prywatności gwarantuje dany portal. Informacje tego typu powinny znajdować się w regulaminie uczestnictwa w serwisie;
- o kontroli dostępu do własnych danych. Bezpieczny portal społecznościowy powinien pozwolić na nadanie takiego statusu prywatności, który zagwarantuje, że informacje będą dostępne tylko dla znajomych, których świadomie doda się do swojej listy;
- o trzymaniu hasła dostępu w tajemnicy;
- o zastanowieniu się, zanim zamieści się w sieci zdjęcia. Publikując zdjęcie, należy ustawić taki status prywatności, który zagwarantuje bezpieczeństwo;
- o zachowaniu ostrożności w kontaktach z osobami znanymi wyłącznie w sieci;
- o odpowiedzialności za informacje, które się publikuje;
- o nieujawnianiu danych innych osób, nieprzesyłaniu dalej cudzych maili czy też niepublikowaniu zdjęć bez zgody;
- o tym, że jeżeli padnie się ofiarą cyberprzemocy można zgłosić ten fakt odpowiednim instytucjom (szkoła, policja, helpline.org.pl – 0-800-100-100) i osobom, które mogą udzielić pomocy: rodzice, psycholog szkolny, nauczyciel;
- o tym, że w serwisach społecznościowych należy używać maksymalnych ustawień prywatności, mieć świadomość kto będzie mógł oglądać posty, co inne osoby zobaczą na naszej osi czasu, do jakich grup zostaliśmy włączeni (często dzieje się to bez wiedzy użytkownika), czy też gdzie zostaliśmy oznaczeni bez swojej wiedzy.

[2] http://www.saferinternet.pl/informacje/jak_byc_bezpiecznym_w_internecie.html

NIEBEZPIECZNE KONTAKTY

10 **Lista pojęć**

Monitoring, niebezpieczne treści, niebezpieczne kontakty, prywatność

11 Celem tej cześci artykułu jest omówienie problematyki niebezpiecznych kontaktów

- wprowadzenie do tematyki niebezpiecznych kontaktów;
- omówienie zagrożeń związanych z nawiązywaniem niebezpiecznych kontaktów ;
- wskazanie zasad ochrony dzieci i młodzieży przed niebezpiecznymi kontaktami.

12 **OPIS ZJAWISKA**

Internet służy przede wszystkim komunikowaniu się. Istnieje wiele platform, programów, serwisów, które umożliwiają komunikację między użytkownikami. Należy jednak mieć na uwadze, że tutaj również użytkownicy – szczególni ci młodsi – są narażeni na nawiązywanie niebezpiecznych kontaktów z nieznajomymi. W badaniach EU Kids Online jednym z najczęściej wymienianych przez polskie dzieci zagrożeń jest właśnie zawieranie internetowych znajomości. Aż 24% dzieci potwierdza, że nawiązuje w Internecie kontakty z niezna-

jomymi. Co czternaste badane dziecko przyznaje, że spotyka się w świecie realnym z osobami poznanymi w Internecie.

13 Rozmowa z osobą nieznajomą może prowadzić do uwiedzenia dziecka przez osobę dorosłą. Ale niebezpieczne kontakty oznaczają szerzenie niebezpiecznych idei, poglądów i zachowań. Nieostrożność może prowadzić do wyłudzenia danych osobowych, haseł, danych bankowych czy nawet pieniędzy.

14 **ROZPOZNANIE PROBLEMU**
OBJAWY

Należy zwrócić szczególną uwagę na znajomości zawiązywane przez osoby małoletnie. Zwłaszcza w wypadku młodszych należy monitorować znajomości zawiązywane przez Internet. Monitoringiem powinny zostać objęte zarówno profile w serwisach społecznościowych, na innych witrynach typu fora internetowe oraz czaty i videoczaty. W wypadku dzieci i młodzieży zaleca się, aby opiekun był „znajomym" dziecka i w ten sposób obserwował działania podopiecznego w Internecie. Należy jednak pamiętać, że serwisy internetowe umożliwiają różne ustawienia prywatności oraz widoczności aktywności online dla różnych grup znajomych i dla poszczególnych znajomych. Zaleca się ustalenie zasad monitoringu razem z dzieckiem. Zdarza się, że osoby o skłonnościach pedofilskich podszywają się pod inne dziecko i w ten sposób nawiązują znajomość. Należy zatem sprawdzać wszystkich znajomych dziecka.

15 **DIAGNOZA**

Niebezpieczna znajomość, w której dziecko uczestniczy jest z reguły trudna do rozpoznania. Może nasunąć pewne podejrzenia zmiana w zachowaniu dziecka, zainteresowanie nowymi tematami, skrytość, podejrzliwość, a przede wszystkim pojawienie się u niego nowych i drogich przedmiotów.

16 Należy sprawdzać aktywność online, obserwować historię przeglądanych stron internetowych. Osoby niebezpieczne mogą polecać strony internetowe, na których są zamieszczone treści radykalne, namawiające do niebezpiecznych zachowań czy materiały pornograficzne.

17 **DOBRE PRAKTYKI**

Nigdy nie wolno podawać danych takich jak login do banku, hasło, adres zamieszkania osobom poznanym na czacie czy forum.

18 Jeśli te informacje zostały podane, należy: bezzwłocznie skontaktować się z bankiem (gdy sprawa dotyczy danych bakowych), jak najszybciej skasować informacje (np. adres zamieszkania). Jeśli użytkownik podał informacje takie jak login i hasło, powinien jak najszybciej powiadomić o tym właściciela serwisu i zmienić hasło. W wypadku zagrożenia odpowiedni będzie kontakt z najbliższą jednostką policji.

19 Kiedy nieznajomy z Internetu zaprosi na spotkanie, należy umówić się w miejscu publicznym. Najlepiej też powiadomić kogoś zaufanego o swoich planach. Takie zasady bezpieczeństwa powinny być stosowane również przez dorosłych internautów.

Należy zwrócić też uwagę na informacje, które są przekazywane na zdjęciach czy filmach, aby nie ujawniać zbyt dużo prywatnych danych.
Edukując dziecko w zakresie bezpieczeństwa online, należy zwrócić szczególną uwagę na zachowanie zasad prywatności oraz uświadamiać, że w Internecie może spotkać osoby o nieodpowiednim i niebezpiecznym zachowaniu. Należy wypracować również procedurę informowania osoby dorosłej o sytuacjach zagrożenia.

CYBERPRZESTĘPCZOŚĆ I NADUŻYCIA

TREŚCI
SZKODLIWE I NIELEGALNE

Marcin Bochenek, Piotr Bisialski,
Martyna Różycka, Anna Rywczyńska,
Krzysztof Silicki, Agnieszka Wrońska

OPIS ZJAWISKA

1 **WPROWADZENIE**

Dla wielu ludzi Internet jest podstawowym, a czasem jedynym źródłem informacji. Korzystanie z zasobów tego ogólnoświatowego medium pozwala na bieżące śledzenie wydarzeń, pozyskiwanie informacji np. naukowych z różnego rodzaju badań naukowych i artykułów, a także jest źródłem rozrywki. Łatwość publikacji oraz brak potrzeby weryfikacji przed publikacją pozwala zamieszczać materiały każdemu użytkownikowi. W praktyce oznacza to, że w Internecie znajdują się również materiały niebezpieczne – szkodliwe przede wszystkim dla najmłodszych odbiorców, ale również nielegalne.

2 Aby ustrzec się przed kontaktem z tego rodzaju treściami, należy korzystać z zaufanych źródeł informacji, odpowiedzialnych i uznanych serwisów informacyjnych. Pobieranie załączników, plików niewiadomego pochodzenia, otwieranie linków publikowanych na forach może prowadzić do pobrania nielegalnych materiałów i/lub zainfekowania urządzenia, z którego korzysta użytkownik. Aby ustrzec się przed naciągaczami i niebezpiecznymi zachowaniami w Internecie, należy również czytać i śledzić regulaminy, które opisują szczegółowe warunki korzystania z serwisu.

3 Napotkanie nielegalnych lub szkodliwych treści powinno zostać zgłoszone moderatorom serwisu, policji lub specjalnym powołanym do tego zespołom takim jak Dyżurnet.pl, Helpline.org.pl.

PRAWO AUTORSKIE W POLSCE

OPIS ZJAWISKA

Naruszanie praw autorskich jest zjawiskiem powszechnym. Jak wykazują liczne badania, a także deklaracje osób korzystających z Internetu, znaczna część użytkowników w różnym stopniu korzysta z utworów i programów komputerowych pozyskanych na drodze nieuprawnionego kopiowania i ściągania. **Naruszenie praw autorskich można zdefiniować jako sytuację, w której dana osoba korzysta z utworów bez zezwolenia autora lub innej osoby uprawnionej z tytułu praw autorskich**. Należy jednak dodać, iż z punktu widzenia prawnego sprawa nie jest prosta. O ile bowiem korzystanie w ten sposób z programu komputerowego jest kwalifikowane jednoznacznie jako czyn niedozwolony i podlegający karze, o tyle w wypadku muzyki, filmów etc. sytuacja nie jest już tak jednoznaczna. Jeśli chodzi o programy komputerowe, to na kwalifikację czynu wpływa specyfika techniczna programów, które w procesie nieuprawnionego pozyskiwania zwielokrotniają się. W wypadku filmów i muzyki sytuacja jest bardziej skomlikowana. Oglądanie filmów, ściąganie muzyki i wykorzystywanie tych utworów prywatnie zasadniczo traktowane jest jako tzw. dozwolony użytek (cały czas mówimy o utworach nielegalnie umieszczonych w sieci). Sankcjom prawnym podlega za to rozpowszechnianie, a więc umieszczanie takiego utworu w miejscu, z którego mogą pozyskać go inni użytkownicy, rozsyłanie, kopiowanie na inne nośniki i dystrybucja. Zjawisko, o którym mowa ma przyczyny ekonomiczne i psychologiczne. Te pierwsze wiążą się z możliwością pozyskania utworów bez konieczności ich kupowania lub kupowanie tychże za cenę stanowiącą ułamek ich ceny rynkowej. Psychologiczne uwarunkowania to głównie chęć szybkiego dostępu do

najnowszych utworów bez konieczności oczekiwania na ich obecność w legalnych kanałach dystrybucji. Niewątpliwie jednak podstawowym motywem podejmowanych przez użytkowników działań jest motyw ekonomiczny.

4 DIAGNOZA

Trudno mówić o jednoznacznych symptomach wskazujących na fakt nielegalnego pozyskiwania treści. Podstawowym sposobem sprawdzenia, czy dane zjawisko ma miejsce, może być wywiad – rozmowa z daną osobą i uzyskanie odpowiedzi na pytania o zakres i sposób korzystania z treści internetowych. W wypadku występowania takiej sytuacji trudno mówić o objawach związanych z problemem.

5 Diagnoza prowadzona metodą opartą na wywiadzie może przyczynić się do uzyskania informacji o występowaniu w danym wypadku zjawiska nielegalnego korzystania z treści lub naruszania praw autorskich. Tak jak zostało to już podkreślone wyżej, należy rozgraniczyć działania penalizowane i działania stanowiące naruszenie praw autorskich. Przeciwdziałanie musi opierać się na jednoznacznym zdefiniowaniu zaobserwowanej sytuacji. W przypadku, gdy ktoś korzysta z treści w sposób naruszający prawa autorskie, należy wskazać przede wszystkim rozwiązania pozytywne. Obecnie w Internecie znajduje się wiele w pełni legalnych serwisów oferujących darmowy kontent filmowy i muzyczny. Jest to niewątpliwie pewna alternatywa dla osób pozyskujących treści nielegalnie umieszczone w sieci. Ten argument może okazać się jednak niewystarczający, ponieważ serwisy oferujące legalne treści nie proponują użytkownikom najbardziej przez nich pożądanych, najnowszych materiałów. Dodatkowo sytuację utrudnia fakt, iż samo korzystanie z takich materiałów, choć nieuprawnione, nie podlega penalizacji (to dominująca opinia prawna w Polsce, ale warto zauważyć, iż sprawa nie jest zupełnie jednoznaczna). Gdy więc argument o innej, również darmowej, drodze korzystania z utworów i argument o ryzyku ponoszenia odpowiedzialności nie mogą w pełni zafunkcjonować, warto zwrócić uwagę na istotne zagrożenia wiążące się z tym problemem. Także w tym przypadku, tak jak i w wielu innych związanych z korzystaniem z Internetu, możemy mówić o zagrożeniu płynącym z cyberprzestrzeni. Użytkując serwisy, często funkcjonujące także poza Polską, internauta naraża się na zainfekowanie swojego komputera wirusami, utratę danych, awarię sprzętu, a także na straty finansowe związane z ewentualnym przejęciem przez hakerów dostępu do jego konta bankowego lub kart płatniczych. Możliwość dochodzenia swoich praw przez osobę poszkodowaną w wypadku zaistnienia takiej sytuacji jest trudna, a w praktyce odzyskanie straconych środków finansowych jest wątpliwe.

6 DOBRE PRAKTYKI

Wydaje się, że dla pracownika socjalnego właśnie wskazanie zagrożeń i ryzyka może być skutecznym argumentem do przekonania osób naruszających prawa autorskie do zmiany postępowania. Argument, o którym mowa ma charakter przede wszystkim ekonomiczny, a więc stanowi niejako odpowiedź na argumenty ekonomiczne stanowiące motywacje działania tych osób. Warto jednak zauważyć, iż stosowanie w praktyce tego typu metod nie powinno powodować rezygnacji ze wskazywania na inne, w tym etyczne, aspekty tego zjawiska. Warto także uświadamiać, iż masowa skala „piractwa" może wpływać i wpływa na kondycję twórców i całej branży muzycznej i filmowej. Gdy więc skurczą się źródła przychodów, zmniejszy się też produkcja, a co za tym idzie pojawi się mniej nowych treści. W rezultacie widzowie i słuchacze po prostu nie będą mieli możliwości słu-

ROZPOZNANIE OBJAWY
DIAGNOZA
DOBRE PRAKTYKI
ĆWICZENIA 36

chania i oglądania nowych utworów z powodu ich braku.

PEER-TO-PEER (P2P)

Jest to termin określający w świecie sieci komputerowych taką topologię połączeń, w której każdy komputer może pełnić zarówno formę serwera (udostępniającego np. pliki muzyczne w Internecie) jak i klienta, czyli komputera, który korzysta z zasobów udostępnianych przez inne komputery. Sieć peer-to-peer może działać w zasadzie bez żadnego centralnego serwera, choć w wielu aplikacjach typu peer-to-peer istnieją serwery centralne, które pełnią rolę ułatwiającą nawigację w sieci.

7 Sieci peer-to-peer działające w Internecie wymagają, aby wszystkie komputery w tej sieci były wyposażone w ten sam (albo inny, kompatybilny – jeśli istnieje) program, który zapewnia łączność z innymi komputerami w sieci w celu wymiany plików, połączeń audio, wideo itp.

8 Przykładem oprogramowania działającego w modelu peer-to-peer jest Skype, aplikacja, która zapewnia łączność głosową, wideo, czat i przekazywanie plików pomiędzy użytkownikami, którzy mają uruchomiony ten program.

9 Warto wiedzieć, że uruchamiając aplikację peer-to-peer nie tylko korzystamy z pewnych usług, takich jak w powyższym przykładzie, ale także komputer staje się niejako serwerem i przekaźnikiem komunikacji dla innych użytkowników. Te procesy dzieją się poza kontrolą właściciela. Jeśli korzystamy z aplikacji, która daje nam dostęp do plików na dyskach komputerów rozmieszczonych na całym świecie – oznacza to jednocześnie, że pliki znajdujące się na danym komputerze mogą być dostępne dla całego świata. Zależy to od tego, jak skonfigurujemy program peer-to-peer. Zdarza się, że domyślnie taki program udostępnia wszystkie pliki znajdujące się na określonym dysku, co jest oczywiście dużym zagrożeniem dla prywatności i bezpieczeństwa użytkownika.

10 Popularność sieci peer-to-peer, takich jak np. pionierski acz kontrowersyjny Napster zaczęła rosnąć w szybkim tempie na przełomie XX i XXI wieku ze względu na możliwość swobodnej wymiany plików muzycznych – a potem także wideo bezpośrednio pomiędzy użytkownikami Internetu. Jednak z drugiej strony, zrodziło to protest organizacji zarządzających prawami autorskimi, które podnosiły, że ściąganie plików w sieci peer-to-peer jest nielegalne, narusza bowiem prawa twórców utworów. Sam Napster w wyniku procesów sądowych w USA zakończył działalność jako bezpłatny serwis w roku 2001.

11 Korzystając więc z serwisów peer-to-peer należy zdawać sobie sprawę, czy to co robi użytkownik (ściąganie lub udostępnianie plików) nie narusza praw autorskich twórców utworów muzycznych, filmów, audiobooków, e-booków czy programów komputerowych. Obecnie coraz częściej jesteśmy świadkami informacji o zatrzymaniu przez policję użytkowników Internetu, którzy ściągali nielegalne pliki i jednocześnie udostępniali je innym przy pomocy aplikacji P2P[1]. Podstawą ścigania są w tym wypadku przepisy ustawy o prawach autorskich i prawach pokrewnych.

[1] http://media2.pl/internet/87965-Korzystali-z-programow-p2p-trafia-przed-sad.html

12 W sieci peer-to-peer znajduje się również wiele materiałów nielegalnych, np. pornografia dziecięca. Nie zawsze można ustrzec się przed jej ściągnięciem, ponieważ tytuł pliku sugeruje film, muzykę czy program. Dopiero po ściągnięciu pliku i jego rozpakowaniu okazuje się, że użytkownik posiada nielegalne materiały, które udostępniał innym od momentu rozpoczęcia ściągania. Zgłaszając naruszenie na policję lub do zespołów reagujących należy podać nazwę używanego programu, numer IP użytkownika udostępniającego nielegalne treści, jak najdokładniejszy czas, w jakim dany plik jest/był udostępniany oraz jego nazwę.

TREŚCI SZKODLIWE I NIELEGALNE

OPIS ZJAWISKA

Treści nielegalne to takie, które są zabronione przez regulacje prawne. W Polsce obowiązują przede wszystkim przepisy Kodeksu Karnego. Polskie prawo zabrania m.in.:

- przechowywania lub posiadania treści pornograficznych z udziałem dziecka poniżej 15 roku życia,
- rozpowszechniania i publicznego prezentowania pornografii z udziałem osoby poniżej 18 roku życia,
- rozpowszechniania i publicznego prezentowania pornografii związanej z prezentowaniem przemocy lub posługiwaniem się zwierzęciem,
- propagowania ustrojów totalitarnych, szerzenia nienawiści wobec jednostki lub grupy społecznej ze względu na jej pochodzenie, kulturę, wyznanie lub ze względu na jej bezwyznaniowość,
- nakłaniania do popełnienia przestępstwa.

Zespół Dyżurnet.pl[2], którego głównym zadaniem jest reakcja na zgłoszone nielegalne lub szkodliwe treści w opublikowanym raporcie za rok 2012 wskazuje, że największą liczbę zgłoszeń stanowią te odnoszące się do pornografii dziecięcej – 706 oraz treści rasistowskich i ksenofobicznych – 464.

Treści szkodliwe to materiały związane z prezentowaniem agresji (np. wulgaryzmy, mowa nienawiści, treści nawołujące do samookaleczeń), nieobiektywna interpretacja faktów historycznych, zjawisk socjologicznych lub treści brutalne. Treści nieodpowiednie bardzo często są atrakcyjne i poszukiwane przez młodego odbiorcę – różnego rodzaju wyniszczające diety, zachęcanie do stosowania substancji zwiększających masę mięśniową, zaproszenie do wstąpienia do sekt.

13 ROZPOZNANIE PROBLEMU

Treści szkodliwe (w tym nielegalne) są to takie treści, które u osoby oglądającej mogą wywołać zaniepokojenie, stany lękowe, długotrwałe obniżenie nastroju, depresję, zaburzenia snu, koncentracji. Kontakt ze szkodliwymi treściami u dzieci może powodować nadmierne i nienaturalne zainteresowanie seksualnością, zaburzenia emocjonalne oraz powstawanie wypaczonego obrazu rzeczywistości.

14 DIAGNOZA

Ograniczenie wpływu szkodliwych treści powinno polegać przede wszystkim na uświadomieniu szkodliwości tego typu materiałów. Należy również zadbać o przygotowanie sprzętu, z którego dziecko korzysta i wyposażenie komputera, telefonu w program filtrujący z dostosowanym do wieku poziomem filtra. Należy uczulić szczególnie

[2] http://www.dyzurnet.pl/pobierz.html

młodsze dzieci, aby zgłaszały wypadki, kiedy zobaczą coś niepokojącego w Internecie.

UWAGA: jeśli dziecko posiada materiały pornograficzne, może być ofiarą przemocy seksualnej!

15 Zespół Dyżurnet.pl jest funkcjonującym w NASK punktem kontaktowym, do którego użytkownicy Internetu mogą kierować anonimowe zgłoszenia o potencjalnie nielegalnych treściach. Zespół podejmuje działania mające na celu podniesienie bezpieczeństwa dzieci i młodzieży w Internecie. Najważniejsze z nich są związane z obsługą zgłoszeń otrzymywanych od użytkowników Internetu, dotyczących treści potencjalnie nielegalnych, takich jak materiały przedstawiające seksualne wykorzystywanie dzieci lub nawołujące do nienawiści na tle rasowym. Oprócz przyjmowania zgłoszeń zespół prowadzi działania popularyzacyjno-edukacyjne związane z bezpiecznym korzystaniem z Internetu i przeciwdziałaniem sieciowym zagrożeniom, takie jak szkolenia dla profesjonalistów i ekspertów, a także dla najmłodszych użytkowników. Więcej na stronie internetowej www.dyzurnet.pl

16 **DOBRE PRAKTYKI**

Im mniejsze dziecko, tym większe powinny być postawione ograniczenia. Opiekunom małych dzieci zaleca się, aby dzieci korzystały tylko i wyłącznie z dedykowanych im witryn. Więcej na ten temat można znaleźć na stronie np. Sieciaki.pl. W europejskim badaniu EU Kids Online[3] dzieci w wieku 9–16 lat najczęściej jako zagrożenie internetowe wymieniają pornografię 23%, przemoc, agresję i sceny drastyczne 18%, nieodpowiednie zachowanie 19%, nieodpowiednie kontakty 13% oraz inne zagrożenia 10% i inne treści 17%. Wśród innych niebezpiecznych treści wskazały strony promujące anoreksję, bulimię oraz samobójstwo.

Treści szkodliwe dla dzieci mogą być dostępne nie tylko w Internecie, ale również w grach komputerowych czy grach na konsolę. Należy zwrócić uwagę, czy gra jest odpowiednio dostosowana do wieku odbiorcy. W wypadku gier komputerowych pomocna jest klasyfikacja PEGI[4], która wskazuje wiek gracza ze względu na poruszane w grze treści.

KRYTYKA ŹRÓDŁA

OPIS ZJAWISKA

Krytyka źródła

Potęga Internetu oznacza przede wszystkim olbrzymie zasoby informacji oraz możliwość łatwej komunikacji z innymi użytkownikami. Każdy może założyć stronę, blog i zamieszczać tam informacje. W praktyce oznacza to, że w sieci znajduje się wiele informacji nierzetelnych, nieprawdziwych i wprowadzających w błąd. Należy zwracać baczną uwagę na jakość treści dostępnych online, datę publikacji oraz jeśli to możliwe weryfikować informacje w innych źródłach.

17 **ROZPOZNANIE PROBLEMU OBJAWY**

Szczególnie niepokojące jest, gdy młodzi ludzie poszukują informacji o życiu seksualnym na forach internetowych, a nie sięgają do materiałów opracowanych przez specjalistów, opublikowanych na stronach instytucji i organizacji zajmujących się edukacją seksualną.

[3] http://swps.pl/images/stories/dokumenty/BPE/In-their-own-words.pdf

[4] http://www.pegi.info/pl/index/id/968, więcej na ten temat w artykule *Uzależnienia od gier komputerowych*.

18 Nierzetelne informacje mogą wprowadzać w błąd oraz wypaczać obraz rzeczywistości (patrz treści szkodliwe).

19 **DIAGNOZA**

Korzystając z zasobów internetowych, należy zwrócić uwagę na miejsce publikacji wykorzystywanych informacji. Wiadomości nierzetelne, niekompletne wprowadzają w błąd użytkownika. Może to prowadzić do niewłaściwej oceny sytuacji lub błędnych decyzji, a nawet strat finansowych czy uszczerbku na zdrowiu. Każdorazowo, kiedy mamy do czynienia z nierzetelną stroną internetową, należy sprawdzić informację w innych źródłach lub zwrócić się o pomoc do specjalisty z danej dziedziny. Przez Internet można skontaktować się z różnego rodzaju poradniami lub ekspertami również nieodpłatnie.

20 **DOBRE PRAKTYKI**

Odwiedzając stronę internetową należy zwróć uwagę na to, czy:

- jest podany autor treści,
- jest podany kontakt,
- jest podana data publikacji,
- na stronie znajduje się regulamin serwisu,
- strona jest powiązana z innymi podobnymi tematycznie stronami,
- strona jest podlinkowana przez inne witryny,
- jak wypowiadają się użytkownicy na stronie,
- czy jest prowadzona moderacja,
- czy strona jest aktualna.

21 Aktualność jest bardzo ważnym aspektem wiarygodności witryny. Informacje mogą być wiarygodne w pewnym okresie, po upływie czasu potrzebna jest aktualizacja. Przykładem może być strona z programem telewizyjnym, która z dnia na dzień musi być aktualizowana, aby przedstawiać wiarygodne informacje.

REGULAMIN SERWISÓW

Korzystając ze strony internetowej, należy zwrócić baczną uwagę na regulamin znajdujący się na stronie. Szczególnie kiedy strona wymaga rejestracji i podania danych osobowych. Może się zdarzyć, że tylko w regulaminie są podane informacje o sposobie płatności za dostęp, przechowywanie lub ściąganie plików. Mogą pojawić się koszty ukryte, o których nie ma informacji na stronie głównej portalu.

22 Regulaminy szczegółowo regulują odpowiedzialność administratorów witryny, ich obowiązki i prawa. Jest również napisane, czego oczekuje się w zamian od użytkownika danego portalu, kto będzie miał wgląd w jego dane osobowe itd.

23 **DOBRE PRAKTYKI**

Regulaminy szczególnie dużych portali często ulegają zmianie, należy zmiany te śledzić na bieżąco.

24 Regulamin witryny, portalu nie może być sprzeczny z prawem krajowym. Ze względu na transgraniczność Internetu, regulaminy popularnych serwisów ogólnoświatowych nie są dostosowane do polskich regulacji. Dominuje tutaj prawo państwa, gdzie znajduje się siedziba firmy.

25 W razie wątpliwości należy skontaktować się z administratorem portalu, nie korzystać z portali niewzbudzających zaufania. W spornych kwestiach i w razie problemów można zwrócić się do UOKiK.

OPIS ZJAWISKA
DIAGNOZA
DOBRE PRAKTYKI
ĆWICZENIA 39
ĆWICZENIA 40
ĆWICZENIA 41
ĆWICZENIA 42

CYBERPRZESTĘPCZOŚĆ I NADUŻYCIA

ZAGROŻENIA
DLA URZĄDZEŃ MOBILNYCH

Łukasz Tomczyk

OPIS ZJAWISKA

ROZPOZNANIE OBJAWY

1 WPROWADZENIE

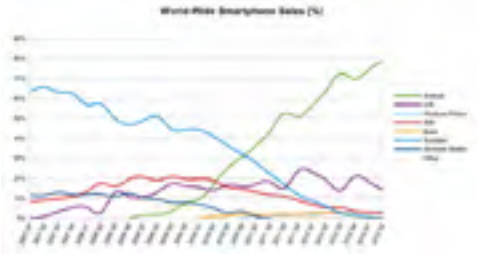
Telefony komórkowe, tablety, a zatem podstawowe urządzenia mobilne cieszą się od kilku lat olbrzymią popularnością. Telefony komórkowe wyposażone w ekran dotykowy na dobre przestały być synonimem luksusu, stając się podstawowym urządzeniem w ofercie operatorów telekomunikacyjnych. Paradoksalnie coraz trudniej znaleźć „tradycyjny" telefon z klawiaturą w formie guzików. Oczywiście jest sporo ofert z prostymi klawiaturami, lecz są one głównie dedykowane mniej wprawnym użytkownikom nowych mediów, a więc zazwyczaj seniorom, czy też osobom niepotrafiącym przyzwyczaić się do dotykowych ekranów.

2 Popularność telefonów dotykowych związana jest z ich nowoczesnym designem oraz przede wszystkim z możliwością o wiele większej konfiguracji systemu operacyjnego. Wgrywanie aplikacji, robienie zdjęć o relatywnie dużej rozdzielczości, możliwość łączenia się z Internetem w technologii N w każdym miejscu, gdzie znajduje się hotspot lub odpowiednio skonfigurowane łącze dostępowe pozwala dzięki smartfonom na bieżące bycie online, również w serwisach społecznościowych. Telefony tego typu pozwalają na proste wgrywanie rożnych aplikacji podnoszących użyteczność tego urządzenia do rangi komputera przenośnego. Bez problemu każdy z użytkowników smartfona jest w stanie odtworzyć czy też wygenerować różnego rodzaju dokumenty począwszy od plików w edytorach tekstu, poprzez pliki muzyczne, a kończąc na nieco bardziej złożonych multimediach. Obecnie telefony komórkowe stały się realnym przykładem zjawiska konwergencji mediów, na dodatek w sposób niezwykle przyjazny, do obsługi oraz konfiguracji dla użytkownika o przeciętnym poziomie kompetencji informatycznych. Ponadto systemy te pozwalają nawet na zamianę telefonu komórkowego w konsolę do gier, również o wyrafinowanej grafice, nieodstającej w żaden sposób od wyspecjalizowanych urządzeń przeznaczonych tylko i wyłącznie do gier.

3 ROZPOZNANIE PROBLEMU

Według danych serwisu E-marketer liczba używanych telefonów komórkowych na świecie przekroczyła w roku 2013 4,3 mld, z czego 672 mln działają na obszarze Europy. Z kolei najwięcej użytkowników znajduje się w Azji – 2,4 miliarda. Do 2017 roku liczba urządzeń ma wynieść około 5 miliardów[1]. Dodatkowo większość sprzedawanych telefonów komórkowych na świecie posiada system operacyjny Android. Na poniższym rysunku można zauważyć, że Android (właścicielem systemu jest firma Google) zdobywa coraz większą popularność kosztem innych mniej konfigurowalnych dla przeciętnego użytkownika systemów.

Rysunek 1. Sprzedaż telefonów komórkowych na świecie a rodzaj oprogramowania



Źródło: Potulski, *Ile jest androidów na świecie*, www.tabletowo.pl, 2013.

4 Ponadto istniejące do tej pory szczątkowe dane mówią o tym, że liczba urządzeń z aktywowanym systemem operacyjnym Android wynosi około 500 mln z tendencją do dziennej aktywa-

[1] P. Kreft, *Do 2017 roku liczba użytkowników telefonów komórkowych przekroczy... 5 mld!*, 2003 http://www.komputerswiat.pl/nowosci/sprzet/2013/40/do-2017-roku-liczba-uzytkownikow-telefonow-komorkowych-przekroczy-5-mld!.aspx data dostępu 02.01.2014.

cji rzędu 1,3 mln urządzeń[2]. Oczywiście nie wszystkie urządzenia są telefonami komórkowymi, ponieważ Android jest również głównym oprogramowaniem dedykowanym do coraz to popularniejszych tabletów.

5 Z danych GFK Polonia wynika, że coraz więcej osób posiada płaskie komputery z dotykową matrycą, zatem tendencja zakupu tabletów jest nowym trendem rozwojowym w sektorze IT. Z badań wynika bowiem, że sprzedaż tabletów w pierwszym półroczu 2013 r., względem 2012, wzrosła o 141,4%. Do końca 2013 r. sprzedaż tabletów na polskim rynku IT według prognoz oscylowała w przedziale od 900 tys. do 1,1 mln sztuk[3], z kolei w roku poprzednim zakupiono w Polsce 880 tys. tych urządzeń (IBS News, 2013).

6 Niestety wzrost sprzedaży urządzeń typu tablet lub smartfon nie jest skorelowany z wiedzą ich użytkowników w zakresie poprawnego użytkowania, zabezpieczenia oraz z ilością powstającego złośliwego oprogramowania. Istnieje spora grupa korzystających z urządzeń mobilnych, zaskoczonych pytaniem o posiadanie antywirusa w urządzeniu przenośnym. Niestety wielu użytkowników nowych technologii jest przekonanych, że urządzenia te nie są zagrożone wirusami, programami szpiegującymi, wykradającymi poufne dane, czy też zamieniającymi smartfon w komputer zombie, atakujący serwery lub inne urządzenia elektroniczne.

7 DIAGNOZA

Specjaliści agencji interaktywnej Heuristic opisując szkodliwość złośliwych aplikacji podkreślili, że złośliwe oprogramowanie potrafi przy pobraniu zarażonej aplikacji (np. pliku z grą na smartfona) uaktywnić się w systemie bez wiedzy właściciela, a następnie wykraść dane z telefonu i przesłać je bez zgody na wskazany serwer. Ponadto niektóre wirusy są niezwykle uciążliwe, ponieważ wyświetlają niechciane reklamy, a ich usunięcie jest możliwe dzięki specjalistycznemu „wyczyszczeniu" systemu Android. Z kolei inne wirusy potrafią namierzać dany telefon według położenia geograficznego i kontrolować jego funkcje. Do najbardziej złośliwych dla portfela użytkownika należą wirusy rozsyłające esemesy pod specjalne numery premium (wysoko płatne). Dodatkowo wirusy potrafią również przechwytywać korespondencję esemesową oraz wszystkie poufne dane[4] np. loginy i hasła do kont bankowych, portali społecznościowych czy też sklepów internetowych oraz portali aukcyjnych.

8 DOBRE PRAKTYKI

Warto zatem uwzględniając powyższe konteksty uwrażliwić użytkowników popularnego systemu Android w zakresie wgrania w system operacyjny oprogramowania skutecznie zabezpieczającego urządzenie mobilne przed przykrymi następstwami opisanego wcześniej malwaru. Oczywiście aplikacje chroniące smartfony i tablety dzielą się na dwie elementarne kategorie, a więc płatne i bezpłatne. Wśród najbardziej popularnych można wymienić następujące aplikacje antywirusowe:

- avast! Mobile Security (http://www.avast.com/pl-pl/free-mobile-security)

[2] P. Pająk, *Ile jest Androidów na świecie? Tak naprawdę nie wiadomo*, 2013 http://www.spidersweb.pl/2013/03/ile-jest-androidow-na-swiecie-tak-naprawde-nie-wiadomo.html datad ostępu 03.01.2014.

[3] K. Pura, *Sprzedaż tabletów w pierwszym półroczu 2013 roku wzrosła o 141,4%*, 2013 http://www.tabletowo.pl/2013/10/29/sprzedaz-tabletow-w-pierwszym-polroczu-2013-roku-wzrosla-o-1414/ data dostepu 03.01.2014.

[4] Heuristic, *Wirusy w Androidzie - czy należy się ich bać i jak się zabezpieczać*, 2013, http://www.heuristic.pl/blog/e-technologie/172.html data dostępu 02.01.2014.

- Norton Mobile Security (http://pl.norton.com/norton-mobile-security/)
- AVG Anti-Virus Free (http://www.avg.com/pl-pl/for-mobile)
- Zoner AntiVirus (http://www.zonerantivirus.com/)
- Lookout Security & Antivirus (https://www.lookout.com/pl)
- G Data Internet Security for Android (https://www.gdata.pl/darmowy-download,pobierz-antywirusa,3)
- Eset mobile security (http://www.eset.pl/Dla_domu_i_firmy/Produkty/ESET_Mobile_Security_for_Android)

9 Poniżej zaprezentowano metodą krok po kroku algorytm wgrania i zainstalowania aplikacji chroniącej urządzenia mobilne na przykładzie darmowego oprogramowania avast! Free Mobile Security. W pierwszym etapie użytkownik powinien mieć utworzone konto w systemie Google, a następnie zalogować się na stronie Google Play (play.google.com) z poziomu urządzenia mobilnego i odszukać daną aplikację internetową. Po wybraniu programu Avast należy kliknąć na przycisk „zainstaluj".

10 Po wybraniu przycisku „zainstaluj" pojawia się standardowe pytanie ze strony twórców oprogramowania o poziom uprawnień, jakie użytkownik telefonu chce przydzielić aplikacji. Tutaj można wybrać opcję „domyślne ustawienia", jednakże użytkownik dbający o swoje dane powinien zapoznać się i zastanowić nad przydzielanymi uprawnieniami. Kolejno w miejscu przycisku „zainstaluj" wyświetlony zostaje komunikat o procesie postępu instalacji, który wyrażany jest procentowo.

Rysunek 2. Proces instalacji oprogramowania Avast

Źródło: opracowanie własne

11 Po zakończeniu instalacji oprogramowanie może zapytać ponownie użytkownika, czy zapoznał się z umową licencyjną oraz zaproponować wersję płatną z opcjami zaawansowanymi. Dzięki opcji zaawansowanej użytkownik uzyskuje możliwość m.in. blokowania reklam na stronach internetowych oraz archiwizowania włamań oraz prób włamań na telefon komórkowy. Po wybraniu opcji „zostań" przy wersji darmowej ukazuje się menu główne aplikacji avast Mobile!

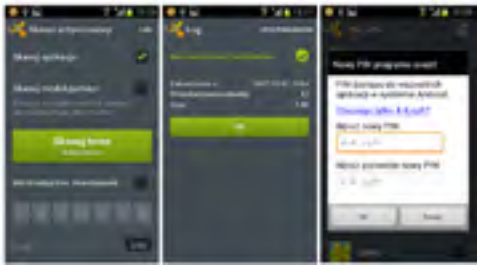
Rysunek 3. Proces konfiguracji oprogramowania

Źródło: opracowanie własne

12 W menu głównym użytkownicy mogą również dograć dodatkowe opcje, np. (Anti-Theft) związane ze zdalną kontrolą skradzionego telefonu lub wykonywaniem kopii zapasowej danych wrażliwych w telefonie (backup), a więc kontaktów, korespondencji, plików. Obie opcje są bezpłatne.

13 Proces skanowania telefonu może odbywać się w tle, o czym świadczy ikona programu Avast (pomarańczowa) z lewej strony na wysokości wskaźników sygnału sieci oraz stanu naładowania baterii czy też wyświetlanej godziny, lecz również może być o wiele precyzyjniej i dogłębniej zaplanowany przy uwzględnieniu dni tygodnia. Dodatkowo użytkownik otrzymuje możliwość zabezpieczenia uruchomienia wybranych aplikacji poprzez kod PIN składający się z od 4 do 6 cyfr. W ten oto sposób można zabezpieczyć np. wejście do galerii systemowej lub innych wrażliwych zasobów urządzenia mobilnego.

Rysunek 4. Dodatkowe opcje oprogramowania



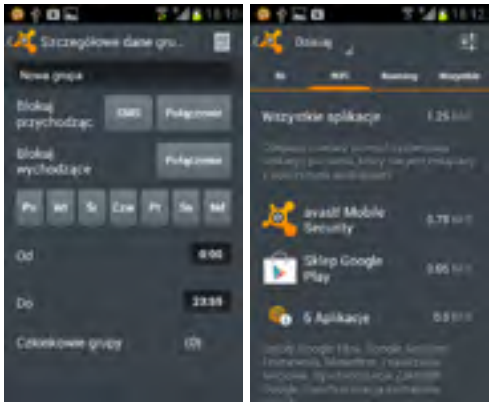
Źródło: opracowanie własne

14 Wśród innych interesujących opcji aplikacji należy podkreślić blokowanie połączeń telefonicznych oraz połączeń tekstowych w wybranych dniach i porach dla poszczególnych grup. Grupy tworzone są poprzez dodanie kontaktów z listy książki telefonicznej lub z bieżącej listy połączeń. Użytkownik, posiadając pakiet Avast, uzyskuje możliwość monitorowania statusu transferu danych, jakie realizują wybrane aplikacje. Dodatkowo monitoring przesyłu danych kategoryzuje transfer według typu połączeń.

15 We wspomnianej wcześniej wersji premium użytkownik otrzymuje także możliwość uzyskania informacji o wgranych aplikacjach, które zbierają informacje o: lokalizacji, zachowaniu użytkownika w sieci, pokazują banery reklamowe, odczytują dane identyfikacyjne oraz posiadają dostęp do wiadomości i kontaktów.

16 Na koniec warto podkreślić, że część aplikacji antywirusowych instalowana jest nie tylko z poziomu Google Play, lecz jest możliwe pobranie pliku instalacyjnego na pamięć telefonu i uruchomienie kreatora instalacji z pobranego pliku apk (odpowiednika rozszerzenia exe w systemie operacyjnym Windows).

Rysunek 5. Blokowanie połączeń i esemesów oraz sprawdzenie transferu danych w aplikacji



Źródło: opracowanie własne

ĆWICZENIA 43

ĆWICZENIA 44

BIBLIOGRAFIA:

Kreft P. (2013), *Do 2017 roku liczba użytkowników telefonów komórkowych przekroczy... 5 mld!*, http://www.komputerswiat.pl/nowosci/sprzet/2013/40/do-2017-roku-liczba-uzytkownikow-telefonow-komorkowych-przekroczy-5-mld!.aspx, data dostępu 02.01.2014.

Potulski P. (2013), *Jak Android zdominował świat*, http://androidnow.pl/jak-android-zdominowal-swiat/, data dostępu 03.01.2014.

Pająk P. (2013), *Ile jest Androidów na świecie? Tak naprawdę nie wiadomo*, http://www.spidersweb.pl/2013/03/ile-jest-androidow-na-swiecie-tak-naprawde-nie-wiadomo.html, data dostępu 03.01.2014.

Pura K. (2013), *Sprzedaż tabletów w pierwszym półroczu 2013 roku wzrosła o 141,4%*, http://www.tabletowo.pl/2013/10/29/sprzedaz-tabletow-w-pierwszym-polroczu-2013-roku-wzrosla-o-1414/, data dostępu 03.01.2014.

IBS News (2013), IDC: *Sprzedaż tabletów w Polsce wzrosła 4-krotnie r/r do 375 tys. sztuk w I kw.*, http://wyborcza.biz/Gieldy/1,132329,13971653,IDC__Sprzedaz_tabletow_w_Polsce_wzrosla_4_krotnie.html#ixzz2pFxbBqGG, data dostępu 02.01.2014.

Heuristic (2013), *Wirusy w Androidzie – czy należy się ich bać i jak się zabezpieczać*, http://www.heuristic.pl/blog/e-technologie/172.html, data dostępu 02.01.2014.

CMENTARZE DANYCH

Wojciech Duranowski
Arkadiusz Durasiewicz

OPIS ZJAWISKA

WPROWADZENIE

1 Kontekst prawny

Ustawa z dnia 29 sierpnia 1997 r. ze zm. o ochronie danych osobowych (Dz. U. nr 133, poz. 883, tekst jedn. Dz.U. nr 101, poz. 926) nie przesądza w sposób jednoznaczny kwestii, czy przetwarzanie danych osobowych osób zmarłych objęte jest ustawą o ochronie danych osobowych.

2 Biorąc pod uwagę konstrukcje powyższej ustawy jako całości, jak i analizując jej poszczególne przepisy, należy dojść do wniosku, że ochrona dotyczy wyłącznie danych osobowych osób żyjących. Takie wnioski można wyciągnąć na podstawie konstrukcji praw sformułowanych w ustawie, dotyczących m.in. praw dostępu do danych, sprostowania danych, zgody osoby, której dane dotyczą, polegającej na złożeniu oświadczenia woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie (art. 7 ust. 5). Prawa te przysługują wyłącznie osobie, której dane dotyczą, a więc osobie żyjącej.

3 Gdyby intencją ustawodawcy była ochrona informacji dotyczących zmarłych, znalazłoby to niewątpliwie wyraźne odzwierciedlenie w regulacji ustawowej. Takie regulacje istnieją np. jeśli chodzi o ochronę autorskich dóbr osobistych przysługujących po śmierci autora innym osobom. Tak więc z analizy art. 1, 6, 7 ustawy o ochronie danych osobowych wynika, że przedmiotem ochrony są jedynie osoby fizyczne identyfikowalne. Natomiast ochronie nie podlegają dane zmarłych. Aczkolwiek nie jest to w ustawie wyrażone expressis verbis.

4 Przechodząc do zagadnienia, kto jest właścicielem danych osobowych osób zmarłych, należy rozważyć problem dotyczący ochrony dóbr osobistych człowieka, które pozostają pod ochroną prawa cywilnego (ustawa z dnia 23 kwietnia 1964 r., Dz. U. nr. 16 poz. 97 ze zm.).

5 Zgodnie z brzmieniem art. 23 K.c.:

> „Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach”[1].

6 Należy stwierdzić, że dobra osobiste powstają, ulegają zmianie i zanikają w wyniku rozwoju stosunków społecznych i kształtowania się świadomości społecznej, określonego porządku prawnego, moralnego, obyczajowego oraz utrwalania się poglądów na to, co w danym okresie rozwoju jest dla jednostki wartością, którą należy objąć ochroną prawną.

7 Art. 23 K.c. nie określa definicji dóbr osobistych, jak również nie zawiera zamkniętego katalogu tych dóbr. Dobra osobiste to pewne wartości o charakterze niematerialnym, łączące się ściśle z człowiekiem. Prawu polskiemu nie jest znany wyczerpujący katalog chronionych dóbr osobistych. Lista ta jest ciągle poszerzana pod wpływem judykatury i doktryny.

8 Powszechnie akceptowany jest pogląd uznający za dobro osobiste kult pamięci po zmarłej osobie bliskiej. Przyjmowana powszechnie jako dobro osobiste ochrona czci osoby zmarłej nie polega na przejściu prawa do czci

[1] Kodeks cywilny, red. prof. Zbigniew Radwański, Warszawa 2012.

przysługującego zmarłemu, lecz jest własnym integralnym prawem najbliższych członków rodziny zmarłego. Trzeba zwrócić uwagę na fakt, że ze sferą kultu po zmarłej osobie bliskiej mogą wiązać się również inne chronione dobra osobiste związane ze sferą życia prywatnego, rodzinnego czy też ze sferą intymności.

9 Należy stwierdzić, że nie każde naruszenie dobra osobistego jest równoznaczne z naruszeniem prawa. Okoliczności wyłączające bezprawność zachowania, zagrożenia lub naruszenia dobra osobistego pozbawiają ochrony osobę dotkniętą naruszeniem.

Do takich okoliczności zalicza się między innymi zgodę uprawnionego.

Zgoda uprawnionego kwalifikowana jest jak czyn zgodny z prawem podobny do czynności prawnych, zbliżonych do oświadczenia woli. Zgoda, o której mowa powyżej, może być wyrażona przez osobę żyjącą na uruchomienie bazy danych dotyczących jej osobiście. Osoba uprawniona (bliska) może również wyrazić zgodę na wprowadzenie do bazy danych osoby zmarłej. Zgłoszenie traktować należy równocześnie jako wyrażenie zgody na podane w Internecie warunki dotyczące umieszczenia osoby w bazie danych wirtualnego cmentarza.

10 ROZPOZNANIE ZJAWISKA

Pojawienie się internetowych nekropolii to efekt postępującej digitalizacji naszego życia – jeśli żyjemy online, to coraz więcej osób chce zostawić po sobie wirtualny ślad również po śmierci. Wirtualny cmentarz to również miejsce, które można bez problemu odwiedzić o każdej porze dnia i nocy.

11 **Wirtualny cmentarz to swoisty serwis społecznościowy, w którym można stworzyć profil zmarłego wraz z jego zdjęciami, filmami czy wspomnieniami najbliższych**. W zależności od serwisu profile przypominają realne nagrobki albo całkowicie odchodzą od konwencji cmentarza, pozwalając na umieszczanie informacji o zmarłym np. w przestrzeni kosmicznej. Na wirtualnym grobie możemy złożyć kwiaty i zapalić świeczkę.

12 Jak szacuje amerykańska spółka I-Post-mortem Ltd.[2], właściciel serwisów I-tomb.net oraz I-memorial.com będących serwisami pamięci o zmarłych, rynek na wirtualne usługi pogrzebowe oraz serwisy przechowujące pamięć o tych, którzy odeszli, jest olbrzymi. Populacja ludzi w ciągu ubiegłego wieku wzrosła z 1,6 mld w 1900 roku do 7 mld w roku 2011, podczas gdy tylko w 2011 roku na całym świecie zmarły 54 mln osób. Ich żyjący bliscy są potencjalnymi klientami wirtualnego cmentarza. W praktyce rynek jest jednak znacznie mniejszy, zwłaszcza w takich krajach jak Polska, chociaż i u nas wirtualne cmentarze już działają.

13 Stworzenie serwisu Wirtualnycmentarz.pl[3] kosztowało ok. 200 tys. zł. Pieniądze te zostały przeznaczone przede wszystkim na prace programistyczne i wynagrodzenia grafików, którzy stworzyli wirtualne pomniki dla ludzi oraz zwierząt, przygotowali również kilka wariantów cmentarzy, na których można zaznaczyć pamięć o bliskich zmarłych.

14 Na wirtualnym cmentarzu można pochować każdego, nie ma bowiem żadnych narzędzi, które pozwalałyby zweryfikować, czy cyfrowy pomnik został postawiony osobie zmarłej czy też żywej, którą ktoś „życzliwy" najchęt-

[2] http://i-postmortem-limited.advertory.com, data dostępu 28.12.2013.

[3] http://www.wirtualnycmentarz.pl, data dostępu 10.01.2014.

niej wysłałby na tamten świat. Oczywiście, najpierw trzeba zapłacić za wirtualny grób i inne artefakty. Jednak jeśli ów żywy, który został pochowany na e-cmentarzu, znajdzie swój wirtualny nagrobek, to może zwrócić się z prośbą o jego usunięcie i administrator ma obowiązek go zlikwidować.

15 **ADMINISTROWANIE DANYMI**

Jeśli chodzi o kwestie administrowania i ochrony danych osobowych osób zmarłych, to polskie prawo nie przesądza w sposób jednoznaczny kwestii, czy przetwarzanie danych osobowych osób zmarłych objęte jest ustawą o ochronie danych osobowych. Analiza prawna wskazuje, że właścicielem danych osobowych osób zmarłych są osoby do tego uprawnione, czyli najczęściej ich bliscy, którzy mogą wprowadzać te dane do bazy wirtualnego cmentarza.

16 Kwestia związana z kontem internetowym zmarłej osoby bądź danymi, które po sobie pozostawiła jest sprawą bardzo delikatną i każdy z zarządców portalu społecznościowego podchodzi do niej w sposób zindywidualizowany.

17 W wypadku posiadania konta na Facebooku należy wypełnić specjalny wniosek, który po rozpatrzeniu przez odpowiednich przedstawicieli serwisu pozwoli stworzyć z konta tzw. tablicę pamiątkową. Należy także dołączyć dowód zgonu; może to być link do nekrologu w gazecie. Bliscy i przyjaciele mogą w dalszym ciągu umieszczać wpisy na Ścianie, ale usunięte zostają na przykład wszelkie informacje kontaktowe. Konto staje się dostępne jedynie dla przyjaciół. Co ważne – zgłoszenie może zostać wysłane nie tylko przez członków najbliższej rodziny, lecz także przez znajomych, przyjaciół czy współpracowników.

18 Facebook udostępnia też aplikację If I Die. Nakładka umożliwia pozostawienie ostatniej wiadomości, którą portal opublikuje po otrzymaniu zgłoszenia o twojej śmierci. – Prawdopodobnie myślisz, że nie zaplanowałeś spotkania ze śmiercią, ale ona czeka tuż za rogiem – głosi reklama aplikacji okraszona dziecięcą, pozytywkową muzyką. – Możesz zostawić po prostu pożegnanie, ulubiony żart, długo skrywany sekret, ukoić zadrę lub udzielić poważnej rady – podsuwa pomysły lektor. Można też zostawiać wiadomości do konkretnych osób.

19 O krok dalej poszli w marcu twórcy aplikacji LivesOn. Aplikacja przeanalizuje historię wiadomości i odtworzy mapę zainteresowań użytkownika. Na tej podstawie wybierane są zagadnienia i artykuły, którymi interesował się użytkownik, aby zasymulować jego osobowość. Gdy użytkownik umiera, sztuczna inteligencja wcieli się w niego, komentując i publikując nowe wpisy. LivesOn umożliwia też wybranie dziedzica, który zdecyduje o przyszłości konta na Twitterze.

20 MySpace zezwala na zgłoszenie konta zmarłej osoby jedynie najbliższej rodzinie. Może okazać się to problematyczne, jeśli np. rodzice nie poruszają się swobodnie w Internecie lub po prostu nie wiedzą o koncie na MySpace. Profil może zostać usunięty lub zachowany wedle życzenia. Należy jednak przesłać akt zgonu lub pogrzebu na wskazany adres mailowy. Do tego trzeba dołączyć MySpace ID razem z wytycznymi, co do profilu (usunąć, zachować, usunąć jedynie pewne treści).

21 Posiadanie konta Google ma swoje plusy – logowanie do wielu usług następuje za pośrednictwem tych samych danych, a w wypadku śmierci bliskiej osoby wszystkie serwisy są dezaktywowane. Na wskazany adres należy przesłać (lub przefaksować) swoje dane kontaktowe, adres Gmail osoby zmarłej, akt zgonu i do-

wód pokrewieństwa. Rozpatrzenie prośby ma trwać do 30 dni. Nie ma niestety innej możliwości, niż skontaktowanie się bezpośrednio z Mountain View.

22 W kwietniu 2013 r. Google umożliwił spisanie e-testamentu. Wystarczy posiadanie poczty elektronicznej Gmail: to w ustawieniach konta Google (google. com/settings/account) można wybrać, co się z nim stanie po śmierci. Oczywiście firma z Mountain View jest taktowna i nie pyta użytkownika, kiedy umrze. Usługa nazywa się Menedżer Nieaktywnego Konta i pozwala zdecydować, komu przekazać prawa do swoich danych, jeśli przez rok nie będzie się w nim logowało. Można zostawić kontakty do maksymalnie dziesięciu osób lub zdecydować o tym, aby skasować swój ślad z sieci raz na zawsze. Nowa funkcja będzie dotyczyć poczty elektronicznej, serwisu społecznościowego Google Plus oraz innych kont osobistych.

23 Użytkownik będzie mógł zdecydować o wykasowaniu przechowywanych przez niego danych lub przekazaniu ich konkretnej osobie. Użytkownicy będą mogli wybrać opcję, w której ich dane zostaną usunięte z serwerów po trzech, sześciu, dziewięciu lub dwunastu miesiącach lub przekazane zostaną wybranej wcześniej osobie.

24 Rozwiązania wprowadzane przez Google spowodowane są rosnącą liczbą danych umieszczanych przez użytkowników w przestrzeni cyfrowej.

25 Jeśli chodzi o konto na Naszej Klasie, to także należy skontaktować się z przedstawicielami serwisu. Profile oznaczone „Ś.p." mają być usuwane w przyspieszonej procedurze, ale generalnych wytycznych, jak należy postępować (przynajmniej na razie) nie ma. Każdy przypadek rozpatrywany jest indywidualnie.

26 Zasady serwisu Gazeta.pl nie przewidują udostępnienia hasła do konta pocztowego osobom postronnym. W wyjątkowych przypadkach nie jest to jednak wykluczone – wówczas należy udowodnić swoje pokrewieństwo z osobą zmarłą, przedstawiając stosowny dokument. Dotychczas, podobnych przypadków do tej pory nie było. Zdarzają się za to prośby rodziny o zablokowanie loginu, tak aby był on już na zawsze przypisany do konkretnej osoby i nie trafiał z powrotem do puli.

27 Regulamin serwisu Onet przedstawia zagadnienie ewentualnego przekazania hasła w dziale Prywatność: Onet.pl udostępnia każdemu użytkownikowi stronę profilową http://profil.onet.pl/, dostępną po autoryzacji. Strona ta pozwala na wgląd, modyfikację i usunięcie posiadanych przez Onet.pl danych osobowych o użytkowniku. W przypadku, gdyby użytkownik uznał takie rozwiązanie za niewystarczające, może zwrócić się pisemnie do Onet.pl S.A., ul. G. Zapolskiej 44, 30-126 Kraków[4].

28 Regulamin Interii zakłada, że hasło dostępu zmarłego użytkownika nie będzie ujawnione. Na własne życzenie można jednak zgłosić się do serwisu o jego udostępnienie innym po naszej śmierci.

29 Zanim Gadu Gadu wprowadziło dożywotnią pulę numerów prawdopodobnie większości użytkowników zdarzyło się odkryć, że jedna z osób na jego liście kontaktów nie jest tą, której się spodziewali. Wcześniej bowiem, jeśli dany użytkownik nie logował się przez pół roku na swoje konto, numer wygasał i bywał przekazany komuś innemu. W przypadku, gdy zmarł jeden z naszych znajomych a jego numer został przekazany innej oso-

[4] http://poczta.onet.pl/oferta/1093055,regulamin.html

bie, można było mieć wrażenie komunikacji z użytkownikiem widmem. Teraz jednak numery już nie wygasają, a samo GG nie jest jedynie komunikatorem, lecz zapewnia także dostęp do poczty elektronicznej. Co więc w sytuacji, gdy dana osoba umiera? Można próbować zwrócić się do GG, ponieważ każdy przypadek ma być traktowany indywidualnie, ale trzeba się liczyć z koniecznością przedstawienia aktu zgonu oraz udowodnienia stopnia pokrewieństwa.

30 Sieć zapewnia także szereg usług, które samoczynnie przekażą cyfrową spuściznę bliskim zmarłego. Do takich należy Zostaw Ślad – serwis, który umożliwia zapisanie haseł dostępu do różnych portali, ważnych dokumentów i innego rodzaju plików, a następnie po śmierci przekazanie ich spadkobiercy. W zależności od wyboru opcji (profil darmowy, płatny), zmienia się także liczba pełnomocników. Jest to polski odpowiednik serwisu Legacy Locker, który oferuje bardzo podobne usługi.

31 PODSUMOWANIE

Kwestia, co robić z danymi użytkownika po jego śmierci, coraz pilniej domaga się rozwiązania w czasach, gdy wiele osób korzysta z serwisów internetowych i zamieszcza w nich tysiące informacji na swój temat.

32 Okazuje się jednak, że informacje dotyczące osób zmarłych znacznie trudniej chronić, niż dane ich żyjących następców. Jak zareagować na wieść, że takie dane naszych bliskich zmarłych są dowolnie przetwarzane, czyli między innymi w nieograniczony sposób udostępniane osobom trzecim?

33 Sposób opisywania, czym są dane osobowe oraz brak zgodności w doktrynie co do czasu trwania ochrony sprawiają, że informacje dotyczące zmarłych znacznie trudniej chronić niż dane osób żyjących. Każdy człowiek ma prawo do ochrony dotyczących go danych osobowych – konstytucyjna zasada prawnej ochrony życia a przy tym jednoznacznie wskazuje na związek osoby fizycznej i prawa do ochrony jej danych osobowych. Zmarły nie jest już jednak podmiotem prawa, więc nie można twierdzić, iż istnieje jego prawo do ochrony danych osobowych. Otwarty pozostaje problem przejścia tego prawa (lub prawa w treści podobnego) na spadkobierców.

34 W obecnym stanie prawnym nie sposób uzasadnić istnienia prywatnoprawnej kontroli nad przetwarzaniem danych osobowych zmarłego. Zasadniczym składnikiem takiej kontroli byłoby rozbudowane prawo do informacji o tym, czy zbiór danych osobowych spadkodawcy istnieje, jaki jest cel, zakres i sposób przetwarzania tych danych, kto jest źródłem informacji przetwarzanych w zbiorze, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej.

BIBLIOGRAFIA:

Dziak P., *Bezpieczne korzystanie z Internetu*, Wiedza i Praktyka, Warszawa 2012.

Kifner T., *Polityka bezpieczeństwa i ochrony informacji*, Warszawa 2011.

Kodeks cywilny, red. Radwański Z., Wyd. Beck, Warszawa 2012.

Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2013.

SERWISY INTERNETOWE:

www.onet.pl, www.interia.pl, www.wp.pl
www.facebook.com, www.twitter.com
www.myspace.com, www.google.pl
www.nk.pl

SZCZEGÓŁOWY
PROGRAM SZKOLENIA

Łukasz Tomczyk

SZCZEGÓŁOWY PROGRAM SZKOLENIA – CYBERPRZESTĘPSTWA I NADUŻYCIA	
Sposób realizacji	W sali komputerowej podłączonej do sieci Internet z podłączonym rzutnikiem multimedialnym
Materiały	**Materiały dydaktyczne dla uczestników szkolenia:** a) materiały szkoleniowe (finalna wersja produktu), b) aplikacje komputerowe typu VISIKID, Beniamin, materiały z YouTube, c) prezentacja PPT.
Treści merytoryczne	**blok tematyczny:** **Cyberprzestępczość i nadużycia (8h dydaktycznych)** 1. **Portfel** Bezpieczne zakupy przez Internet Rozumienie szyfrowania (połączenia SSL) Rozumienie zjawiska Phishingu Bankowość elektroniczna Usługi „krypto" płatne Aukcje internetowe – super promocje Zasady bezpiecznych zakupów internetowych **2. Komputer** Panel sterowania Wyszukiwania ukrytych plików w komputerze (mp3, avi, exe) Dodaj/usuń programy Rejestr systemu Windows Załączniki/złośliwe oprogramowanie/spam USB/Dyski zewnętrzne – wirusy komputerowe Botnety Inne sprzęty w domu/pracy/szkole – Smartfon (kopie numerów telefonów w sieci, antywirus dla smartfona) Antywirusy/Firewall/filtry rodzicielskie na przykładzie VISIKID, Beniamin Aktualizacje systemu oraz opcje panelu sterowania Kopie zapasowe – backup, pendrive, dysk przenośny, chmura Hasła (silne hasła) – proste metody na generowanie silnych haseł internetowych Bezpieczna przeglądarka dla dziecka BEST **3. Prywatność** Serwisy społecznościowe (bezpieczny profil, spam, cyberprzemoc) Zgłaszanie nadużyć w serwisach społecznościowych Ujawnianie informacji i pozostawianie śladów (adres IP, serwisy PROXY, adres Mac) Niebezpieczne kontakty poprzez e-mail czy serwisy społecznościowe Serwis geolokacji „Gdzie jest dziecko" **4. Treści** Prawa autorskie – pobieranie treści Peer-to-peer (pobieranie i udostępnianie plików) Treści szkodliwe i nielegalne (serwisy warezowe, zasada działania portali typu chomikuj.pl) Krytyka źródła Regulaminy w sklepach internetowych, serwisach udostępniających pliki E-nauczanie i e-niebezpieczeństwa na przykładzie portalu Fundacji Dzieci Niczyje Szukanie pomocy w Internecie – Dyżurnet Destruktywne gry komputerowe

Obszary	Efekty kształcenia
Wiedza zdobyta w czasie zajęć	W wyniku przeprowadzonych zajęć, Uczestnik powinien być w stanie: - rozróżniać legalne i nielegalne oprogramowanie, - znać pojęcia odnoszące się do bezpieczeństwa w sieci, - rozróżniać aplikacje i urządzenia służące pobieraniu loginów i haseł, - znać zasady bezpiecznych zakupów oraz korzystania z serwisów społecznościowych, - wskazać zasady bezpiecznego korzystania ze sprzętu komputerowego i stron z grupy „podwyższonego ryzyka”.
Umiejętności zdobyte w czasie zajęć	W wyniku przeprowadzonych zajęć, Uczestnik powinien umieć: - konfigurować komputer pod względem zwiększenia swojego bezpieczeństwa, - zabezpieczać komputer w zakresie kontroli rodzicielskiej, - odnaleźć serwisy z bezpiecznym oprogramowaniem, - instalować i konfigurować oprogramowanie antywirusowe i antyszpiegujące, - sprawdzić destruktywność zainstalowanych gier komputerowych, - przechowywać w sposób bezpieczny dane komputerowe.
Forma zajęć	**Metody szkolenia:** Wykład, ćwiczenia, burza mózgów, praca z komputerem, quiz, pokaz multimedialny, instruktaż, metoda problemowa Formy: indywidualna, grupowa
Metody prowadzenia zajęć	Wykład, ćwiczenia, burza mózgów, praca z komputerem, quiz, pokaz multimedialny, instruktaż, metoda problemowa
Zalecane ćwiczenia	Ćwiczenia 19-43 znajdujące się w module *Kształcenie*
Sprawdzenie efektów szkolenia	Ankiety, testy kompetencyjne

METODY KSZTAŁCENIA PRACOWNIKÓW SŁUŻB SPOŁECZNYCH

METODY KSZTAŁCENIA
PRACOWNIKÓW SŁUŻB SPOŁECZNYCH

Józef Bednarek

1 **WPROWADZENIE**

Przedstawione w tej części treści dotyczą ogólnych założeń teoretycznych i wskazują działania, które należy realizować w ramach metodyki prowadzonych zajęć, przestrzegając określone zasady ogólne i specyficzne. Prowadzone analizy mają charakter uniwersalny, choć w maksymalnym stopniu ukierunkowane są na metodykę kształcenia pracowników socjalnych (będących także uczniami dorosłymi), przystępujących do realizacji zajęć dydaktycznych związanych z nową rolą i miejscem zagrożeń cyberprzestrzeni w polityce społecznej, a więc zupełnie nowym, wcześniej nieznanym obszarem wiedzy do tej pory niebędącej przedmiotem kształcenia (szkolenia), badań i opracowania metodycznego. Każda osoba prowadząca zajęcia może je przygotować na podstawie nw. treści, przygotowując optymalny plan zajęć i starając się je w sposób celowy, świadomy, przemyślany, racjonalny i skuteczny realizować, uwzględniając wiele różnorodnych uwarunkowań.

DYDAKTYKA KSZTAŁCENIA DOROSŁYCH – PODSTAWĄ METODYKI NAUCZANIA

2 **Charakterystyka dydaktyki i metodyki kształcenia**

Skąd zatem wynika znaczenie dydaktyki, a w jej ramach nauczania-uczenia się? Od właśnie tego przełomu dydaktykę utożsamiano nie tylko z teorią nauczania, ale także teorią uczenia się (analiza czynności uczniów wykonywanych w szkole). Dziś uważa się, że proces nauczania wiąże się ściśle z uczeniem się, tworząc zintegrowaną całość, a ściślej proces nauczania-uczenia się. Dydaktykę traktuje się jako naukę o nauczaniu i uczeniu się. Jest ona zatem zbiorem obserwacji, twierdzeń i hipotez dotyczących zjawisk, zależności i prawidłowości uczenia się oraz sposobów analizy i przekształcenia tych procesów (zjawisk).

3 **Dydaktyka należy do nauk teoretycznych i praktycznych (metodyka), gdyż zajmuje się badaniem działalności osób nauczających i uczących się (proces kształcenia)**, celów, treści, metod, form, zasad i środków (technologii informacyjnych) oraz organizacji kształcenia, jak również badaniem społecznego i materialnego środowiska oraz psychologiczno-społecznych uwarunkowań, w których się ta działalność odbywa. Jej głównym zadaniem jest ustalenie zależności warunkujących działalność dydaktyczną.

4 **Dydaktyka (metodyka) bada zachowania celowe nauczycieli (prowadzących zajęcia) i uczniów, w tym także dorosłych**[1] tzn. te, które zmierzają do dokonania jakichś zmian w uczniach. Wyniki badań dydaktycznych informują mianowicie o tym, jak za pomocą opisanego systemu zabiegów i środków uzyskać zmianę danego stanu w stan pożądany. Z tych powodów dydaktyka jest nauką, która nie może zawierać tylko wypowiedzi teoretycznych, lecz zarówno zdania teoretyczne, jak i oceniające oraz normatywne. Nie można jej więc uważać za naukę wyłącznie praktyczną czy stosowaną, jest bowiem nauką teoretyczno-praktyczną.

Dydaktyka jako dyscyplina naukowa należy do nauk indukcyjnych, zakłada się, że jej twierdzenia, wywiedzione w drodze indukcji, mogą okazać się zawodne i – jako takie – mogą zostać odwołane, podobnie jak w naukach przyrodniczych i humanistycznych. Jednakże oprócz twierdzeń indukcyjnych nauki te, a więc i dydaktyka, posługują się twierdzeniami o rodowodzie dedukcyjnym. Są to bądź zdania definicyjne, bądź twierdzenia czerpane z nauk matematycz-

[1] Por. Cz. Kupisiewicz, *Dydaktyka ogólna*, Oficyna Wydawnicza GrafPunkt, Warszawa 2000; Cz. Kupisiewicz, *Podstawy dydaktyki ogólnej*, Wyd. Nauk. PWN, Warszawa 2010; Cz. Kulisiewicz, *Wybrane problemy teorii i praktyki pedagogicznej na progu XXI w.*, IBE, Ryki 2003. J. Półturzycki, *Akademicka edukacja dorosłych*, Wyd. Uniwersytetu Warszawskiego, Warszawa 1994.

nych. Oprócz nich w naukach indukcyjnych występują oparte na indukcji zdania spostrzeżeniowe. W wypadku dydaktyki odnoszą się one do przyjętych w programie kształcenia rzeczy i zdarzeń, swoją treść zaś czerpią z bezpośrednich spostrzeżeń zmysłowych.

5 **Dydaktyka jako nauka dostarcza wiedzy o stanie rzeczy istniejącym w obrębie przedmiotu jej badań.** Spełnia w ten sposób funkcję diagnostyczną (poznawczą), polegającą na gromadzeniu wiedzy o przedmiocie i ocenie obiektywnej rzeczywistości dydaktycznej. Funkcja prognostyczna przejawia się w przewidywaniu przebiegu przyszłych zmian rzeczywistości dydaktycznej na podstawie poznanych prawidłowości procesu dydaktycznego. Te dwie funkcje składają się na pełnienie przez dydaktykę funkcji teoretycznej. Funkcja instrumentalno-techniczna dydaktyki (określana także funkcją praktyczną) zajmuje się jej częściami składowymi: metodami, formami, środkami itd.

6 **Dydaktyka jest nauką interdyscyplinarną.** Ma bowiem wiele ścisłych związków nie tylko z naukami o wychowaniu, ale także naukami humanistycznymi, społecznymi, politologicznymi, filozoficznymi, prawnymi i wieloma innymi. Nie funkcjonuje ona w izolacji, lecz w ścisłych związkach i zależnościach z innymi naukami. Zarówno dydaktyka, jak i inne nauki służą wychowaniu i nauczaniu, rozwijaniu osobowości wychowanków.

Dydaktyka dzieli się na dydaktykę ogólną i szczegółową (przedmiotową) – metodykę. Dydaktyka ogólna, stając się pewną filozofią nauczania, bada problemy podstawowe, a przy tym wspólne dla wszelkiego nauczania i uczenia się. **Dydaktyka szczegółowa**, zwana też przedmiotową, czy **metodyką nauczania**, bada zagadnienia specyficzne dla poszczególnych kierunków nauczania (wybranego przedmiotu nauczania) czy też jakiegoś typu lub szczebla szkoły, jak również kształcenia na określonym poziomie.

7 Postępowanie metodyczne jest celowym i świadomym przygotowaniem zajęć dydaktycznych i ich prowadzeniem, poprzez realizację zespołu poprawnie zorganizowanych czynności pedagogicznych, umożliwiającym osiągnięcie zakładanych celów kształcenia, głównie poprzez właściwy dobór oraz przekaz wiedzy, stosowanie określonych metod i form organizacyjnych, przestrzeganie zasad nauczania z zastosowaniem mediów cyfrowych i technologii informacyjno-komunikacyjnych oraz z rzetelną, zweryfikowaną kontrolą i oceną postępów.

8 Najnowsze wyniki badań w zakresie nauczania-uczenia się uzasadniają nowe podejście, dostosowane do możliwości poznawczych i zainteresowań ucznia, rozwoju jego osobowości, **procesów nauczania i uczenia się oraz stosowanie w praktyce edukacyjnej najnowszych technologii informacyjnych i przetwarzania informacji, a także korzystania z multimediów[2]. Nowym obszarem kształcenia staje się cyberprzestrzeń i jej zagrożenia[3].**

[2] T. Lewowicki, B. Siemieniecki, (red.) *Technologie edukacyjne – tradycja, współczesność, przewidywana przyszłość,* Wyd. Adam Marszałek, Toruń 2011; T. Lewowicki, B. Siemieniecki (red.), *Pedagogika medialna*, t. 1 i 2, Wyd. Naukowe PWN, Warszawa 2011; T. Lewowicki, B. Siemieniecki, (red.) *Technologie edukacyjne w wymiarze praktycznym*, Wyd. Adam Marszałek, Toruń 2011; D. Tapscott, *Cyfrowa dorosłość. Jak pokolenie sieci zmienia nasz świat,* Wydawnictwo Akademickie i Profesjonalne, Warszawa 2010.

[3] B. Siemieniecki, *Rzeczywistość wirtualna a edukacja*, w: T. Lewowicki, B. Siemieniecki, (red.) *Cyberprzestrzeń i edukacja,* Multimedialna Biblioteka Pedagogiczna, Wyd. Adam Marszałek, Toruń 2012, s. 22-23; T. Lewowicki, B. Siemieniecki, (red.) *Cyberprzestrzeń i edukacja,* Multimedialna Biblioteka Pedagogiczna, Wyd. Adam Marszałek, Toruń 2012; por. także inne publikacje w: T. Lewowicki, B. Siemieniecki, (red.) *Cyberprzestrzeń i edukacja,* Multimedialna Biblioteka Pedagogiczna, Wyd. Adam Marszałek, Toruń 2012; E. Bendyk, *Antymatrix, Człowiek w labiryncie sieci*, Wyd. WAB, Warszawa 2004; A. Andrzejewska, J. Bednarek, *Możliwości i zagrożenia świata wirtualnego,* Wyd. Akademickie ŻAK, Warszawa 1999.

Te zaś, jak wynika z powyższych analiz, **nowoczesne urządzenia mogą być stosowane na wszystkich poziomach** (od wychowania przedszkolnego, a skończywszy na kształceniu dorosłych) **i kierunkach kształcenia** (wszystkie przedmioty, ścieżki edukacyjne, kierunki studiów, a w ich ramach specjalności i specjalizacje.

9 Co wynika z prowadzonych badań, związanych z metodyką ich prowadzenia?[4]

Poniżej przedstawiono niektóre wyniki badań nad przydatnością mediów w kształceniu[5]. Ich analiza pozwoli docenić rolę i miejsce kształcenia z wykorzystaniem mediów cyfrowych w kształceniu pracowników socjalnych i doskonaleniu ich kompetencji społeczno-komunikacyjnych i medialno-informacyjnych, związanych z zagrożeniami cyberprzestrzeni i świata wirtualnego.

UCZYSZ SIĘ PRZEZ TO, CO:
- widzisz,
- słyszysz,
- wyczuwasz smakiem,
- wyczuwasz węchem,
- dotykasz,
- robisz,
- sobie wyobrażasz,
- wyczuwasz intuicyjnie,
- czujesz[6].

PREFEROWANE STYLE NAUKI (sposoby uczenia się) w typowej grupie uczniów

1. Działaniowy (dotykowy)	37%
2. Słuchowy	34%
3. Wzrokowy	29%

Jest to przegląd stylów uczenia się w typowej grupie uczniów, przygotowany przez Specific Diagnostic Studies (SDS) z Rockville w stanie Maryland na podstawie badań 5300 uczniów ze Stanów Zjednoczonych, Hongkongu i Japonii, uczęszczających do klas od piątej do dwunastej.

Uczniowie wypełnili ankietę na temat preferowanego przez siebie sposobu uczenia się[7].

10 ZWIĄZEK MIĘDZY ZAPAMIĘTYWANIEM A PERCEPCJĄ

Istnieje ścisły związek między zdolnością zapamiętywania a rodzajem zmysłowej percepcji.

W pamięci uczącego się pozostaje bowiem:
- 20% informacji, gdy jest ona słyszalna,
- 30%, gdy jest widzialna,
- do 40% przy percepcji wzrokowej i słuchowej[8].

11 WYNIKI BADAŃ NAD EFEKTAMI KSZTAŁCENIA MULTIMEDIALNEGO

W kształceniu multimedialnym, w którym oddziałuje się na prawie wszystkie zmysły człowieka, w odróżnieniu od nauczania konwencjonalnego uzyskuje się m.in. następujące wyniki:

- skuteczność nauczania wyższa o 56%;
- zrozumienie tematu wyższe o 50–60%,
- nieporozumienia przy przekazywaniu wiedzy mniejsze o 20–40%,
- oszczędność czasu – 38–70%,
- tempo nauczania wyższe o 60%,
- zakres wiedzy przyswojonej o 25–50% wyższy[9].

[4] Większą liczbę cytatów zamieszczono w książce J. Bednarka, *Multimedia w kształceniu,* Wyd. Nauk. PWN, Warszawa 2012.

[5] Ze względu na ich przydatność dla prowadzonych zajęć dydaktycznych celowo je wyeksponowano.

[6] J. Vos, *Rewolucja w uczeniu się. Chcesz myśleć sprawniej niż inni*?, Wydawnictwo Moderski i S-ka, Poznań 2000, s. 30.

[7] *Readers Digest Book of Facts,* (cyt. za Gordon Dryden, J. Vos, *Rewolucja w uczeniu się. Chcesz myśleć sprawniej niż inni*?, Wydawnictwo Moderski i S-ka, Poznań 2000, s. 116.

[8] G. L. Adams, *Why Interactive?*, w "Multimedia & Videodisc Monitor", 3/1992.

[9] B. Steinbrink, *Multimedia u progu technologii XXI wieku*, Robomatic 1992, s. 50–51

12 EFEKTY NAUCZANIA POGLĄDOWEGO

Przekaz poglądowy w rozwiązywaniu problemu przyczynia się do:

- dogodniejszych warunków dla wzrostu płynności, giętkości i oryginalności myślenia;
- szybszego i lepszego opanowania umiejętności dostrzegania problemu, powstawania pomysłów rozwiązań oraz ich weryfikacji;
- występowania współzależności między efektami kształcenia po zastosowaniu różnych rodzajów przekazu wiadomości a cechami indywidualnymi.

PIĘĆ CECH, KTÓRE POSIADA TYLKO CZŁOWIEK:

1. Umiejętność mówienia i pisania.
2. Zdolność rozumienia mowy.
3. Umiejętność czytania.
4. Zdolność poruszania się w postawie wyprostowanej.
5. Możliwość prostokątnego ustawienia kciuka i palca wyprostowanego[10].

Wszystkimi tymi czynnościami kieruje kora mózgowa, kiedy więc ulegnie ona uszkodzeniu, tracimy jedną (lub więcej) z tych funkcji.

13 CYTATY PRZYDATNE W PROWADZENIU ZAJĘĆ

Poniżej przedstawiono kilka cytatów wskazujących na znaczenie zmysłów w nauczaniu-uczeniu się oraz istotę samego kształcenia.

„Umysł nie jest naczyniem, które należy napełnić, lecz ogniem, który trzeba rozniecić".

Plutarch (grecki pisarz i filozof), słowa te zostały napisane niemal trzy tysiące lat temu.

„Dobrze rozwinięty umysł, pasja do nauki i umiejętność praktycznego wykorzystania wiedzy to nowe klucze do przyszłości".

Raport SCANS (U.S. Labor Secretary's Commission on Achieving Necessary Skills (Komisja ds. Osiągania Niezbędnych Umiejętności powołana przez ministra pracy USA).

„Natura zbudowała mózg w taki sposób, że przez pierwsze sześć lat życia człowieka potrafi on przyswajać informacje z niezwykłą szybkością i bez najmniejszego wysiłku".

G. Doman, *Jak nauczyć małe dziecko czytać,* wywiad z autorem, Filadelfia za: *Readers Digest Book of Facts*, (cyt. za G. Dryden, J. Vos, *Rewolucja w uczeniu się. Chcesz myśleć sprawniej niż inni?*, Wydawnictwo Moderski i S-ka, Poznań 2000, s. 240)

„Jeśli chcemy pomóc dzieciom, musimy zająć się ich mózgiem – w końcu nie czytają nerkami".

D. Waber (Uniwersytet Harvarda), za: J. M. Healey, *Endangered Minds,* Simon & Schuster, New York

„Myślenie wertykalne polega na kopaniu tej samej dziury, tylko coraz głębiej. Myślenie lateralne to próbowanie za każdym razem gdzie indziej".

Edward de Bono (twórca myślenia lateralnego), fragment wywiadu autora dla „Radia i" w Auckland, Nowa Zelandia, za *Readers Digest Book of Facts*, (cyt. za G. Dryden, J. Vos, *Rewolucja w uczeniu się. Chcesz myśleć sprawniej niż inni?*, Wydawnictwo Moderski i S-ka, Poznań 2000, s. 188,)

[10] G. Doman, *Jak postępować z dzieckiem z uszkodzeniem mózgu*, Wydawnictwo Protext, Poznań 1996.

„Aby nauczyć się czegoś szybko i efektywnie, trzeba to zobaczyć, usłyszeć i poczuć".

T. Stocklwell *Accelerated Learning in Theory and Practice,* (EFFECT – European Foundation for Education, Comunication and Teaching, Lichtenstein).

„Im więcej informacji łączysz, tym więcej zapamiętujesz".

G. Dryden, J. Vos, Rewolucja w uczeniu się, Chcesz myśleć sprawniej niż inni?, Wydawnictwo Moderski i S-ka, Poznań 2000, s. 132.

„Nasz mózg może nieustannie się uczyć – od urodzenia aż po kres życia".

M. Diamonf (współautorka *Magic Trees of the Mind)* Dutton, New York, za: G. Dryden, J. Vos, *Rewolucja w uczeniu się. Chcesz myśleć sprawniej niż inni*?, Wydawnictwo Moderski i S-ka, Poznań 2000, s. 126

Metodyka prowadzenia zajęć, będąca dydaktyką szczegółową, wskazuje na sposoby, na podstawie badań i doświadczeń, jak przygotować i przeprowadzić zajęcia dydaktyczne.

CHARAKTERYSTYKA PROCESU KSZTAŁCENIA

14 PROCES KSZTAŁCENIA JAKO ZWIĄZEK NAUCZANIA I UCZENIA SIĘ

Proces kształcenia to system powiązanej ze sobą działalności nauczyciela informatyki (technologii informacyjnej) i uczniów, w której toku tworzone są niezbędne warunki do świadomego i trwałego przyswajania przez tych drugich (uczniów) wiadomości, umiejętności i nawyków przewidzianych w programie nauczania. Stanowi on prawidłowościowy układ zachodzącego w toku zorganizowanego przez nauczyciela uczenia się uczniów. Na proces ten składają się trzy elementy: czynności nauczycieli, materiał nauczania i czynności uczniów.

Ze względu na czynności nauczyciela w procesie kształcenia nazywane – nauczaniem i odpowiadające im czynności ucznia – nazywane uczeniem się, proces ten nosi także nazwę procesu nauczania-uczenia się.

W systemowym ujęciu procesu kształcenia należy wymienić:

1. cele dydaktyczno-wychowawcze i treści;
2. metody i formy (organizacja);
3. zasady dydaktyczne;
4. media cyfrowe i technologie informacyjno-komunikacyjne oraz bazę szkoleniową;
5. nauczycieli i uczniów.

Tak rozumiany proces kształcenia jest zróżnicowany ze względu na:

- indywidualne umiejętności pracy umysłowej;
- metody nauczania stosowane przez nauczycieli;
- stosunek uczącego się do wiadomości, które mogą być wyłącznie zapamiętane, bądź odpowiednio ustrukturyzowane, tworząc w ten sposób podstawę do tworzenia nowej wiedzy.

Nauczanie i uczenie się to dwa wzajemnie powiązane i uzupełniające się procesy, które warunkują skuteczność kształcenia **informatyki (technologii informacyjnej)**. W różnych systemach dydaktycznych i w różnych pod względem zaawansowania dojrzałości zespołach, wzajemne relacje między nauczaniem a uczeniem się nie są jednakowe.

15 UŚWIADAMIANIE UCZNIOM (DOROSŁYM) CELÓW I ZADAŃ KSZTAŁCENIA

Świadomość to pojęcie trudno definiowane. **Uważa się, że jest ona najważniejszym mechanizmem regulacyjnym czynności ludzkich**. Jest to proces informacyjny, polegający

na odbiorze informacji przez szczególnego rodzaju system kodowania (mózg) oraz na ich wewnętrznym przetwarzaniu za pomocą wewnętrznych modeli i programów działania.

Dzięki świadomości człowiek potrafi:

- regulować swoją działalność w warunkach zmiennych;
- uświadamiać sobie pojedyncze zdarzenia, jak i całość sytuacji zewnętrznej;
- spełniać funkcję sterowniczą oraz integrować działania innych mechanizmów regulacyjnych.

Można zatem przyjąć, że świadomość człowieka odgrywa główną rolę w zakresie orientacji zewnętrznej i wewnętrznej (samoregulacji). Bardzo ważne znaczenie ma tu fakt prawidłowego widzenia siebie jako elementu rzeczywistości i odbioru tej rzeczywistości.

Zakres i forma aktywności człowieka rozszerza się wraz z rozbudową układu nerwowego (w tym analizatorów i efektorów), doprowadzając na szczeblu ludzkim do najwyższej postaci aktywności – do działania świadomego.

Uświadomienie uczniom celów i zadań kształcenia pozwala na jasne i jednoznaczne określenie wyników nauczania. Wytworzenie pozytywnej motywacji do nauki pozwala także zmobilizować uczniów do nauki. Niezbędnym elementem jest jednak należyte sformułowanie celów operacyjnych. Pierwszym krokiem do uświadomienia celów jest sformułowanie celu ogólnego, równoznacznego z wynikiem nauczania, który przedstawia dla uczniów pewną wartość.

Pozytywne motywy uczenia się są efektem prowadzonego na wysokim poziomie procesu kształcenia, zwłaszcza przeprowadzonych już zajęć z danego przedmiotu. Z tego też powodu poszczególne elementy procesu kształcenia winny współprzyczyniać się do powodzenia całości. Z tej racji konieczne jest planowanie (przygotowanie) zajęć dydaktycznych, jako określonej organizacji czynności pedagogicznych. W warstwie celów ogólnych chodzi o nakreślenie dążeń, które powinny stanowić źródło celów szczegółowych (operacyjnych). Bardziej zwięzłe i zwykle lepiej sprecyzowane są cele szczegółowe, zwane operacyjnymi. Stanowią one opis wyników, które mają być uzyskane[11]. Opis ten winien być na tyle pełny i dokładny, by wykładowca mógł łatwo sprawdzić, czy uczeń cel osiągnął. Cele te należy uczniom uświadomić.

16 ZDOBYWANIE NOWEJ WIEDZY (POZNAWANIE NOWYCH FAKTÓW)

Poznawanie nowych faktów przez uczniów jest procesem złożonym i długotrwałym. Składa się on z wielu etapów: od zmysłowego ich ogarnięcia poprzez poznanie abstrakcyjne do praktycznych zastosowań. Niezbędnym warunkiem jest jednak opieranie się na dobrze zorganizowanej obserwacji (pozwala dochodzić do sądów spostrzeżeniowych) lub na działaniu praktycznym. Pozwala przygotować uczniów do uogólniania pojęć i sądów ogólnych. Kreuje także własną aktywność i samodzielność uczniów.

W tworzeniu pojęć naukowych W. Okoń wyróżnia następujące momenty:

1. zestawienie przez uczniów danego obiektu lub zdarzenia z innymi wynikami w celu wyodrębnienia go spośród innych;
2. wyszukiwanie cech podobnych i ich uogólnianie;
3. poszukiwanie cech różniących dane rzeczy bądź zdarzenia od innych;
4. wytworzenie sobie danego pojęcia na podstawie znajomości istotnych cech danej kategorii przedmiotów;
5. zastosowanie przez uczniów poznanego pojęcia w nowych sytuacjach poznawczych bądź praktycznych[12].

[11] B. Niemierko, *Cele kształcenia,* w: K. Kruszewski (red.), *Sztuka nauczania. Czynności nauczyciela*, PWN, Warszawa 1991, s. 12.

[12] W. Okoń, *Wprowadzenie do dydaktyki ogólnej*, Wyd. Akademickie „ŻAK", Warszawa 2003.

Na zdobywanie nowych wiadomości zwraca uwagę K. Kruszewski[13]. Następuje ono stosownie do schematów poznawczych. Fakty docierają do ucznia w wyniku jego osobistych doświadczeń (poznanie bezpośrednie) i w formie przekazu (po wcześniejszym ich zdobyciu, uporządkowaniu i wyrażeniu w jakimś kodzie przez innych).

W pierwszym wypadku wiadomości o faktach, w granicach wyrażonych przez zadanie, są selekcjonowane i organizowane wyłącznie przez ucznia, według jego własnych możliwości uczenia się i percepcji zadania. Są one selekcjonowane i organizowane tak, aby jak najlepiej były włączone do wiedzy posiadanej, tworząc określony system wiedzy. W drugim przypadku stosunek ucznia do wiadomości może być różny; po pierwsze – dąży do odtworzenia ich jako ustrukturyzowanej sumy w swojej wiedzy; i po drugie – dokonuje własnej selekcji i reorganizacji. Ponadto może samodzielnie odkrywać związki między tymi wiadomościami.

17 POZNAWANIE PRAWIDŁOWOŚCI I SYSTEMATYZOWANIE WIEDZY

Poznawanie prawidłowości i systematyzowanie wiedzy następuje głównie poprzez obserwację, doświadczenia i samodzielne przetwarzanie wiedzy.

Bardzo przydatne są też różne odmiany nauczania problemowego, w toku którego następuje uzupełnienie luk w wiedzy ucznia, uzupełnienie brakującego elementu w określonym systemie wiedzy.

Proces poznawania dokonuje się głównie na dwóch „piętrach". Pierwsze z nich dotyczy prawidłowości pierwszego rzędu. Po ich odkryciu wyraża je uczeń za pomocą „łańcucha" pojęć. Zestawienie ze sobą dwu lub więcej prawidłowości w procesie samodzielnego myślenia może stać się odskocznią do wykrycia nowej prawidłowości, tym razem wyższego rzędu, a więc znajdującej się niejako na drugim „piętrze".

Wykorzystywane metody poznawania faktów i systematyzowania wiedzy mają wpływ na procesy generalizacji, na obydwu piętrach przebiegają łatwiej i prędzej. Ważnym elementem tych procesów jest formułowanie prawidłowości (zależności) przez uczniów oraz posługiwanie się nimi w nowych sytuacjach, a przede wszystkim włączanie ich do systemu wiedzy w obrębie danego przedmiotu.

Uwzględnienie powyższej procedury postępowania sprzyja hierarchizacji wiedzy, budowaniu jej systemu. Ma to duże znaczenie dla porządkowania i systematyzowania wiedzy oraz tworzenia złożonych prawidłowości i praw, co przyczynia się do utrwalania wiedzy.

18 PRZECHODZENIE OD TEORII DO PRAKTYKI

Istota przechodzenia od teorii do praktyki wyraża się w posługiwaniu się wiedzą naukową informatyki (technologii informacyjnej) w praktyce. Jej podstawą są zdania normatywne, czyli normy, dzielące się na rzeczowe i emocjonalne. Wśród tych pierwszych, najważniejszych w tym procesie, wyróżnia się normy językowe, normy biologiczne, techniczne i inne. Wiedza naukowa, opisująca rzeczywistość i wyjaśniająca zależności w niej występujące jest ich podstawą. Związek norm z wiedzą zapewnia każdemu działaniu praktycznemu lepsze efekty.

W procesie przechodzenia od teorii do praktyki można wyróżnić pewne fazy:

1. uświadomienie sobie przez uczniów nazwy, naukowych podstaw i znaczenia danej umiejętności;
2. sformułowanie na podstawie znanych uczniom wiadomości jednej lub więcej reguł działania;
3. pokaz danej czynności;

[13] K. Kruszewski, *Zmiana i wiadomość*, PWN, Warszawa 1987, s. 47–48.

4. pierwsze samodzielne czynności uczniów;
5. systematyczne i samodzielne ćwiczenia.

Uświadomienie tych faz sprzyja efektywnemu kierowaniu procesem.

19 Przechodzenie od teorii do praktyki służy bezpośredniemu przygotowaniu uczniów do racjonalnego posługiwania się wiedzą w rozmaitych sytuacjach praktycznych. Ma ono ścisły związek z wiązaniem opanowania wiadomości z jednoczesnym ich stosowaniem, czyli posługiwaniem się nimi przy rozwiązywaniu zadań praktycznych.

Na podstawie badań K. Lech wykazał, że racjonalne łączenie teorii z praktyką podnosi walory kształcące nauczania. Jego zdaniem przestrzeganie tej zasady może następować w czterech postaciach:

1. Łączenia myślenia i poznawanych treści o charakterze praktycznym z myśleniem i treściami teoretycznymi.
2. Łączenie zdobywanych wiadomości w struktury i posługiwanie się nimi w praktyce, zwłaszcza przy zdobywaniu dalszych partii wiedzy.
3. Łączenie nauki z techniką; przechodzenie od praw nauki do zasad techniki – przy zachowaniu systematyczności nauczania według logicznego układu praw nauki.
4. Łączenie poznania z działaniem: planowanie i wykonywanie różnorodnych przedmiotów i czynności związanych z treścią nauczania; posługiwanie się przy tym prostymi narzędziami, wyrabianie nawyków i sprawności ruchowych[14]. Przykładem potwierdzającym tę tezę mogą być pomysły racjonalizatorskie i nowatorskie zgłaszane przez szkolonych.

Badania te potwierdziły konieczność stosowania zasady powiązania teorii z praktyką, co wpływa dodatnio na wyniki nauczania. Uwzględnienie tej zasady pozwala lepiej zrozumieć zjawiska przyrodnicze i procesy techniczne, a także optymalizować stosowanie różnorodnych urządzeń.

Poznanie różnorodnych prawidłowości procesu kształcenia jest niezbędnym warunkiem dalszych działań związanych z przygotowaniem zajęć i ich realizacją.

CELE I TREŚCI KSZTAŁCENIA

20 TAKSONOMIA CELÓW KSZTAŁCENIA

Pojecie celu jest interpretowane różnie. Etymologicznie i znaczeniowo wiąże się z niemieckim słowem wieloznacznym oznaczającym punkt, do którego skierowane jest jakieś działanie[15]. „Celem jest to, do czego się dąży, co chce się osiągnąć, punkt, miejsce, do którego się zmierza”[16].

Świadomość celów jest warunkiem skuteczności, sprawności i ekonomizacji wszystkich ludzkich działań. Im bardziej precyzyjnie zarysowują się przed działającymi zamierzone efekty ich wysiłku, tym łatwiej zapewnić im można sprawność, ekonomiczność i skończoność podejmowania działania.

Przez cele kształcenia i wychowania rozumie się najogólniejszą wizję pożądanych właściwości: fizycznych, umiejętności, społecznych, kulturowych, duchowych jednostki ludzkiej, które chce się uzyskać poprzez tworzenie odpowiednich warunków indywidualnego rozwoju i jego stymulowanie, zwłaszcza w systemie kształcenia zarówno w trakcie zajęć, jak i poprzez inne formy kształcenia oraz zabiegi mające na celu przyswojenie odbiorcy nie tylko wiedzy i związanych z nią umiejętności, ale też poglądów, przeko-

[14] Por. K. Lech, *Rozwijanie myślenia uczniów przez łączenie teorii z praktyką*, WSiP, Warszawa 1960, s. 126.

[15] *Słownik Wyrazów Obcych*, PWN, Warszawa, 2013.

[16] *Słownik Języka Polskiego*, PWN, Warszawa, 2013.

nań, orientacji i motywacji[17].

W zależności od stopnia świadomości celów działań bywają one określone jako: zamiar, zamierzenie lub intencja. Zdaniem J. Zieleniewskiego zamiar to wyobrażone i zaakceptowane, lecz jeszcze nie wykonane działanie, ale pomyślane jako to, które prowadzi do celu. Zamierzenia to świadomy cel zaakceptowany. Intencja to cel zaakceptowany nieświadomie lub niezupełnie świadomie.

21 Podstawowymi właściwościami celów działań są:

1) stopień ich ogólności (poziom uszczegółowienia);
2) stopień jasności i zrozumienia jego sformułowania;
3) stopień realności, czyli dostępności formalnej i rzeczywistej.

Wymienione czynniki wpływają na skuteczność działania, ułatwiają zbliżenie się do jego osiągnięcia.

Dokładne sprecyzowanie celów jest warunkiem pełnienia przez nie regulacyjnych funkcji. Umożliwiają one bowiem:

1. Planowanie działania, czyli przewidywanie jego etapów, koncepcyjne etapy działań składowych.
2. Projektowanie ciągu działań pedagogicznych.
3. Programowanie sekwencji sytuacji dydaktyczno-wychowawczych.
4. Optymalizację i koordynację doboru środków.
5. Prowadzenie racjonalnej regulacji procesów.
6. Pełną, obiektywną i racjonalną kontrolę i ocenę.

Określone wartości są pożądane przez działającego, oczekiwane w przyszłości, uznane za ważne, godne wysiłku człowieka, mogą być mniej lub bardziej uświadomione.

Klasyfikacja celów:
Ze względu na stopień ogólności celów wymienia się:

1. Cele dalekiego czasu (zasięgu) – nazywane funkcjami teleologicznymi.
2. Cele ogólne – globalne, dalekiego czasu.
3. Cele naczelne opisujące poszczególne dyspozycje psychiczne.
4. Cele etapowe – nazywane standardami psychicznymi.
5. Cele operacyjne – nazywane celami konkretnych działań.

Najważniejszymi elementami każdego procesu kształcenia są więc cele i treści kształcenia. Cele kształcenia to zamierzone zmiany, które powinny nastąpić u uczniów w organizowanym przez nauczycieli procesie dydaktycznym. Ostatecznie zmiany te powinny zapewnić człowiekowi możliwość adekwatnego pojmowania rzeczywistości i twórczego uczestnictwa w niej.

Na ogół zmian, objętych celami kształcenia, składają się zmiany rzeczowe, osobowe, percepcyjne, operacjonalizacyjne i funkcjonalizacyjne. Oczekiwanym w procesie kształcenia zmianom odpowiadają formułowane często w literaturze cele poznawcze, kształcące i wychowawcze. Występujące między jednymi i drugimi relacje można przedstawić następująco:

Tabela 1. Relacje między zmianami i celami

zmiany rzeczowe	cele poznawcze
zmiany osobowe percepcyjne i operacjonalizacyjne	cele kształcące
zmiany funkcjonalizacyjne	cele wychowawcze

Źródło: opracowanie własne

[17] W. Okoń, *Słownik Pedagogiczny*, PWN, Warszawa 1992, s. 168–169.

Formułowanym celom edukacyjnym odpowiadają cele poznawcze, kształcące i wychowawcze. Występujące między jednymi i drugimi relacje można ująć w następujący sposób: zmiany rzeczowe – cele poznawcze, zmiany osobowe percepcyjne i operacjonalizacyjne – cele kształcące, zmiany osobowe funkcjonalne – cele wychowawcze.

22 **Najpopularniejsza w Polsce ramowa taksonomia celów nauczania zwana jest taksonomią ABC:**

Tabela 2. Taksonomia celów wychowania

Poziom	Kategoria
I. Wiadomości	A. Zapamiętanie wiadomości B. Zrozumienie wiadomości
II. Umiejętności	C. Stosowanie wiadomości w sytuacjach typowych D. Stosowanie wiadomości w sytuacjach problemowych

Źródło: opracowanie własne

„A. Zapamiętanie wiadomości oznacza gotowość ucznia do przypominania sobie pewnych terminów, praw i teorii naukowych, zasad działania. Wiąże się to z elementarnym poziomem rozumienia tych wiadomości: uczeń nie powinien ich mylić ze sobą i zniekształcać.

B. Zrozumienie wiadomości oznacza, że uczeń potrafi je przedstawić w innej formie, niż je zapamiętał, uporządkować i streścić, uczynić podstawą prostego wnioskowania.

C. Stosowanie wiadomości w sytuacjach typowych oznacza opanowanie przez ucznia umiejętności praktycznego posługiwania się wiadomościami wg podanych mu uprzednio wzorów. Cel, dla którego wiadomości mają być stosowane, nie powinien być bardzo odległy od celów osiąganych w toku ćwiczeń szkolnych.

D. Stosowanie wiadomości w sytuacjach problemowych oznacza opanowanie przez ucznia umiejętności formułowania problemów, dokonywania analizy i syntezy nowych dla niego zjawisk, formułowania planu działania, tworzenia oryginalnych przedmiotów, wartościowania przedmiotów według kryteriów”[18].

W dziedzinie motywacyjnej najbardziej znana jest następująca taksonomia:

Tabela 3. Taksonomia celów wychowania

Poziom	Kategoria
I. Działania	A. Uczestnictwo w działaniu B. Podejmowanie działania
II. Postawy	C. Nastawienie na działanie D. System działań

Źródło: opracowanie własne

A. Uczestnictwo w działaniu polega na świadomym i uważnym odbieraniu określonego rodzaju bodźców oraz wykonaniu czynności odpowiadających przyjętej roli, jednak bez wykazywania inicjatywy. Wychowanek ani nie unika danego rodzaju działania, ani też go nie podejmuje z własnej woli, natomiast chętnie dostosowuje się do sytuacji.

B. Podejmowanie działania polega na samorzutnym rozpoczynaniu danego działania i wewnętrznym zaangażowaniu w wykonywanie danego rodzaju czynności. Wychowanek nie tylko dostosowuje się do sytuacji, w jakiej się znalazł, ale i organizuje ją w pewien sposób. Jest to jednak postępowanie mało jeszcze utrwalone.

C. Nastawienie na działanie polega na konsekwentnym wykonywaniu danego rodzaju działania na skutek trwałej potrzeby wewnętrznej i dodatniego wartościowania jego wyników. Wychowanek jest zwolennikiem tego działania i zachęca do niego innych, poglądom jego brak jednak szerszego uogólnienia i pełnej spoistości.

D. System działań polega na regulowaniu określonego typu działalności za pomocą harmonijnie uporządkowa-

[18] Tamże, s. 13.

nego zbioru zasad postępowania, z którymi wychowanek identyfikuje się do tego stopnia, że można je uważać za cechy jego osobowości. Wychowanek nie zawodzi nawet w bardzo trudnych sytuacjach, a jego działania odznaczają się skutecznością oraz swoistością stylu”[19].

Formułowanie celów szkolenia powinno zatem obejmować:

- analizę celów ogólniejszych, wyższych w hierarchii ważności;
- określenie celów danego ćwiczenia z podziałem na cele ogólne i szczegółowe;
- wyodrębnienie zadań jako dyspozycji do działania;
- ukazanie możliwości wpływania na psychikę ucznia i rozwijanie jego cech osobowościowych niezbędnych we współczesnym życiu.

Ta właśnie część pracy metodycznej poświęcona celom kształcenia jest najtrudniejsza, ale odpowiednio przeanalizowana może w istotny sposób wzbogacić efektywność kształcenia.

23 CELE OGÓLNE I SZCZEGÓŁOWE (OPERACYJNE) A TREŚCI KSZTAŁCENIA

Pojęcie celów kształcenia i wychowania ma fundamentalne znaczenie dla pedagogiki, a w tym i dla całej edukacji. Zawiera ono swoistą wizję rozwoju człowieka od najwcześniejszej fazy jego życia. Równocześnie jednak istota celów kształcenia sprowadza się do zapewnienia każdej jednostce ludzkiej bogatego i zróżnicowanego rozwoju intelektualnego, zawodowego, moralnego i kulturalnego. Kategorią nadrzędną wobec celów nauczania i wychowania jest ideał wychowawczy, który ma być całościową, generalną wizją pożądanej osobowości[20]. Przypomnijmy, iż cele kształcenia i wychowania to „najogólniejsza wizja pożądanych właściwości fizycznych, które chce się uzyskać poprzez tworzenie odpowiednich warunków indywidualnego rozwoju i jego stymulowanie, zwłaszcza w systemie oświatowo-wychowawczym zarówno na lekcji szkolnej, jak i poprzez przyswojenie uczniowi i wychowankowi nie tylko wiedzy i związanych z nią umiejętności, ale też poglądów, przekonań, orientacji, motywacji”[21].

24 W prowadzonych zajęciach można przyjąć następujące ich cele

1. **Poznawczy (dydaktyczny)** – zapoznanie z podstawami wiedzy o najważniejszych zagrożeniach cyberprzestrzeni, a w szczególności tymi, które dotyczą dzieci, młodzieży, dorosłych i osób starszych. Wskazanie nowych uwarunkowań związanych z przebywaniem w cyberprzestrzeni będącym już zjawiskiem o charakterze społecznym i masowym, mającym określone skutki dla polityki społecznej i zdrowia.
2. **Kształcący** – kształcenie i doskonalenie najważniejszych kompetencji (umiejętności, sprawności, nawyków) związanych z rozpoznawaniem poszczególnych zagrożeń występujących w cyberprzestrzeni i podejmowaniem sprawnych i skutecznych działań w zakresie minimalizowania ich skutków w ramach polityki społecznej.
3. **Wychowawczy** – kształtowanie świadomości nowej roli i miejsca tradycyjnych zagrożeń występujących w świecie rzeczywistym i ścisłego ich związku z nowymi zagrożeniami mającymi miejsce w cyberprzestrzeni i świecie wirtualnym, a także z zupełnie nowymi patologiami i cyberprze-

[19] Tamże, s. 15.

[20] Por. *Cele kształcenia i wychowania, ideały wychowawcze, wzorce osobowe (z punktu widzenia świeckiego)*, w: *Encyklopedia Pedagogiczna* (red.) W. Pomykało, Warszawa 1993, Fundacja Innowacja, s. 54 i następne.

[21] Tamże, s. 54.

stępstwami, prowadzącymi do różnorodnych dysfunkcji, ryzykownych zachowań, a nawet marginalizacji, które muszą być przedmiotem polityki społecznej.

25 **Treści kształcenia, wynikające z analizowanych celów, są podstawą pedagogicznego oddziaływania na uczniów. Powinny one uwzględniać, zarówno aktualne, jak i przyszłe potrzeby w każdej działalności pracowników socjalnych. Tymi treściami są zagadnienia przedstawione w powyższym opracowaniu.**

METODY KSZTAŁCENIA

26 POJĘCIE METODY

W szkoleniu metody często utożsamiane są z formami prowadzenia zajęć. Pomiędzy nimi w procesie nauczania-uczenia się występują liczne związki. One też wzajemnie się uzupełniają. Metody też są utożsamiane z kierunkami lub systemami kształcenia, a niekiedy z metodami rozumowania. Jednocześnie interesujący nas termin bywa zastępowany nie tylko „formą nauczania", ale także pojęciem „zasada nauczania", które jednak dotyczy reguły postępowania prowadzącego zajęcia.

27 Termin „metoda" pochodzi od greckiego słowa methodos, co znaczy badanie, droga dochodzenia do prawdy. Jest on zatem etymologicznie powiązany z tym znaczeniem, jakie ma metodologia czy metodyka badania, poszukiwania prawdy. Według *Słownika języka polskiego* mamy do czynienia z dwoma określeniami. Pierwsze z nich dotyczy świadomie i konsekwentnie realizowanego sposobu postępowania dla osiągnięcia określonego celu, zespół celowych czynności i środków. Zgodnie z drugim – jest to sposób naukowego badania rzeczy i zjawisk, ogół reguł stosowanych przy badaniu rzeczywistości[22].

28 Według W. Okonia „metoda kształcenia jest to wypróbowany i systematycznie stosowany układ czynności nauczycieli i uczniów, realizowanych świadomie w celu spowodowania zmian w osobowości uczniów"[23]. Nie jest to jednak sposób „stosowany wielokrotnie", lecz zgodnie z poglądem T. Kotarbińskiego „z intencją zastosowania przy powtórzeniu się tego zadania". **Przez metodę rozumie się zatem celowo i systematycznie stosowany sposób pracy prowadzącego zajęcia ze szkolonymi, umożliwiający im opanowanie wiedzy wraz z umiejętnością posługiwania się nią w praktyce, a także rozwijanie zdolności i zainteresowań poznawczych.**

Charakterystyczne w tej kwestii jest także stanowisko K. Kruszewskiego, który analizując pojęcie metody nauczania uwzględnia w jej obrębie umysłowe operacje uczniów prowadzące do zmian psychicznych, głównie dzięki operacjom związanym z treścią kształcenia[24].

Z powyższych analiz wynika zatem, że „metoda w procesie kształcenia staje się podstawowym elementem, obok sposobu postępowania określa organizację procesu, jego tok, właściwe reguły i prawidłowości nauczania przy zastosowaniu określonej metody"[25].

Metody kształcenia to więc kolejny niezwykle istotny czynnik mający wpływ na efektywność procesu nauczania-uczenia się. Niedobór czasu na realizację progra-

---

[22] *Słownik języka polskiego*, PWN, Warszawa 1979, tom II, s, 144.

[23] W. Okoń, *Wprowadzenie do dydaktyki ogólnej*, PWN, Warszawa 1987, s. 270.

[24] Por. K. Kruszewski, *Zmiana i wiadomość. Perspektywa dydaktyki ogólnej*, PWN, Warszawa 1993, s. 182.

[25] J. Półturzycki, *Dydaktyka dorosłych*, WSiP, Warszawa 1991, s. 160.

mu teoretycznego w szkołach zmusza do poszukiwania najefektywniejszych metod nauczania oraz lepszej organizacji i planowania procesu dydaktycznego.

29 Metoda to świadomie i konsekwentnie stosowany sposób postępowania dla osiągnięcia określonego celu. T. Kotarbiński twierdzi, że „przez metodę rozumiemy sposób systematycznie stosowany, tzn. stosowany w danym przypadku z intencją zastosowania go przy ewentualnym powtórzeniu się analogicznego zadania".

Użyty w powyższym zdaniu równoważnik definicyjny: sposób może prowadzić do zamierzonego stosowania terminów: metoda i sposób. „Tymczasem – stwierdza W. P. Zaczyński – stosunek wymienionych dwóch terminów jest niepowszedni, znaczy to, że każda metoda jest niewątpliwie sposobem działania, ale nie każdy sposób zasługuje na miano metody".

Można zatem przyjąć, że dowolna metoda zakłada pewien cel i system czynności. W. Okoń przez metodę nauczania rozumie „systematycznie stosowany sposób pracy nauczyciela z uczniami, umożliwiający uczniom opanowanie wiedzy wraz z umiejętnością posługiwania się nią w praktyce, jak również rozwijanie zdolności i zainteresowań umysłowych".

Metoda nauczania jest zatem określonym sposobem kierowania działalnością poznawczą uczniów.

30 **TYPOLOGIA METOD KSZTAŁCENIA**

W rozwoju metod, w pierwszej kolejności, możemy wyróżnić metody oparte na naśladownictwie. Obserwując i powtarzając za dorosłymi określone czynności uczniowie przyswajali je sobie stopniowo w toku bezpośredniego uczestnictwa w życiu tej grupy społecznej, której byli członkami. Następnie, po pojawieniu się szkół, dominującą rolę zaczęły odgrywać metody słowne, a wśród nich metody wykładowe i pytające, których jednak stosowanie prowadziło do jednostronności w nauczaniu. Z tego też powodu słowo mówione było zastępowane przez słowo pisane, a następnie drukowane, które stało się podstawowym nośnikiem informacji.

Inną metodą, która pojawiła się w nauczaniu była metoda heurystyczna, (od *heurisco* – znajduję). Jej stosowanie w nauczaniu pozwoliło na pozbycie się długotrwałego, dominującego aż do końca XX wieku sposobu werbalnego w nauczaniu. Następnie przedmiotem powszechnego zainteresowania stała się koncepcja tzw. uczenia się przez działanie. Żadna jednak z tych metod stosowanych oddzielnie nie zapewniała pozytywnych wyników.

31 Metody słowne i oglądowe zostają więc zastąpione lub wzbogacone metodami aktywizującymi oraz praktycznymi, sprzyjającymi zaznajamianiu szkolonych z wiedzą, przy jednoczesnym pełnym rozwijaniu i wykorzystaniu ich zdolności i zainteresowań. Niezależnie od nich do kształcenia wprowadzono jeszcze nauczanie programowane.

32 **TYPOLOGIE METOD NAUCZANIA**

Obecnie w literaturze przedmiotu wyróżnić można kilka klasyfikacji. Ze względu na rolę i zadania prowadzącego zajęcia oraz stopień aktywności szkolonych można wyróżnić trzy grupy metod nauczania. Do pierwszej – zalicza się metody podające (opis, opowiadanie, wykład, uczenie się z książki, itp.). Kolejną grupę stanowią metody poszukujące (pogadanka, dyskusja itp.). Trzecia grupa – to metody doświadczalne albo laboratoryjne (obserwacja, eksperyment itp.). Te ostatnie mają wiele związków z metodami drugiej grupy.

33 Inny podział obejmujący cztery grupy metod, opracowany został przez W. Okonia, który uporządkował je w kon-

cepcji kształcenia wielostronnego. Mieszczą one w sobie obok poznania i działania również przeżywanie. Stąd też oparte są na czterech rodzajach nauczania. Pierwsza grupa obejmuje metody podające, które pozwalają uczyć się przez przyswajanie. Druga grupa – to metody problemowe, których cechą charakterystyczną jest uczenie się przez przyswajanie. Uczenie się przez odkrywanie właściwe jest dla grupy metod problemowych i one zaliczane są do grupy trzeciej. Czwartą zaś stanowią metody praktyczne, w których uczenie się następuje przez działanie[26].

34 Cz. Kupisiewicz wprowadził następujący podział metod:

- oparte na słowie: pogadanka, wykład, praca z książką, dyskusja;
- oparte na obserwacji i pomiarze: pokaz, pomiar;
- oparte na praktycznej działalności uczniów: metoda laboratoryjna, metoda zajęć praktycznych, ćwiczenia;
- nauczanie programowane[27].

35 Ze względu na cel dydaktyczny, jaki sobie stawia prowadzący zajęcia, przyjmuje się następujące rodzaje metod:

Tabela 4. Rodzaje metod w zależności od celu dydaktycznego

CEL DYDAKTYCZNY	METODY NAUCZANIA
podanie nowego materiału	opowiadanie, wykład, praca z podręcznikiem, demonstracje zjawisk, przedmiotów i środków poglądowych, obserwacja, praca z tekstami programowanymi
poszukiwanie wiedzy	przygotowanie referatów, zajęcia laboratoryjne, rozwiązywanie zadań problemowych
utrwalanie wiedzy	powtarzanie systematyzujące, ćwiczenia utrwalające
kontrola wiadomości	egzamin praktyczny, sprawdziany, testy

Źródło: opracowanie własne

Powyższe zasady podziałów nie w pełni są zgodne z wymogami adekwatności i rozłączności.

36 **Dobór metod zależy od wielu czynników**, stąd też kryteria w tym zakresie mają nie tyle charakter wykluczający, co raczej ukierunkowujący i wskazują tendencje główne, aczkolwiek nie jedyne. Dlatego też w doborze metod nie może być jednostronności, a muszą one być łączone w sposób racjonalny.

Zgodnie z poglądem W. Okonia[28] bez względu na rodzaj klasyfikacji, należy zwrócić uwagę na następujące kilka aspektów, które podano w tabelach:

37 **Treść kształcenia**, gdy granice zastosowania metody stanowią takie alternatywy, jak:

Tabela 5. Treści a dobór metod kształcenia

Strukturalizacja	konwencjonalne ujęcie treści
związek treści z rzeczywistością	oderwanie treści od realiów
funkcjonalność treści	werbalizm

Źródło: opracowanie własne

[26] Podział ten opiera się na opracowanej przez W. Okonia koncepcji wielostronnego nauczania-uczenia się. Por. W. Okoń, *Wprowadzenie do dydaktyki ogólnej*, op.cit.,; także: W. Pomykało (red.), *Encyklopedia pedagogiczna*, op.cit., s. 332–335; W.P. Zaczyński, *Uczenie się przez przeżywanie. Rzecz o teorii wielostronnego kształcenia*, WSiP, Warszawa 1990.

[27] Cz. Kupisiewicz, *Podstawy dydaktyki ogólnej*, PWN, Warszawa 2010.

[28] Por. J. Półturzycki, *Dydaktyka dorosłych*, op.cit., s. 162.

Styl pracy nauczyciela, gdy jego czynności mają wpływ na wybór alternatywy, jak:

Tabela 6. Styl pracy a dobór metod kształcenia

styl demokratyczny	styl autorytarny
nacisk na uczenie się młodzieży	nacisk na nauczanie
wielostronne rozwijanie młodzieży	nauczanie treści programowych

Źródło: opracowanie własne

Styl pracy uczniów, gdy ich działania mieścić się mają między alternatywami, jak:

Tabela 7. Styl pracy a dobór metod kształcenia

autonomia	heteronomia
twórczość	naśladownictwo
wielostronna aktywność	aktywność jednostronna

Źródło: opracowanie własne

Społeczne uwarunkowania pracy uczniów, gdy w grę wchodzą pewne alternatywy:

Tabela 8. Społeczne uwarunkowania pracy a dobór metod kształcenia

łączenie różnych form pracy grupowej i jednostkowej	praca jednostkowa
więź szkoły ze środowiskiem	izolacja szkoły od środowiska
wszechstronny rozwój osobowości uczniów	jednostronny rozwój osobowości uczniów

Źródło: opracowanie własne

Każda z wyróżnionych grup metod nauczania, łącznie ze składającymi się na nią metodami szczegółowymi, może spełniać następujące funkcje dydaktyczne: służyć zaznajamianiu z nowym materiałem; zapewnić utrwalenie zdobytej wiedzy; umożliwić kontrolę i ocenę stopnia opanowania tej wiedzy[29]. Wartość metod zależy zatem od charakteru czynności prowadzących zajęcia i szkolonych oraz środków dydaktycznych wspierających lub zastępujących niektóre czynności. Znaczenie ich wynika ze stopnia możliwości wywołania aktywności poznawczej, emocjonalnej i praktycznej szkolonych, jak również warunków pozwalających je osiągnąć. Do najważniejszych czynników determinujących wybór metody nauczania należy zaliczyć:

- najbliższy cel dydaktyczny zajęć, który ulega licznym modyfikacjom;
- treści nauczania będące zróżnicowane w zależności od przedmiotu;
- środki nauczania wyznaczające bezpośrednio sposoby pracy prowadzącego zajęcia;
- organizację procesu dydaktycznego jako całości i jego poszczególnych jednostek metodycznych[30].

METODY OGLĄDOWE

38 **Istota stosowania tych metod polega na odpowiednio ukierunkowanych procesach spostrzegania, a zwłaszcza obserwacji**. Czynności dydaktyczne prowadzącego zajęcia najczęściej ograniczają się do demonstracji szkolonym naturalnych przedmiotów lub modeli, procesów i zjawisk. Towarzyszy im objaśnianie ich specyficznych cech, co w literaturze przedmiotu określane jest pokazem. Jego przedmiotem mogą być określone rodzaje uzbrojenia, ich poszczególne elementy, dzieła sztuki, dokumenty archiwalne, mapy, schematy, tablice poglądowe. Aby pokaz spełnił swoje zadania, należy przestrzegać wiele wymagań dydaktycznych, jak:

1. precyzyjne określenie celu i przedmiotu planowanej obserwacji;
2. skupienie uwagi szkolonych na demonstrowanym przedmiocie lub pokazie całego układu czynności oraz zapewnienie im dobrych warunków spostrzegania;
3. pokaz wszystkich elementów demonstrowanego przedmiotu i poszczególnych składników przerabianych czynności z równoczesnym zachowaniem

[29] Por. W. Pomykało,(red.), *Encyklopedia pedagogiczna*, op.cit., s. 354.

[30] W. Zaczyński, *Metody nauczania*, w: *Pedagogika. Podręcznik akademicki*, PWN, Warszawa 1990, s. 568.

optymalnego tempa i wyjaśniania odpowiednio dostosowanego do kolejnych faz pokazu;
4. pokaz całego demonstrowanego przedmiotu i całego układu czynności;
5. umożliwienie wszystkim szkolonym „dotykowe" poznawanie tych przedmiotów, które są treścią pokazu i spostrzegania;
6. pokaz odpowiednich materiałów wizyjnych (filmy, nagrania wideo, programy komputerowe itp.).

Metody oglądowe stosuje się najczęściej w trzech przypadkach:
1. w celu wzbogacenia obserwacji poprzez odpowiedni komentarz lub wyjaśnienie;
2. wzbogacenia poznania dokonanego za pomocą innych metod;
3. zebrania w całość i usystematyzowania informacji.

39 **Metody oglądowe przybierać mogą następujące formy: demonstrowanie (pokaz), projekcja filmu, hospitacja, wycieczka itp**. Cennym środkiem metodycznym są przeźrocza, obrazy filmowe, episkopowe oraz materiały telewizyjne i komputerowe. Obok środków audiowizualnych dość często stosuje się pokaz map, tablic, wykresów, schematów itp., gdyż ułatwiają one zrozumienie treści, nadając abstrakcyjnym pojęciom formę wyobrażeń wzrokowych. Taki pokaz, tworząc warunki jednoczesnego odbierania wrażeń przez kilka receptorów, przyśpiesza procesy poznawcze.

METODY SŁOWNE

40 **Metody słowne najogólniej można podzielić na dialogowe, polegające na rozmowie prowadzącego zajęcia ze szkolonymi oraz monologowe**. Poniżej dokonano charakterystyki wykładu, pogadanki, dyskusji, opowiadania, pracy z książką i treningu interpersonalnego.

41 **Wykład** budzi duże zainteresowanie ze względu na wielość jego dydaktycznych konstrukcji, jak również powszechność stosowania w szkoleniu. Celem wykładu jest przekazanie szkolonym określonych informacji, zaś jego przedmiotem jest przeważnie opis złożonych układów rzeczy, zjawisk, wydarzeń i procesów oraz zachodzących między nimi związków i zależności, głównie o charakterze przyczynowo-skutkowym. Do skutecznego korzystania z wykładu należy wdrażać młodzież, a proces ten powinien polegać na: zaznajamianiu z celem, tematem i podtematami wykładu; systematycznym kontrolowaniu sporządzanych przez szkolonych notatek z wykładu; rygorystycznej kontroli i ocenie treści oraz zakresu przyswajanych przez nich informacji.

42 Dobrze przygotowany i przeprowadzony wykład pozwala te braki w dużej części wyeliminować, tkwią one bowiem nie tyle w samej metodzie wykładu, co w niewłaściwym i nieumiejętnym jej stosowaniu. Uzyskanie wysokich wyników zajęć prowadzonych metodą wykładu wymaga od wykładowcy:
- dbałości o naukowy poziom wykładu oraz dokonania prawidłowej analizy przedstawionych faktów, wyciągnięcia wniosków i uogólnień;
- logicznego i konsekwentnego przekazu przygotowanych treści;
- dbałości w wywodach, a zwłaszcza udowodnienia słuchaczom prawdziwości podawanych faktów i uogólnień;
- utrzymywania kontaktu psychicznego ze słuchaczami w toku podawania nowych treści;
- nawiązywania – przy wyjaśnianiu nowych zagadnień – do dotychczasowych doświadczeń zawodowych i społecznych słuchaczy, do wcześniej nabytych przez nich wiadomości

i opanowanych umiejętności;
- wykład powinien kończyć się podsumowaniem oraz wysunięciem problemów, które powinny być przedyskutowane ze słuchaczami.

43 **Pogadanka** należy do powszechnie stosowanych metod w szkoleniu. Jej istota polega na rozmowie prowadzącego zajęcia ze szkolonymi, przy czym ten pierwszy jest w tej rozmowie osobą kierującą. Pogadanka zatem zmusza szkolonych do samodzielnej pracy myślowej.

Zajęcia dydaktyczne prowadzone są metodą pogadanki wówczas, gdy zagadnienia, o których zamierzamy mówić, są zbyt skomplikowane, jeżeli szkoleni nie są w stanie zrozumieć określonych treści ani podczas wykładu, ani podczas samodzielnego studiowania dostępnych materiałów. Stosujemy ją zarówno przekazując nowe treści, jak i przy jego utrwalaniu i kontrolowaniu wyników.

44 **Dyskusja**, której istotą jest wymiana poglądów na określony temat. Jej prowadzenie polega na wymianie zdań między prowadzącym zajęcia a szkolonymi lub tylko między szkolonymi. Wartości dydaktyczno-wychowawcze tej metody wynikają stąd, że wymaga ona od szkolonych nie zwykłych odpowiedzi, lecz rozwiniętych i wartościujących wypowiedzi, merytorycznego uzasadnienia własnego stanowiska oraz jasnego i zwięzłego przedstawienia własnych poglądów.

45 **Opowiadanie** to metoda, której cechą charakterystyczną jest przedstawienie pewnego konkretnego wydarzenia w sposób ciągły, barwny i żywy. Opowiadanie pełni swoją funkcję dydaktyczno-wychowawczą jedynie wówczas, gdy wybrany temat do prowadzenia tą metodą zapewni zainteresowanie odbiorców, które możemy uzyskać poprzez plastyczność i jasność odtwarzanego zjawiska czy wydarzenia. Niezbędnym elementem wysokiej skuteczności tej metody jest właściwa modulacja głosu przez prowadzącego, zaś język powinien być zrozumiały i odpowiednio zabarwiony uczuciowo. Sposób jej prowadzenia powinien wywoływać wśród podwładnych odpowiednie przeżycia i wpływać na kształtowanie się pożądanych postaw. W toku jej prowadzenia zaleca się stosowanie pytań.

46 **Praca z książką** jest metodą, której sposoby wynikają z funkcji, jakie spełnia podręcznik, skrypt, instrukcja, regulamin itp. teksty drukowane. Jej przebieg może mieć różnorodny charakter; w każdym z nich powinno sporządzić się plan przeczytanego tekstu oraz uczynić odpowiednie notatki. Są one przydatne w czasie odtwarzania poznanych treści oraz w porządkowaniu przeczytanego materiału w określoną funkcjonalną całość.

47 **Trening interpersonalny** należy do metod bardzo rzadko stosowanych i mało znanych, zwany jest niekiedy „metodą ćwiczenia wrażliwości na sprawy otoczenia". Cele tej metody najczęściej dotyczą nabycia kwalifikacji w zakresie rozwiązywania spraw międzyludzkich i właściwego postępowania z ludźmi oraz poznania samego siebie i krytycznej oceny własnego postępowania. Metoda ta jest szczególnie zalecana do stosowania w czasie szkolenia i doskonalenia kwalifikacji kadry zarządzającej wszystkimi szczeblami dowodzenia.

METODY WALORYZACYJNE

48 Z doznaniami intelektualnymi procesu kształcenia mają związek przeżycia emocjonalne i ich ocena. **Miejsce i rola metod waloryzacyjnych polega na tym, iż mają zasadniczy wpływ na system wartości i ideałów życiowych**. Metody te charakteryzują się bogactwem odmian, gdyż w zależności od rodzaju wartości mogą się zmieniać.

Wśród nich wymienia się metody impresyjne i ekspresyjne.

49 **Metody impresyjne**, charakteryzujące się organizowaniem uczestnictwa dzieci, młodzieży i dorosłych w odpowiednio eksponowanych wartościach: społecznych, moralnych, estetycznych, naukowych i innych. Organizacja zajęć zgodnie z tymi metodami polega na tworzeniu sytuacji dydaktycznych, w których uczniowie:

1. zdobywają informacje o dziele eksponowanym i jego twórcy;
2. w toku ekspozycji dzieła w pełni mogą się skupić;
3. wyrażają główną ideę dzieła przez stosowanie odpowiednich form aktywności własnej:
4. konfrontują jej założenia z zasadami postępowania i w jej toku wyprowadzają wnioski praktyczne co do ich własnych postaw i własnego postępowania.

50 **Metody ekspresyjne** polegają na stwarzaniu sytuacji, w których uczestnicy sami poprzez własną aktywność twórczą wytwarzają bądź odtwarzają dane wartości, wyrażając niejako siebie, a zarazem je przeżywają.

METODY PRAKTYCZNE

51 **Ćwiczenie polega na wielokrotnym wykonywaniu jakiejś czynności dla nabycia wprawy i uzyskania sprawności (aż do osiągnięcia biegłości lub wyrobienia nawyków) przede wszystkim w działaniach psychomotorycznych.** Trzeba jednak w tym miejscu dodać trzy, tyleż oczywiste co ważne spostrzeżenia:

1. wraz ze zwiększeniem materiału wzrasta czas potrzebny na opanowanie jednego elementu;
2. o utrwalaniu materiału przez powtarzanie można mówić wówczas, gdy został on już przyswojony;
3. rozłożenie powtórzeń w czasie jest bardziej efektywne aniżeli uczenie się skomasowane.

52 Przypuszcza się jednak, że sposób uczenia się w tym aspekcie jest zróżnicowany ze względu na indywidualne preferencje[31]. Całość (materiału, działania) jest zwykle bardziej sensowną strukturą niż poszczególne jej części. Z drugiej strony, w wypadku uczenia się całościowego cele są odleglejsze – uczący się nie dostrzega w ciągu długiego czasu efektów swego wysiłku.

53 Ćwiczenie w najogólniejszym ujęciu może być zatem uważane za jedną z metod opanowywania umiejętności polegającą na powtarzaniu jakiejś czynności lub jej fragmentu, albo też ciągu czynności składających się na działanie. W pierwszym przypadku ćwiczenie prowadzi do opanowania umiejętności i jest przygotowaniem do odpowiednich czynności, w drugim – do jej doskonalenia i nabywania wprawy wykonawczej. W tym drugim przypadku idzie o przyspieszenie wykonawstwa, które podlega pomiarowi (np. pokonanie toru przeszkód w odpowiednim czasie, zajęcie stanowiska itp.).

54 Ćwiczenie może się odnosić do umiejętności umysłowych i wtedy podlega na opanowywaniu lub usprawnianiu czynności umysłowych albo też do umiejętności praktycznych. I w pierwszym, i w drugim przypadku ćwiczeń doskonalących możliwe jest zastosowanie maszyn treningowych (trenażerów), pozwalających bądź na opanowanie, bądź na doskonalenie umiejętności.

55 Staje się ono podstawą uzyskania umiejętności wprawy i doświadczeń. Ćwiczenia mogą być też rozumiane jako rodzaj materiału nauczania, który wykładowca przekazuje uczniom do bezpośredniego

[31] A. Matczak, *Style poznawcze*, w: Z. Włodarski, A. Matczak, *Wprowadzenie do psychologii*, WSiP, Warszawa 1987, s. 362.

wykonania w procesie szkolenia. Ten rodzaj materiału nauczania wymaga zazwyczaj samodzielnych obserwacji dokonywanych przez uczniów w trakcie prowadzonych doświadczeń. Wszystkie ćwiczenia przedstawione w programach szkolenia można ująć w trzech podstawowych grupach:

1) ćwiczenia wyrabiające umiejętności zastosowania przyswojonej wiedzy;
2) ćwiczenia służące wyrabianiu umiejętności twórczego zastosowania wiadomości i umiejętności;
3) ćwiczenia charakteru poszukiwawczego.

56 **Metody problemowe**, nazywane też nauczaniem problemowym, są metodą kompleksową kształcenia. Podkreśla się, że jest to odrębna metoda, czy nawet organizacja procesu nauczania[32]. Metody problemowe ze względu na swoje właściwości, w istotnym stopniu przyczyniają się do rozwijania zdolności poznawczych oraz samodzielnego myślenia.

57 Duża swoboda w interpretacji podstawowych pojęć ściśle związanych z istotą kształcenia problemowego powoduje wiele nieporozumień. Kształcenie problemowe, bądź też problemowo-zespołowe i uczenie się problemowe stanowią pewną nazwę skrótową. Jeżeli mówimy o uczeniu się problemowym, mamy zazwyczaj na myśli taki proces poznawczy, w czasie którego uczniowie pod wpływem własnej aktywności i świadomego wysiłku umysłowego dostrzegają, formułują i samodzielnie rozwiązują zadania, bądź to za pomocą określonych algorytmów operacji myślowych, bądź też samodzielnych prób poszukiwawczych.

58 **Sytuację problemową tworzy się przez nawiązywanie do znanych wiadomości, doświadczeń i przeżyć oraz uświadomienie sobie braku wiadomości lub umiejętności w określonym zakresie.** Ta niewiedza zostaje sformułowana w postaci pytania-problemu głównego, które jest podstawą sytuacji problemowej.

Przy stosowaniu nauczania problemowego należy uwzględniać następujące założenia:

- organizacja zajęć musi być szczególnie dobrze przemyślana;
- uczestnicy zajęć powinni się dobrze przygotować do rozwiązania problemu;
- przeznaczyć określony limit czasu na przebieg tych zajęć, gdyż rozwiązanie sytuacji bywa często czasochłonne.

Metody problemowe stosowane w toku zajęć w istotnym stopniu przyczyniają się do rozwijania samodzielnego myślenia i podejmowania decyzji. Przygotowują kształconych do samodzielnych poszukiwań badawczych i samokształcenia. Pobudzają i rozwijają zainteresowanie.

59 **Metoda sytuacyjna** należy do metod aktywizujących i jest swoistą odmianą metody problemowej. Jej cechą charakterystyczną jest przedstawienie wybranej konkretnej sytuacji do rozwiązania. Dlatego też celem stosowania tej metody jest doskonalenie umiejętności analizowania określonych informacji oraz podejmowania decyzji optymalnych. Zajęcia prowadzone tą metodą dają największe efekty wówczas, gdy ich uczestnicy dokonują samodzielnie, chociaż pod kierunkiem prowadzącego zajęcia, analizy sytuacji, gdy przedyskutują możliwe rozwiązania problemu i wybiorą optymalne rozwiązanie. Odmianą analizowanego postępowania jest metoda przypadków, której cechą charakterystyczną jest skromniejszy zestaw wiadomości przekazywanych szkolonym.

60 **Metoda inscenizacji**, należąc do symulacyjnych metod nauczania jest odmianą metody problemowej, a jej celem jest doskonalenie umiejętności odpowiednich zachowań i działań w kontaktach z uczniami w sytuacjach konfliktowych.

[32] W. Okoń, *U podstaw problemowego uczenia się*, PZWS, Warszawa 1964.

Zajęcia prowadzone tą metodą wymagają od uczestników odgrywania ról społeczno-zawodowych na podstawie przygotowanej uprzednio sytuacji problemowej, jak również odpowiednich ról, które trzeba odegrać, mając podane tylko ogólne wskazówki dotyczące zachowań i postaw poszczególnych osób.

61 **Burza mózgów** (giełda pomysłów) jest techniką zespołowego i twórczego myślenia nad rozwiązaniem sytuacji problemowej poprzez zgłoszenie możliwie największej liczby pomysłów (nawet nierealnych i fantastycznych), które następnie są poddawane ocenie i selekcji. Wszystkie pomysły zostają wzięte pod uwagę w czasie podejmowania decyzji o rozwiązaniu problemu. Następnie przystępuje się do wyboru wariantu optymalnego.

KSZTAŁCENIE WIELOSTRONNE

62 OGÓLNA CHARAKTERYSTYKA KSZTAŁCENIA WIELOSTRONNEGO

Z przedstawionymi powyżej metodami ściśle powiązane jest kształcenie wielostronne, będące rodzajem nauczania, w którym stosuje się zróżnicowane metody i środki, umożliwiające uczącym się zarówno przyswajanie gotowych wiadomości, jak i rozwiązywanie problemów teoretycznych i praktycznych, a zarazem przeżywanie treści naukowych, społecznych, moralnych i estetycznych oraz bezpośredni udział w przekazywaniu warunków otoczenia.

63 Teoria kształcenia wielostronnego odnosi się więc do rozwoju człowieka, dokonującego się pod wpływem kształcenia, a więc wszelkiego (nie tylko szkolnego) nauczania i uczenia się. Chodzi w niej zarówno o rozwój poszczególnych jednostek poddanych edukacji, jak pośrednio o rozwój całych pokoleń, stopniowo wpływający na postęp w życiu społecznym. Koncepcja ta przeciwstawia się tym koncepcjom pedagogicznym, które traktują wychowującą się jednostkę jako zbiór pewnych cech, które to cechy poddaje się manipulacjom pedagogicznym.

Wielostronność kształcenia wyraża się nie tylko w respektowaniu czterech kategorii uczenia się i nauczania, ale również w zróżnicowanych formach pracy młodzieży. Działanie praktyczne podnosi atrakcyjność pracy szkolnej, korzystnie wpływa na strukturę społeczną klasy szkolnej i ma istotny wpływ na wyniki procesów edukacyjnych.

64 TRZY RODZAJE AKTYWNOŚCI CZŁOWIEKA

Osobowość ucznia należy traktować jako stopniowo harmonizującą się całość, oddziałując na nią i uruchamiając własne siły jednostki poprzez trzy funkcje, które pełni. Zalicza się do nich poznawanie świata i siebie, przeżywanie świata i nagromadzonych w nim wartości oraz zmienianie świata. Te trzy typowo ludzkie funkcje leżą u podstaw teorii kształcenia wielostronnego. Funkcjom tom odpowiadają trzy **rodzaje aktywności: intelektualna, emocjonalna i praktyczna.**

Aktywność intelektualna w procesie nauczania-uczenia się może być przejawiana w dwojaki sposób. Po pierwsze – przyswajanie wiedzy przekazywanej przez nauczycieli i po drugie – samodzielne rozwiązywanie własnych problemów.

Aktywność emocjonalna polega na przeżywaniu wartości poznawczych, moralnych, społecznych, estetycznych i ich wytwarzaniu.

Aktywność praktyczna charakteryzuje się przekształcaniem rzeczywistości zgodnie z określonymi celami.

65 Poznawanie rzeczywistości a przyswajanie wiedzy

Poznawanie rzeczywistości następuje przez uczenie się poznawcze, występujące

w trzech odmianach:
- uczenie się spostrzeżeniowe;
- warunkowanie sensoryczne;
- nabywanie wiedzy, będące najważniejszą odmianą uczenia się poznawczego.

Na pośrednim i bezpośrednim poznawaniu rzeczywistości, a więc konkretnych rzeczy, procesów i zdarzeń oraz zachodzących między nimi związków i zależności, opiera się działalność poznawcza. Następuje ona więc w naturalnych warunkach i sytuacjach. Poznanie bezpośrednie stanowi podstawę do poznawania pośredniego, o charakterze abstrakcyjnym, a więc pozbawionym konkretności.

W poznawaniu rzeczywistości wyróżnić można kilka momentów nauczania, do których należy zaliczyć:
1. część wstępną;
2. sprawdzenie pracy domowej;
3. pogadankę wstępną;
4. podanie nowego materiału;
5. utrwalenie nowych wiadomości;
6. zastosowanie nowych wiadomości,
7. objaśnienie pracy domowej[33].

W strukturze zajęć, rozumianej jako forma przygotowanego planu, zgodnie z poglądem Cz. Kupisiewicza, można wymienić:
„1) czynności przygotowawcze, np. sprawdzenie poziomu wiedzy wstępnej;
2) czynności podstawowe, których rodzaj jest zdeterminowany przez dominującą funkcję dydaktyczną zajęć;
3) czynności końcowe: utrwalenie materiału[34].
4) Zalecenie samodzielnej pracy.
5) Działalność odkrywcza

Ważną częścią kształcenia wielostronnego jest samodzielne poznawanie świata w toku rozwiązywania problemów. Powstanie sytuacji problemowej, wyreżyserowanej przez nauczyciela lub spontanicznie stworzonej przez uczniów, staje się pierwszym etapem procesu rozwiązywania problemu dydaktycznego.

Na cykl kreatywnego działania człowieka składa się pięć etapów:
1. wyszukanie lub wyznaczenie problemów.
2. pogrążenie lub przygotowanie (wyszukanie informacji oraz wysunięcie hipotez);
3. inkubacja (odprężenie i podświadome przemyśliwanie nad zebranym materiałem, podświadomie układa fakty w nowe wzory);
4. zrozumienie lub olśnienie (w najmniej oczekiwanym momencie nowy pomysł, który należy szybko zanotować, bo można o nim zapomnieć);
5. weryfikacja i zastosowanie (udowodnienie za pomocą eksperymentu lub logicznego rozumowania, że pomysł może rozwiązać dany problem)[35].

Technologia umysłowego generowania, rozwinięcia i wdrożenia innowacyjnego pomysłu do praktyki w pełni pokrywa się z fazami procesu twórczego przedstawionymi w rodzimej literaturze psychologicznej.

66 PRZEŻYWANIE WARTOŚCI A AKTYWNOŚĆ EMOCJONALNA

Koncepcja kształcenia wielostronnego w szerszym stopniu niż inne koncepcje uwzględnia problematykę uczenia się przez przeżywanie. Uczenie się przez przeżywanie polega na stwarzaniu takich sytuacji w pracy szkolnej i pozaszkolnej, w których ma miejsce wywoływanie przeżyć emocjonalnych (i poznawczych) u wychowanków – pod wpływem odpo-

[33] W. Okoń, *Organizacyjne formy nauczania*, w: *Zarys pedagogiki*, t. 2, PWN, Warszawa 1959, s. 407.

[34] Cz. Kupisiewicz, *Podstawy dydaktyki ogólnej*, PWN, Warszawa 2010, s. 236.

[35] Por. J. A. F. Stoner, Ch. Wankel, *Kierowanie*, PWN, Warszawa 1989.

wiednio eksponowanych wartości.

W teorii wszechstronnego kształcenia przeżywanie wartości i aktywność emocjonalna jest więc najważniejszym elementem strategii emocjonalnej. Podstawową częścią tej zajęć jest jednorazowa lub dwukrotna ekspozycja utworu, która zajmuje dowolną część zajęć. W tym czasie mogą być eksponowane wiersze (poezja), dzieła muzyczne, obrazy malarskie i inne wytwory sztuk plastycznych.

W związku z powyższym najczęściej proponuje się następującą strukturę takich zajęć:

1. organizacja klasy i przygotowanie do pracy;
2. przygotowanie utworu, który będzie eksponowany;
3. eksponowanie utworu z wykorzystaniem środków technicznych;
4. analiza i zrozumienie utworu w wyniku wspólnych poszukiwań odpowiedzi, dyskusji czy przedstawienia indywidualnych odczuć;
5. podsumowanie rezultatów pracy, korekta niewłaściwych interpretacji, zwrócenie uwagi na indywidualność przeżyć i zakres rozumienia itd.;
6. końcowa ekspozycja całości lub wybranego fragmentu zamykająca lekcję.

Efekty uczenia się przez przeżywanie, ze względu na głębokie zapadanie w świadomość, mają duże znaczenie dla rozwoju osobowości uczniów, młodzieży ale także dorosłych (przyp. red.). Obejmuje ono poznanie, zwłaszcza podmiotowe, a więc związane z uczeniem jako przedmiotem poznania i w ogóle człowiekiem, jego czynami i twórczością oraz całą kulturą.

67 **DZIAŁANIE I DZIAŁALNOŚĆ PRAKTYCZNA**

Działanie jest to mniej lub bardziej złożony układ czynności realizowanych świadomie, których celem jest przystosowanie się do otoczenia lub jego zmiana. Działanie jest zachowaniem się celowym i świadomym; jest przejawem aktywności człowieka, podstawą jego rozwoju. Zakłada się, że jeżeli dany podmiot w danej chwili działa, to w tej samej chwili wie, jak się zachowuje – jakie wykonuje ruchy lub co myśli itd.[36]. Do poszczególnych rodzajów działania ludzkiego można zaliczyć – poza snem i odpoczynkiem – zabawę, uczenie się, pracę.

68 Rozwój osobowości dokonuje się także poprzez działalność praktyczną, znajdującą wyraz w procesach uczenia się przez działanie. Wielostronne stosowanie metod w kształceniu umiejętności praktycznych pozwala uwzględnić zróżnicowanie doświadczenia uczniów oraz ułatwia im opanowanie niezbędnej wiedzy i umiejętności praktycznych, przy czym efektywność nauczania i uczenia się przez działanie w dużym stopniu zależy od przygotowania teoretycznego. Dlatego też w pierwszej części modelu zajęć znajduje się ogniwo zwane wprowadzeniem, polegające na uświadomieniu uczniom znaczenia nauczanej umiejętności w całokształcie szkolenia i nabywania umiejętności.

69 W drugim ogniwie zajęć (rozwinięcie tematu) następuje wyposażenie uczniów w określony zasób wiedzy teoretycznej za pomocą instruktażu, który może być prowadzony metodą wykładu, wyjaśnienia, pogadanki, pokazu itp. Prowadzący zajęcia daje nie tylko wzór do naśladowania danej umiejętności, ale jednocześnie objaśnia, co i jak należy robić. Wytworzony na tej drodze w świadomości uczących się model pożądanej czynności ułatwia jej opanowanie.

70 Trzecim ogniwem zajęć jest praktyczna nauka poszczególnych umiejętności. Ich kształtowanie rozpoczyna się od wzorowego pokazu, demonstrowa-

[36] T. Pszczołowski, *Mała encyklopedia prakseologii i teorii organizacji*, PWE, Wrocław-Warszawa-Kraków-Gdańsk 1978, s. 56.

nego przez prowadzącego zajęcia. Jeśli dana umiejętność jest złożona i trudna do opanowania, należy dzielić ją na poszczególne, cząstkowe czynności i dokładnie omawiać w czasie pokazu.

71 Samodzielne ćwiczenie, będące czwartym ogniwem, najlepiej jest dzielić na trzy fazy. W pierwszej ćwiczący próbują samodzielnie, pod nadzorem instruktora, wykonywać poszczególne czynności. Ich systematyczne powtarzanie ma na celu eliminowanie ruchów błędnych i pozwala uchwycić zależności między czynnościami a wynikami. W drugiej fazie doskonali się pewne sprawności, tworzące zespół umiejętności, a w trzeciej całość opanowanych umiejętności.

72 J. Półturzycki daje następującą propozycję struktury lekcji ćwiczeniowej:

I. Część przygotowawcza
1. czynności organizacyjne;
2. sprawdzenie pracy domowej;
3. powtórzenie materiału.

II. Część podstawowa
1. uświadomienie uczniom zadania i podanie tematu;
2. wprowadzenie nowego materiału;
3. pokaz czynności z objaśnieniem;
4. próbne ćwiczenia uczniów;
5. korekta i dodatkowe objaśnienia;
6. ćwiczenia wdrażające;
7. kontrola i korekta wykonywanych ćwiczeń.

III. Część końcowa
1. podsumowanie tematu, omówienie uzyskanych rezultatów;
2. zadanie pracy domowej;
3. uporządkowanie stanowisk i zakończenie lekcji[37].

73 Działalność praktyczna ma duży wpływ na kształtowanie charakteru uczniów. Jest ona jednocześnie terenem zastosowania teorii, nabytych w toku uczenia się poznawczego.

Z kształceniem wielostronnym ściśle powiązane jest problemowe nauczanie-uczenie się.

74 **Nauczanie problemowe opiera się nie na przekazywaniu gotowych wiadomości, lecz na uzyskiwaniu przez uczestników zajęć nowych wiadomości i sprawności za pośrednictwem problemów teoretycznych i praktycznych.** Istota tego nauczania polega więc na powstawaniu sytuacji problemowych, na samodzielnym poszukiwaniu przez uczniów pomysłów ich rozwiązania oraz na sprawdzeniu ich trafności. Jest ono zatem sekwencją takich czynności nauczyciela i uczniów, jak organizowanie sytuacji problemowych i formułowanie problemów, indywidualne lub grupowe ich rozwiązywanie, weryfikacja uzyskanych rozwiązań oraz systematyzowanie, utrwalanie i stosowanie nowo nabytej wiedzy w działaniach umysłowych i praktycznych.

75 Nauczanie problemowe charakteryzuje się następującym cyklem postępowania dydaktycznego:
1. dostrzeganie problemów na podstawie obserwacji określonych rzeczy, zjawisk, wydarzeń lub procesów;
2. formułowanie hipotez zmierzających do rozwiązywania tych problemów, zwłaszcza stawianie pytań o charakterze analitycznym oraz wstępna, niejako przedempiryczna, oceny wysuwanych hipotez;
3. wskazanie logicznych następstw tych hipotez;
4. decydowanie o tym, jakie dane będą niezbędne dla oceny wybranej hipotezy lub hipotez, a także dokonywanie selekcji materiałów źródłowych z punktu widzenia ich przydatności do

[37] J. Półturzycki, *Dydaktyka dla nauczycieli,* Wyd. A. Marszałek, Toruń 1996, s. 226–227.

weryfikacji tej hipotezy czy tych hipotez;
5. analizowanie, interpretacja i ocena danych pod kątem ich zgodności z rozwiązywanym problemem;
6. oceny hipotez w świetle zebranych danych;
7. postępowanie zgodne z hipotezą uznaną za prawdopodobną w świetle czynności wymienionych w poprzednich punktach.
8. Kształcenie wielostronne jest najbardziej wszechstronną koncepcją kształcenia i może być w pełni przydatne w realizacji zajęć, których jakość, skuteczność i atrakcyjność może być wysoka.

ORGANIZACYJNE FORMY KSZTAŁCENIA

76 POJĘCIE ORGANIZACYJNYCH FORM KSZTAŁCENIA

Zewnętrzną, organizacyjną stroną procesu dydaktycznego jest forma kształcenia. Obejmuje ona m.in. takie problemy, jak: dobór uczniów i nauczycieli, tworzenie grup i zespołów oraz zasady współpracy poszczególnych uczniów, czas zajęć, warunki miejsca. Nie można utożsamiać form nauczania z metodami nauczania; metody wskazują, jak uczyć, formy jak organizować pracę dydaktyczną.

Wprowadzenie różnych form kształcenia sprzyja rozwojowi osobowości uczniów, stwarza bowiem wiele nowych sytuacji dydaktyczno-wychowawczych. Najczęściej rozróżnia się formy kształcenia stosowane w toku zajęć lekcyjnych i pozalekcyjnych. Do pierwszej grupy można zaliczyć formy jednostkowe (indywidualne), zespołowe (grupowe) i zbiorowe, zajęcia teoretyczne (np. wykłady, ćwiczenia, seminaria, konsultacje), zajęcia praktyczne (ćwiczenia, zajęcia laboratoryjne, zajęcia sztabowe, zajęcia instruktorsko-metodyczne itp.), wycieczki, itp. W toku zajęć pozalekcyjnych uczniów można wyszczególnić takie formy, jak: nauka własna, praktyki zawodowe, zajęcia poświęcone kontroli i ocenie wyników kształcenia, zwiedzanie muzeów, udział w różnego rodzaju kursach, konferencjach itp.

77 Organizacyjne ramy zajęć dydaktycznych określają tzw. ogniwa procesu nauczania. Ich analiza umożliwia jednak ukazanie zaledwie dróg metodycznej pracy nauczyciela w obrębie już przyjętej formy organizacyjnej. Stąd też istnieje interpretacja formy nauczania w skalach: mikro i makro.

78 W szkoleniu ze względu na przyjmowane cele i realizowane zadania wyróżnia się formy przyjmowane w środowisku cywilnym, jak i te, które są specyficzne dla tej edukacji.

Do najczęściej wymienianych form zaliczyć można:

- jednostkowe (indywidualne);
- zespołowe (grupowe);
- zbiorowe.

Ponadto można dokonać także podziału form na:

- teoretyczne (wykłady, ćwiczenia, seminaria, konsultacje);
- praktyczne (ćwiczenia, zajęcia laboratoryjne, zajęcia sztabowe, zajęcia instruktorsko-metodyczne, podróże specjalistyczne, wycieczki itp.).

79 CHARAKTERYSTYKA LEKCJI (JEDNOSTKA ZAJĘĆ)

Lekcja wg Cz. Kupisiewicza, będąc głównym elementem klasowo-lekcyjnego systemu pracy dydaktycznej, „określa nie tylko czas pracy nad tematami, na które podzielony jest materiał programowy, lecz wpływa również na tok kształcenia, tzn. na rozkład w czasie poszczególnych działów programu oraz związanych z nimi zadań dydaktycznych”[38]. Jest to zatem sposób organi-

[38] Cz. Kupisiewicz, *Podstawy dydaktyki ogólnej*, Wyd. PWN, Warszawa 1976, s. 234.

zowania procesu nauczania i uczenia się, wyrażający się w zachowaniu określonego układu składowych elementów tego procesu, zwanych ogniwami lekcji. Lekcja szkolna przeprowadzana jest w pewnej jednostce czasu, w godzinie lekcyjnej, w nauce zbiorowej, przy ograniczonym wymiarze treści nauczania, przy czym uczenie się uczniów jest tu kierowane w sposób nieprzerwany przez nauczyciela.

Typy lekcji przejawiają się w jej odmianach. Możliwe są tu dwa wypadki. Jeden z nich polega na tym, że pewne ogniwa ogólnej budowy lekcji nie są uwzględniane, a inne rozszerzają się ich kosztem, lub też, że częściowo zmienia się ich kolejność wraz z metodą nauczania. W różnych typach lekcji występuje łączenie dwóch odmian uczenia się, uczenia się sztucznego i naturalnego, często łączonego ze zmienionym organizowaniem lekcji w klasie.

80 CZTERY TOKI KSZTAŁCENIA

Ze względu na przebieg typowych czynności w toku zajęć możemy wyróżnić **toki (strategie), stanowiące podstawę struktur jednostek metodycznych**, a zarazem części ogólniejszych toków (strategii) dydaktycznych.

81 Pierwszym z tych toków jest **przyswajanie wiedzy** w „gotowej" postaci, które obejmuje następujące ogniwa (momenty, fazy):

- zetknięcie z nowym materiałem;
- skojarzenie go z wiadomościami wcześniej nabytymi;
- uporządkowanie nowej wiedzy;
- zastosowanie jej w nowych sytuacjach.

82 Drugi – polegający na **samodzielnym dochodzeniu do nowej wiedzy** przez rozwiązywanie zagadnień, opiera się na następującym modelu:

- znalezienie się uczącego w sytuacji problemowej i sformułowanie wynikających z niej pytań;
- sprecyzowanie na podstawie samodzielnych poszukiwań odpowiedzi na te pytania (hipotezy);
- ich teoretyczne lub praktyczne sprawdzenie (weryfikacja);
- zastosowanie wiadomości w nowych sytuacjach.

83 Trzeci z nich obejmuje **uczenie się działań**. Zalicza się do nich:

- poznanie celu działania (czynności) oraz jednej lub więcej reguł, które mają być zastosowane w działaniu;
- ustalenie jego modelu;
- pokaz działania wzorowo wykonanego;
- pierwsze, dokładnie kontrolowane próby szkolonych;
- ćwiczenia w sprawnym wykonywaniu całości działania;
- samodzielne wykonanie działania (czynności) przez szkolonych. W modelu tym ukierunkowanym na przekształcanie rzeczywistości można wyróżnić dwie fazy działania: orientacyjną (ukierunkowującą) i operacyjną, rozumianą jako praktyczne działanie, a niekiedy też jej charakter jest intelektualny.

84 Ostatni tok pozwala emocjonalnie **oddziaływać na postawy i uczucia szkolonych**. Jego istota polega na eksponowaniu wartości i kształtowaniu ocen moralnych, społecznych, estetycznych, politycznych i religijnych w celu tworzenia odpowiedniego stosunku do nich, jak również kształtowania własnego systemu wartości.

W modelu tym można wyróżnić:

- kontakt z dziełem;
- jego eksponowanie;
- analizę problemową wartości i ich ocenę;
- umiejscowienie dzieła na tle dorobku;
- aktywność własną uczniów i ewentu-

alne wnioski praktyczne dotyczące ich własnych postaw.

85 **ORGANIZACJA PRACY UCZNIÓW NA LEKCJI**

W zakresie form organizacyjnych zajęć dydaktycznych możemy wyróżnić trzy zasadnicze rodzaje pracy kształcone w toku ich trwania: pracę jednostkową, pracę grupową i pracę zbiorową. Ich wybór zależy od charakteru przedmiotu (teoretyczny czy praktyczny), celu i zadań zajęć, potrzeby kształtowania umiejętności działania zespołowego itp.

86 **Praca jednostkowa** charakteryzuje się tym, że szkolony sam realizuje swoje zadania wynikające z wymogów określonych w programach, jak również poleceń prowadzącego zajęcia. Najczęściej jest ona spotykana w toku zajęć przeznaczonych na wykonanie samodzielnych zadań, jak również ich kontrolę i ocenę.

87 **Praca grupowa** stanowi formę pośrednią pomiędzy już wspomnianą a pracą zbiorową. Jej istota polega na wzbogaceniu wymienionych form, gdyż funkcjonujące w sposób twórczy zespoły stanowią rozwiązanie pośrednie pomiędzy nimi. Niezwykle ważne są walory wychowawcze jej stosowania, w związku z tym, że ma ona na celu kształtowanie przekonań naukowych, przeżywanie rozwiązywanych problemów, swobodę funkcjonowania w zespołach szkolonych, jak również wytwarzanie więzi.

88 **Praca zbiorowa** (frontalna) polega na realizacji wspólnego dla wszystkich programu kształcenia, tych samych zadań dydaktyczno-wychowawczych przez wszystkich szkolonych. Zajęcia te umożliwiają obok realizacji wspólnego programu także właściwy rozwój społeczny szkolonych, zapobiegają dezintegracji czy atomizacji zespołów klasowych. Tok ten charakteryzuje się też ograniczonymi możliwościami aktywizacji poszczególnych uczestników zajęć.

O efektywności poszczególnych toków czy też zajęć, w których występują elementy wielu z nich, decydują m.in.:

1. dobre przygotowanie pedagogiczne i merytoryczne nauczyciela;
2. dokładne sprecyzowanie tematu zajęć;
3. precyzyjne określenie celów zajęć;
4. dobór właściwych metod nauczania;
5. zastosowanie różnych środków dydaktycznych.

Najbardziej skutecznymi formami zajęć mogą być zajęcia grupowe, w których stosując odpowiednie metody, zapewni się optymalne wyniki kształceniowe.

ROLA TECHNOLOGII INTERAKTYWNYCH I MEDIÓW CYFROWYCH W TOKU ZAJĘĆ

89 **Funkcje mediów cyfrowych w kształceniu**

Środki dydaktyczne w procesie kształcenia mogą pełnić następujące funkcje:

1. służą bezpośredniemu poznawaniu przez szkolonych określonych fragmentów rzeczywistości (funkcja poznawcza);
2. są narzędziem rozwijania zdolności poznawczych oraz uczuć, woli i aktywności młodzieży (funkcja kształcąca);
3. stanowią istotne źródło zdobywanych przez kształcących się wiadomości i umiejętności, utrwalenie poznanych już treści, weryfikację hipotez, sprawdzenie stopnia opanowania wiedzy i umiejętności itp. (funkcja dydaktyczna);
4. przyspieszają przebieg informacji i ułatwiają tworzenie z nich układów ustrukturalizowanych, szczególnie przez odwołanie się do różnego rodzaju schematów i grafów[39].

[39] Cz. Kupisiewicz, *Podstawy dydaktyki*, op.cit., s. 213–214; W. Okoń, *Wprowadzenie do dydaktyki*, op.cit.

Powyższe funkcje wyznaczają miejsce i rolę środków w ułatwianiu i pogłębianiu:

1. poznawania rzeczywistości;
2. poznawania wiedzy o rzeczywistości;
3. kształtowania postaw i emocjonalnego stosunku do rzeczywistości;
4. rozwijania działalności przekształcającej rzeczywistość[40].

90 Obecnie rozwój nowoczesnych technik informacji, upowszechnienie środków masowej komunikacji, coraz wyraźniejsze ich powiązania z edukacją **wyznaczają nowe obszary technologii kształcenia w szkolnictwie**. Do najważniejszych z nich należy zaliczyć:

1. określenie celów kształcenia, a zwłaszcza formułowanie celów operacyjnych szkolenia;
2. strukturalizację treści programowych oraz przekazywanych przez mass-media, które zawładnęły edukacją współczesnej młodzieży;
3. tworzenie i udostępnianie nowych źródeł wiedzy (drukowanych), jak i niedrukowanych, audiowizualnych (telewizyjnych, komputerowych itp.);
4. wzbogacanie i uatrakcyjnianie interakcji pomiędzy prowadzącym zajęcia dydaktyczne a szkolonymi;
5. przygotowanie do korzystania z nowoczesnych technik i technologii gromadzenia i przekazu informacji;
6. indywidualizację kształcenia dzięki możliwościom korzystania przez każdego szkolonego z nowych technologii kształcenia;
7. doskonalenie kontroli i oceny procesu nauczania-uczenia się.

91 **FUNKCJE I ZADANIA KOMPUTERA**

Kształcenie wspomagane komputerowo ma na celu usprawnienie procesu kształcenia poprzez jego wzbogacenie oraz podniesienie jakości.

92 Dwa podstawowe rodzaje kształcenia wspomaganego komputerem:

1. kształcenie podstawowe (wykorzystanie komputera w całości lub w części przewidzianego cyklu tematycznego lub całego kursu);
2. kształcenie uzupełniające (komputer do wzbogacenia, wizualizacji lub uatrakcyjnienia określonej sytuacji lekcyjnej).

93 Dwie grupy strategii kształcenia wspomaganego komputerem:

1) podstawowe (przyczyniają się do przekazywania określonej wiedzy, umożliwiając uczącemu się wiązanie wiadomości oraz ich przetwarzanie). W ich ramach wyróżnić można dwie strategie:
   a) strategia przetwarzania materiału;
   b) strategia aktywnej nauki;
2) pomocnicze (uzupełniają, wspierają i wzbogacają określone sytuacje dydaktyczne) obejmujące strategie systemowego uczenia się: metanauczanie, strategie monitorujące itp.

94 Inny podział strategii:

1. mechanicznego kształtowania nawyków (automat ćwiczący określoną umiejętność);
2. korepetycyjna (dialog użytkownik – komputer);
3. symulacyjna (przedstawienie fikcyjnej sytuacji świata);
4. modelowania (przedstawienie sytuacji świata rzeczywistego).

95 **ZASADY DOBORU MEDIÓW CYFROWYCH**

Przedstawienie reguł i zasad posługiwania się środkami dydaktycznymi, a także odpowiednimi materiałami dydaktycznymi w toku zajęć jest zadaniem trudnym i złożonym,

[40] W. Okoń, *Wprowadzenie do dydaktyki*, op.cit., s. 314.

ze względu na odmienność celów i treści kształcenia, jak również specyfikę stosowanych urządzeń i prezentowanych pomocy.

96 **ZASADY OGÓLNE**

Do najbardziej ogólnych zasad i reguł można zaliczyć te, które są podporządkowane celowości użycia technologii i aplikacji multimedialnych. Zasada ta wymaga od wszystkich prowadzących zajęcia dydaktyczne precyzyjnego określenia celu i zadań prezentowanych materiałów.

A oto one:

1. Znajomość sprzętu i materiałów stosowanych na zajęciach.
2. Przedstawiane treści muszą być ściśle powiązane z tematem (zagadnieniami) zajęć. Ich dobór nie może być przypadkowy.
3. Celowe jest sprawdzenie sprawności i funkcjonalności poszczególnych środków dydaktycznych przed zajęciami, na których będą stosowane.
4. Należy nauczyć uczestników zajęć „umiejętności" odbioru prezentowanych treści, a także w miarę możliwości samodzielnego korzystania z nich i posługiwania się nimi.
5. W czasie prezentowania treści należy ukierunkować uwagę kształconych i pobudzać ich do wnikliwej obserwacji i myślenia, co wpływa na rozwój logicznego myślenia i rozumowania.
6. Czas przedstawiania materiałów dydaktycznych powinien być uzależniony od stopnia złożoności prezentowanych treści i ich przystępności.
7. W miarę możliwości należy wyjaśniać wszystkie wątpliwości, odpowiadać na pojawiające się pytania.
8. Korzystanie w toku zajęć z różnych materiałów powinno być z sobą skorelowane i wzajemnie uzupełniane, co ożywi zajęcia i w znacznym stopniu osłabi umysłowe zmęczenie, przyczyniając się w ten sposób do wzrostu aktywności.
9. Bez uzasadnienia środki (materiały) bardziej proste nie powinny być zastępowane przez środki (materiały) złożone.

97 **METODYCZNE REKOMENDACJE WYKORZYSTANIA TECHNOLOGII KSZTAŁCENIA W TOKU ZAJĘĆ**

Metodyczne rekomendacje wykorzystania środków technicznych w toku zajęć dydaktycznych przedstawione będą w trzech podstawowych etapach, jakimi są ich przygotowanie, realizacja i zakończenie.

98 **Przygotowanie zajęć**

- dokonać analizy celów, zadań i treści zajęć dydaktycznych;
- sprecyzować rolę i miejsce wybranych środków i materiałów dydaktycznych w realizacji zajęć;
- sprawdzić tytuły posiadanych materiałów dydaktycznych i ich przydatność w realizacji określonego tematu;
- przygotować niezbędne materiały dydaktyczne (w przypadku ich braku);
- sprawdzić jakość materiałów dydaktycznych i sprawność środków technicznych;
- wyznaczyć wybranym bądź przygotowanym materiałom określone zadania dydaktyczne;
- szczegółowo ustalić kolejność i sposoby ilustrowania omawianych problemów środkami poglądowymi;
- dokonać przeglądu sali, w której będą prowadzone zajęcia pod kątem pełnego wykorzystania przygotowanych materiałów i środków dydaktycznych.

99 **Prowadzenie zajęć dydaktycznych**

- zapoznać szkolonych z prezentowanymi materiałami i stosowanym w nich słownictwem;
- przedstawić szkolonym przygotowany konkretny „repertuar nastawień i oczekiwań";
- demonstrować pomoce zgodnie z celami i treścią zajęć dydaktycznych;

- ukierunkować uwagę szkolonych na istotne problemy danego materiału dydaktycznego;
- dążyć do rozwijania zainteresowań i spostrzegawczości szkolonych;
- stosować komentarz naprowadzający (zmuszający szkolonego do samodzielnej werbalizacji tego, co ogląda na ekranie);
- respektować zasadę, iż stosowanie środków audiowizualnych powinno skracać czas przekazu informacji;
- demonstrować środki (materiały) dydaktyczne w sposób sprawny i bez wydłużania czasu przeznaczonego na ten cel;
- eksponować (jeśli to możliwe) istotę analizowanego procesu lub zjawiska;
- traktować prezentowanie materiału dydaktycznego jako element logicznej konstrukcji treściowej i metodycznej zajęć;
- dostrzegać zróżnicowanie wyzyskania środków dydaktycznych spełniających funkcję źródła wiedzy, ilustracji przedstawień słownych, sposobu formułowania problemu, środka oddziaływania na emocje słuchaczy.

100 **Podsumowanie zajęć**

- przeprowadzić operacje: analizy, porównania, uogólniania, systematyzacji i przetwarzania opanowanej wiedzy;
- wskazać na możliwości ponownego przejrzenia materiałów dydaktycznych ułatwiających pogłębienie i poszerzenie wiedzy poznanej w toku zajęć dydaktycznych;
- zachęcić do obejrzenia innych materiałów poglądowych wzbogacających tematykę zajęć dydaktycznych.

Aplikacje multimedialne oraz nowe możliwości mediów cyfrowych i technologii interaktywnych zapewnić mogą wyjątkowo wysoką atrakcyjność zajęć dydaktycznych.

PRZYGOTOWANIE ZAJĘĆ DYDAKTYCZNYCH

101 NAUCZYCIEL JAKO ORGANIZATOR PROCESU NAUCZANIA -UCZENIA SIĘ

Nauczyciel to specjalność zawodowa; odpowiednio przygotowany specjalista do prowadzenia pracy dydaktyczno-wychowawczej (nauczającej) w instytucjach (szkołach, przedszkolach, na kursach lub w innych placówkach pozaszkolnych albo szkolnych).

102 W organizacji procesu nauczania-uczenia się nauczyciel spełnia podstawową rolę. S. Wołoszyn akcentuje, iż nauczyciel jest dobrym specjalistą o możliwie gruntownej wiedzy i wyrobionej kulturze naukowej, który potrafi nie tylko „przekazywać wiedzę", ale – co ważniejsze – budzić w młodzieży zainteresowania, wyrabiać nastawienia (chęci) i kształcić umiejętności i nawyki samodzielnego uczenia się, zdobywania wiedzy i doskonalenia własnej kultury intelektualnej (myślenia krytycznego i heurystycznego). Jest organizatorem, animatorem i realizatorem procesu nauczania-uczenia się. Chcąc i umiejąc korzystać z ułatwień, jakie daje mu postęp techniczny, a także chcąc być spolegliwym oraz życzliwym młodzieży wychowawcą i fachowym doradcą rodziców. Sam musi prezentować wartościową osobowość i mieć wyrobioną „otwartą postawę"[41].

103 Niezwykle istotnym elementem nauczyciela jako organizatora procesu nauczania-uczenia się jest jego postawa twórcza. Twórczość bywa różnie interpretowana. Jest wiele desygnatów utożsamiających ją z określonymi pojęciami, do których najczęściej zalicza się: aktywność, pomysłowość, innowacyjność itp. Homoniczność

[41] S. Wołoszyn, *Nauczyciel – przegląd historycznych definicji,* w: *Encyklopedia pedagogiczna*, Fundacja Innowacja, Warszawa 1993, s. 444–445.

twórczości zależy od kontekstu jej użycia, co powoduje dodatkowy chaos interpretacyjny. Mówimy zatem o twórczym zadaniu, twórczym pomyśle, twórczym procesie, twórczej osobowości itd.

Twórczość pedagogiczna jest zjawiskiem wielowymiarowym, odnoszącym się do różnych aspektów działalności naukowo-dydaktycznej nauczycieli.

Wg jednej z najbardziej rozpowszechnionych koncepcji pedagogicznych – R. Schulza[42] twórczość pedagogiczna może być traktowana jako: sztuka; wynalazczość i racjonalizatorstwo; dział badawczo-rozwojowy; zmiana, tzn. jako tworzenie lub przyswajanie innowacji; twórcza praca kreująca i urzeczywistniająca w teorii i praktyce nowości edukacyjnej; samorozwój.

Do kategorii zachowań twórczych, z pedagogicznego punktu widzenia R. Schulz zalicza:

- procesy samodzielnego projektowania i wprowadzania do praktyki przez indywidualnych nauczycieli określonych innowacji pedagogicznych;
- procesy zastosowania w praktyce wyników badań naukowych (badań zinstytucjonalizowanych);
- procesy pionierskiej asymilacji nowości pochodzących z zewnętrznych źródeł.

Kategorie te wyznaczają główne strategie działań twórczych, które można odnieść do czynnościowej (proces) lub rzeczowej (wytwór) wykładni innowacji.

Do prawidłowości zalicza się następujace zjawiska: pedagogiczne zdolności twórcze są w dużej mierze kształtowane: coś nowego powstaje z elementów już istniejących w rzeczywistości: elastyczność i giętkość umysłu: paradoksalny i antynomiczny charakter twórczości.

[42] R. Schulz, *Nowatorstwo pedagogiczne jako forma więzi nauki z praktyką, Nauki pedagogiczne a praktyka edukacyjna*, 1989.

Poniżej przedstawiono sposoby postępowania nauczyciela w czasie zajęć.

Tabela 9. Sposoby postępowania nauczyciela w czasie zajęć

Lp.	Postępowanie nauczyciela	Forma/Metoda
1.	Mówić do uczących się	Wykład informacyjny
2.	Rozmawiać z nimi	Seminarium konwersatorium
3.	Sprawiać, aby rozmawiali między sobą	Metoda pracy w małych grupach
4.	Pokazać, jak powinno się wykonywać jakąś czynność, a następnie polecić naśladowanie i kontrolować jej wykonanie	Ćwiczenie
5.	Ukierunkować i kontrolować pracę kształcących się	Metoda konsultacji
6.	Wdrażać praktycznie wiedzę podaną uprzednio innymi metodami	Zajęcia praktyczne

Źródło: opracowanie własne

Organizatorów doskonalenia obowiązuje zapewnienie wykładowców i instruktorów. Wykładowcą może być każdy, kto posiada odpowiednie przygotowanie merytoryczne i pedagogiczne. Instruktorem może być osoba z wyższym stopniem przygotowania od uczestników zajęć, wskazane byłoby też posiadanie minimum przygotowania pedagogicznego (wymóg ten spełniają aspiranci i podoficerowie kształceni według ostatnio obowiązujących programów).

104 FORMALNE PODSTAWY DZIAŁAŃ KSZTAŁCENIOWYCH

Liczne unijne i polskie dokumenty normatywne sankcjonują zadania i plany w zakresie tradycyjnych zagrożeń związanych z wyzwaniami i zagrożeniami cyberprzestrzeni.

Szczególnie ważne są

1. Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011–2016, (MSWiA, Warszawa 2010).

Dokument ten sankcjonuje nowe działania społeczno-edukacyjne i profilaktyczne do realizowania tylko przez szkoły w odniesieniu do nauczycieli i uczniów (szkoła)

i rodziców. Więcej na temat dokumentów regulacyjnych w załączniku: Wybrane formalno-prawne podstawy polityki społecznej.

2. Polityka bezpieczeństwa cyberprzestrzeni RP, MAiC, wrzesień 2012.

Precyzuje dokładnie zadania, obejmujące:
1. Szkolenia pełnomocników ds. ochrony cyberprzestrzeni.
2. Racjonalizację programów kształcenia studentów i doskonalenia kwalifikacji specjalistycznych.
3. Kształcenie kadry urzędniczej oraz ustanowienie dodatkowych kryteriów obsady stanowisk w administracji publicznej.

Działalność społeczna o charakterze głównie edukacyjno-profilaktycznym skierowana będzie do poszczególnych podmiotów odpowiedzialnych za kształtowanie postaw i wychowanie dzieci i młodzieży.

105 **Metodyczne przygotowanie zajęć**

Przygotowanie metodyczne ogólnie obejmuje wszystkie odpowiedzi na pytanie: jak prowadzić przygotowane zajęcia? Podstawowym zadaniem do rozwiązania metodycznego jest określenie rodzaju lekcji. Jest to trudne zadanie, ponieważ wkracza w zakres systemów kształcenia i teorii wielostronnego nauczania i uczenia się.

106 Czterech podstawowych rodzajów dydaktycznego postępowania i wielu możliwości rozwiązań mieszanych nie można stosować przypadkowo, wymagają bowiem one przemyślanego uzasadnienia.

107 Oprócz metod szczególnie skutecznych dla realizacji zadań przedmiotowo-metodycznych należy uwzględnić takie, których stosowanie wyrabia pożądane umiejętności i postawy uczniów. Metodyka każdego przedmiotu zawiera bogate propozycje metod nauczania i uczenia się zależnie od różnych działów programowych przedmiotu oraz poziomu nauczania.

Przegląd posiadanych środków, dobór tych, które najlepiej spełniają zadania wynikające z treści i celów przygotowywanych lekcji, to kolejne działania nauczyciela w przygotowaniu się do zajęć. Warto wstępnie ustalić, jakie funkcje wydają się szczególnie pożądane przy realizacji najbliższych tematów i za pomocą jakich środków można je najlepiej spełnić, jeżeli zostaną zastosowane w procesie nauczania i uczenia się.

Przygotowanie metodyczne lekcji powinno objąć także przewidywane w toku zajęć formy i metody kontroli pracy i osiągnięć uczniów. Z kontrolą łączy się stopniowe i systematyczne wdrażanie uczniów do samokontroli. Oba działania, aby były skuteczne dla prawidłowego przebiegu procesu kształcenia, powinny być wcześniej zaplanowane i przygotowane, z uwzględnieniem konkretnego materiału przewidzianego dla lekcji.

W toku przygotowania metodycznego należy zwrócić uwagę na motywację do uczenia się. Trzeba uczniów uczestników zajęć zachęcać do nauki nie tylko środkami werbalnymi, ale także atrakcyjnym ujęciem tematu, ciekawymi przykładami, aktywizującymi metodami pracy i wzbudzającymi zainteresowanie środkami dydaktycznymi. Do zakresu przygotowania organizacyjnego należy zarezerwowanie sobie odpowiedniego miejsca (pomieszczenia, pracowni, sali) dla odbycia zajęć.

Odpowiednie przygotowanie środków dydaktycznych i materiałów do wykorzystania w trakcie zajęć to także zakres powinności organizacyjnych, poprzedzających zajęcia i należących do fazy przygotowań. Nie wystarczy bowiem mieć środki i materiały w pracowni, trzeba ustalić, z jakich i w jakim czasie należy skorzystać, do których zagadnień szczególnie się nadają i jak zostaną wykorzystane w czasie zajęć dydaktycznych.

108 KONSTRUKCJA KONSPEKTU LEKCYJNEGO Z OBUDOWĄ

Zewnętrznym wyrazem przygotowania nauczyciela jest konspekt zajęć, zawierający plan, układ materiału do przekazania i opracowania z uczniami, planowane metody i środki dydaktyczne do wykorzystania w toku pracy. Konspekt spełnia rolę scenariusza dla tak złożonego wydarzenia pedagogicznego, jakim są zajęcia i podobnie jak w scenariuszu są w nim przewidziane poszczególne działania i sytuacje dydaktyczne, ich właściwości, odpowiednią kolejność, trafnie dobrane przykłady.

Konspekt, stanowiąc trwały zapis przygotowania zajęć, służy nie tylko do właściwego odbycia zajęć dydaktycznych, ale także może być wykorzystany w innej grupie lub w roku następnym, pod warunkiem jego uaktualnienia, z uwzględnieniem doświadczenia i wniosków wynikających z przeprowadzonych już zajęć.

Naczelnym zadaniem konspektu jest pomoc w zrealizowaniu tych celów, jakie zostały sformułowane dla tematu, dlatego też konspekt – aczkolwiek dotyczy konkretnych zajęć dydaktycznych lub ich cyklu dla obszerniejszego tematu czy zagadnienia – nie pozostaje w izolacji, a łączy się nie tylko z poprzednimi zajęciami, ale także z dotychczasowymi rezultatami pracy dydaktycznej i uzyskanymi postępami uczniów w poznawaniu i przyswajaniu treści programowych, rozwijaniu umiejętności poznawczych i zdolności oraz zamiłowań samokształceniowych.

Konspekt powinien stanowić szczegółowe opracowanie zadań projektowanych wcześniej w planie dydaktyczno-wychowawczym nauczyciela. Zainicjowane w tym planie wątki realizacji materiału programowego, a jednocześnie rozwoju instrumentalnych i kierunkowych cech osobowości ucznia, wdrażanie go do samokształcenia i rozwiania zainteresowań i zamiłowań poznawczych – znajdują się w konspektach kolejnych zajęć naturalną kontynuację w ujęciu rozwojowym. Jest to nie tylko podstawowe założenie konspektu, ale także punkt wyjścia do jego przygotowania.

109 Cz. Kupisiewicz uważa, iż „konspekt jest szczegółowym rozwinięciem planu lekcji, obejmuje on zwykle punkty, jak: temat lekcji, jej cele i zadania, porządek lekcji wraz z rozbiciem na poszczególne etapy, w konspekcie lekcji zamieszcza się rejestr tych metod i środków dydaktycznych, które mają być zastosowane w poszczególnych etapach jej realizacji”[43]. Ponadto w konspekcie warto jeszcze zamieścić dodatkowe elementy, takie jak: rodzaj (strategie podające, problemowe, ćwiczeniowe i eksponujące) i typ zajęć, które winny wynikać z założeń rocznego rozkładu materiału i określonych planów nauczania.

110 Niezależnie od powyższych uwag warto w konspekcie jeszcze uwzględnić:

1. część przygotowawczą z odpowiednimi zadaniami i konkretnym materiałem programowym;
2. część podstawową zgodną z rodzajem, typem i funkcją dydaktyczną;
3. część końcową obejmującą utrwalenie, zadanie pracy domowej i wskazanie możliwości kontynuowania tematu w sposób samodzielny w ramach aktywności poznawczej uczniów.

111 Ten trójdzielny układ może być stosowany zarówno w zajęciach pojedynczych, jak i w cyklu tworzącym jednostkę metodyczną. Celowym jest zaznaczenie czasu (liczba minut, od–do) przeznaczonego na realizację poszczególnych części zajęć.

[43] W. Okoń, *Wprowadzenie do dydaktyki*, op. cit., s. 386–399.

W kształceniu znajdują zastosowania także inne rozwiązania konspektów. Poniżej podano dwa przykłady ich struktury:

PRZYKŁAD PIERWSZY

1. TEMAT
2. CEL(E) ZAJĘĆ: A) DYDAKTYCZNY, B) KSZTAŁCĄCY, C) WYCHOWAWCZY
3. TYP LEKCJI
4. FORMA PRACY
5. METODA PRACY
6. TECHNOLOGIE I APLIKACJE MEDIALNE
7. CZAS TRWANIA ZAJĘĆ
8. WYKAZ LITERATURY

PLAN ZAJĘĆ

Zagadnienia szczegółowe	Uwagi	Czas w min
1. Część wstępna		
2. Część zasadnicza		
3. Synteza materiału		
4. Zakończenie lekcji		

PRZYKŁAD DRUGI

Punkty 1—8 jak w przykładzie pierwszym.

PLAN LEKCJI

L.p.	Zagadnienia	Czas w min	Czynności nauczyciela	Czynności ucznia
1.	Część organizacyjna			
2.	Cześć wstępna			
3.	Część zasadnicza			
4.	Synteza materiału			
5.	Zakończenie lekcji			

BIBLIOGRAFIA:

Aleksander T., *Andragogika. Podręcznik akademicki*, Instytut Technologii Eksploatacji – PIB, Radom-Kraków 2009.

Andrzejewska A., *Dziecko w cyberprzestrzeni,* Fundacja Pedagogium, Warszawa 2007.

Andrzejewska A., *Magia szklanego ekranu – zagrożenia płynące z telewizji*, Wyd. Fraszka Edukacyjna, Warszawa 2007.

Andrzejewska A., *(Nie)Bezpieczny komputer – od euforii do uzależnień*, APS, Warszawa 2008.

Andrzejewska A., *Gry komputerowe i sieciowe. Nasze dziecko w wielkiej sieci,* ASPRA -JR, Warszawa 2009.

Andrzejewska A., *Patologie moralne w sieci,* ASPRA- JR, Warszawa 2009.

Andrzejewska A., Bednarek J. (red.), *Cyberświat – możliwości i zagrożenia,* Wyd. Akademickie „Żak", Warszawa 2009.

Aouil B., Maliszewski W. J., *Media – komunikacja: zdrowie i psychologia.* Wyd. Adam Marszałek, Toruń 2007.

Aouil B., *Internet jako środowisko komunikacyjne*, w: M. Tanaś (red.), *Kultura i język mediów*, Oficyna Wydawnicza „Impuls", Kraków 2007.

Aouil B., Maliszewski W. J., *Media – komunikacja – zdrowie. Wyzwania – szanse – zagrożenia,* Wyd. Adam Marszałek, Toruń 2008.

Barczak A., Florek J., Jakubowski S., Sydoruk T., *Zdalna edukacja. Potrzeby, problemy, szanse i zagrożenia,* Inst. Audytu i Ewaluacji Sp. z o.o., Akademia Pedagogiki Specjalnej, Warszawa 2006.

Bąkiewicz M., Grewiński M. (red.), *Praca socjalna w środowisku lokalnym,* WSP TWP, Warszawa 2009.

Bednarczyk H. (red.) *Podstawy teoretyczne i modele systemów zarządzania w ustawicznej edukacji zawodowej*, Instytut Technologii Eksploatacji – Państwowy Instytut Badawczy, Radom 2005.

Bednarczyk H., Łopacińska L., Charraud A.M. (red.), *Kształcenie zawodowe w kontekście Europejskich Ram Kwalifikacji*, Instytut Technologii Eksploatacji – Państwowy Instytut Badawczy, Radom 2008.

Bednarek J., *Multimedialne kształcenie nauczycieli,* WSP TWP, Warszawa 2010.

Bednarek J., *Podstawy kształcenia multimedialnego,* w: Tanaś M., *Technologia informacyjna w procesie dydaktycznym,* MIKOM, Warszawa 2005.

Bednarek J., *Społeczeństwo informacyjne i media w opinii osób niepełnosprawnych,* APS, Warszawa 2005.

Bednarek J., *Multimedia w kształceniu*, Wyd. Naukowe PWN, Warszawa 2012.

Bednarek J., Lubina E. (red.), *Kształcenie na odległość. Podstawy dydaktyki,* Wyd. Naukowe PWN, Warszawa 2008.

Dylak S., *Wizualizacja w kształceniu nauczycieli*, UAM, Poznań 1995.

Dylak S., *Edukacja medialna w szkole,* w: Strykowski W. (red.), *Media a edukacja*, Poznań 1997.

Dylak S., Moorman G., Trathen W., *Dialog w kształceniu na odległość – jego znaczenie i struktura*, w: Wrycza S., Wojtkowiak J. (red.), *Nauczanie na odległość, wyzwania – tendencje – aplikacje*, Uniwersytet Gdański, Gdańsk 2002.

Ejsmont M., Kosmalska B., *Media. Wartości. Wychowanie*, Oficyna Wydawnicza. „Impuls", Kraków 2008.

Furmanek W., Piecuch A. (red.), *Dydaktyka informatyki. Multimedia w teorii i praktyce szkolnej,* Uniwersytet Rzeszowski, Rzeszów 2008.

Gajda J., *Kulturotwórcze i edukacyjne funkcje mass mediów*, w: Strykowski W., Skrzydlewski W. (red.), *Media a Edukacja*, Wyd. eMPi², Poznań 2000.

Gajda J., Juszczyk S., Siemieniecki B., Wenta K. (red.), *Edukacja medialna,* Wyd. Adam Marszałek, Toruń 2005.

Gajda J., *Media w edukacji,* Oficyna Wydawnicza „Impuls", Kraków-Warszawa, 2003, 2005.

Gajda J., *Hipermedia szansą wzbogacenia tradycyjnych form multimedialnego kształcenia otwartego na odległość,* „Pedagogika Mediów" 2006, 1-2.

Gajda J., *Pedagogika kultury w zarysie*, Wyższa Szkoła Pedagogiczna ZNP, Oficyna Wydawnicza „Impuls", Warszawa-Kraków 2006.

Gajda J., *Antropologia kulturowa,* cz.2., *Kultura obyczajowa początku XXI wieku*, Oficyna Wydawnicza „Impuls", Kraków 2008.

Galloway Ch., *Psychologia uczenia się i nauczania,* PWN, Warszawa 1988.

Galwas B., *Techniki teleinformatyczne w edukacji*, w: Galwas B., Błeszczyński J., Kudowski R., *Internet i techniki multimedialne w edukacji*, Instytut Problemów Współczesnej Cywilizacji, Warszawa 2004.

Gaś Z.B., *Doskonalący się nauczyciel*, UMCS, Lublin 2001.

Gaś Z.B., *Nauczyciel jako osoba wspomagająca ucznia w rozwoju*, w: Gaś Z. B. (red.), *Szkoła i nauczyciel w percepcji uczniów*, IBE, Warszawa 1999.

Goban-Klas T., *Komunikowanie i media*, w: Bauer Z., Chudzikowski E. (red.), *Dziennikarstwo i świat mediów*, UNIVERSITAS, Kraków 2000.

Goban-Klas T., *Media i komunikowanie masowe. Teorie i analizy prasy, radia telewizji i Internetu*, Wyd. Naukowe PWN, Warszawa -Kraków 2001.

Goban-Klas T., *Powstanie i rozwój mediów. Od malowideł naskalnych do multimediów*, Akademia Pedagogiczna, Kraków 2001.

Goban-Klas T., Sienkiewicz P., Soliński A., *Implikacje społeczne i kulturalne rozwoju telekomunikacji*, KBN, Warszawa 1995.

Gogołek W., *Paradoks Sieci*, w: J. Morbitzer (red.), *Komputer w edukacji*, Akademia Pedagogiczna, Kraków 2008.

Gogołek W., *Internet w zdalnej edukacji,* w: Mitas A. W. (red.), *Technologie informacyjne w edukacji policjantów,* Centrum Szkolenia Policji w Legionowie, Legionowo 2008.

Grewiński M., Karwacki A. (red.), *Strategie w polityce społecznej,* Mazowieckie Centrum Polityki Społecznej, Warszawa 2009.

Grewiński M., *Wielosektorowa polityka społeczna,* WSP TWP, Warszawa 2009.

Grzenia J., *Komunikacja językowa w Internecie,* Wyd. Naukowe PWN, Warszawa 2006.

Grzeszczyk E., *Edukacja informatyczna nauczycieli u progu e-edukacji*, WSP TWP, Warszawa 2007.

Grzywak A., *Bezpieczeństwo systemów komputerowych*, Pracownia Komputerowa Jacka Skalmierskiego, Warszawa 2001.

Izdebska J. (red.), *Media elektroniczne – kreujące obraz rodziny i dziecka,* Wyd. Trans Humana, Białystok 2008.

Jagodzińska M., *Obraz w procesach poznania i uczenia się*, WSiP, Warszawa 1991.

Juszczyk S., *Człowiek w świecie elektronicznych mediów – szanse i zagrożenia (o problemach tworzącego się społeczeństwa informacyjnego)*, Uniwersytet Śląski, Katowice 2000.

Juszczyk S., *Edukacja medialna w społeczeństwie informacyjnym*, Wyd. Adam Marszałek, Toruń 2002.

Juszczyk S., *Edukacja na odległość, Kodyfikacja pojęć, reguł i procesów*, Wyd. Adam Marszałek, Toruń 2002.

Juszczyk S., *Dydaktyka informatyki i technologii informacyjnej jako element przestrzeni edukacyjnej*, w: Furmanek W., Piecuch A. (red.), *Dydaktyka informatyki. Problemy teorii*, Uniwersytet Rzeszowski, Rzeszów 2004.

Juszczyk S., *Cele i zadania technologii informacyjnej i edukacji medialnej*, w: *Pedagogika medialna*, t. 2, Siemieniecki B. (red.), Wyd. Naukowe PWN, Warszawa 2007.

Juszczyk S., *Edukacja na odległość*, Wyd. Adam Marszałek, Toruń 2008.

Karpińska A., Wróblewska W. (red.), *Pola poznawcze dydaktyki w dialogu i perspektywie,* Wyd. Trans Humana, Białystok 2008.

Kędzierska B., *Rola nauczycieli w przygotowaniu dzieci i młodzieży do uczestnictwa w społeczeństwie informacyjnym. Kształcenie w wyższych uczelniach pedagogicznych,* w: Migdałek J., Kędzierska B. (red.), *Informatyczne przygotowanie nauczycieli,* Wyd. Rabid, Kraków 2002.

Kędzierska B., *Informatyczne kształcenie i doskonalenie nauczycieli,* Akademia Pedagogiczna, Kraków 2005.

Kędzierska B., *Kompetencje informacyjne w kształceniu ustawicznym,* Instytut Badań Edukacyjnych, Warszawa 2007.

Konarzewski K. (red.), *Sztuka nauczania. Szkoła,* t. 2, PWN, Warszawa 1991.

Kotusiewicz A.A., Koć-Seniuch G. (red.), *Nauczyciel akademicki w refleksji nad własną praktyką edukacyjną*, WSP ZNP, Wyd. Akademickie „Żak", Warszawa 2008.

Kramek Z. (red.), *Teoretyczno-metodyczne podstawy rozwoju e-learningu w edukacji ustawicznej,* Instytut Technologii Eksploatacji – PIB, Radom 2007.

Kruszewski K., *Zmiana a wiadomość, perspektywa dydaktyki ogólnej,* PWN, Warszawa 1987.

Kruszewski K., *Najpotrzebniejsze zasady dydaktyczne,* w: Kruszewski K. (red.), *Sztuka nauczania. Czynności nauczyciela,* Warszawa 2001.

Kruszewski K., *Sztuka nauczania. Szkoła*, Wyd. Naukowe PWN, Warszawa 2002.

Kruszewski K., *Człowiek na biegunach,* BEL Studio, Warszawa 2004.

Kruszewski K., *Sztuka nauczania. Czynności nauczyciela*, Wyd. Naukowe PWN, Warszawa 2004.

Kruszewski K., *Słowiki i wróble*, w: Tanaś M. (red.), *Pedagogika @ środki informacyjne i media*, Oficyna Wydawnicza „Impuls", Warszawa-Kraków 2004.

Kruszewski K. (red.), *Sztuka nauczania,* t. 1, *Czynności nauczyciela. Podręcznik akademicki*, Wyd. Naukowe PWN, Warszawa 2007.

Kupisiewicz Cz., *Dydaktyka ogólna*, Oficyna wydawnicza GrafPunkt, Warszawa 2000.

Kupisiewicz Cz., *Podstawy dydaktyki ogólnej*, Wyd. Nauk. PWN, Warszawa 2010.

Kupisiewicz Cz., Wybrane problemy teorii i praktyki pedagogicznej na progu XXI w., IBE, Ryki 2003.

Półturzycki J., *Akademicka edukacja dorosłych*, Wyd. Uniwersytetu Warszawskiego, Warszawa 1994.

Kupisiewicz Cz., *Paradygmaty i wizje reform oświatowych*, PWN, Warszawa 1985.

Kupisiewicz Cz., *Szkolnictwo w procesie przebudowy. Geneza i kierunki reform oświatowych 1945-1995,* PWN, Warszawa 1995.

Kupisiewicz Cz., *Dydaktyka ogólna*, Oficyna Wydawnicza GrafPunkt, Warszawa 2000.

Kupisiewicz Cz., *Wybrane problemy teorii i praktyki pedagogicznej na progu XXI w.*, WSUPiZ, Warszawa 2003.

Kupisiewicz Cz., *Efekty reform edukacyjnych w Polsce. Główne tezy i wpływ na funkcjonowanie szkolnictwa,* Wyd. Naukowe PWN, Warszawa 2006.

Kupisiewicz Cz., Kupisiewicz M., *Złote myśli o wychowaniu i kształceniu,* Wyższa Szkoła Umiejętności Pedagogicznych i Zarządzania, Warszawa-Ryki 2005.

Kupisiewicz Cz., Kupisiewicz M., *Poczet wybitnych nauczycieli.* Część druga, Akademia Humanistyczna im. Aleksandra Gieysztora, Pułtusk 2007.

Kupisiewicz Cz. (red.), współpraca Kupisiewicz M., Nowakowska-Siuta R., *Drogi i bezdroża polskiej oświaty w latach 1945—2005. Próba wybiórczo-retrospektywnego spojrzenia,* Komitet Prognoz „Polska 2000 Plus" przy Prezydium PAN, Warszawa 2005.

Kwiatkowska H., *Źródła inspiracji nowego myślenia o edukacji nauczycielskiej,* w: Kwiatkowska H., Lewowicki T. (red.), *Źródła inspiracji współczesnej edukacji nauczycielskiej,* Wyższa Szkoła Pedagogiczna ZNP, Warszawa 1997.

Kwiatkowska H., *Współczesne orientacje w kształceniu nauczycieli*. PWN, Warszawa 1988.

Kwiatkowska H., *Tożsamość nauczycieli. Między anomią a autonomią*, GWP, Gdańsk 2005.

Kwiatkowska H., Kwieciński Z. (red.), *Demokracja a oświata, Kształcenie i wychowanie. Materiały z II Ogólnopolskiego Zjazdu Pedagogicznego,* Wyd. Edytor, Toruń 1996.

Kwiatkowska H. i in., (red.), *Współczesność a kształcenie nauczycieli*, WSP ZNP, Warszawa 2000.

Kwiatkowska H., Lewowicki T. (red.), *Społeczno-kulturowe konteksty edukacji nauczycieli i pedagogów,* WSP ZNP, Warszawa 2003.

Kwiatkowski S.M., *Media a przebieg procesów poznawczych w kształceniu zawodowym*, w: Strykowski W. (red.), *Media a edukacja*, Wyd. eMPi², Poznań 1997.

Kwiatkowski S. M., *Kształcenie zawodowe, Dylematy teorii i praktyki*, IBE, Warszawa 2001.

Kwiatkowski S. M., *Komputer w zarządzaniu informacją oraz w szkolnictwie zawodowym*, w: Siemieniecki B. (red.), *Pedagogika medialna*, t. II, Wyd. Naukowe PWN, Warszawa 2007.

Kwiatkowski S. M., *Edukacja ustawiczna. Wymiar praktyczny i teoretyczny,* Wyd. IBE, Instytut Technologii Eksploatacji – PIB, Warszawa-Radom 2008.

Kwiatkowski S. M., *Kształcenie zawodowe w systemie szkolnym*, (w:) Lewowicki T. (red.), *Gorące problemy edukacji w Polsce, Ekspertyzy i opinie,* Komitet Nauk Pedagogicznych PAN, WSP ZNP, Warszawa 2007.

Kwiatkowski S. M. (red.), *Kształcenia zawodowe – rynek pracy – pracodawcy*. IBE, Warszawa 2000.

Kwiatkowski S. M. (red.), *Innowacje,* Uniwersytet Warszawski, Warszawa 2004.

Kwiatkowski S. M., Sharif N. M. (red.), *Intellectual Entrepreneurship and Courage to Act,* Publishing House of Leon Kozminsky Academy of Entrepreneurship and Management, Warsaw 2005.

Kwiatkowski S. M., Kamiński M.B. (red.), *Knowledge Café for Intellectual Entrepreneurship: Wiedza, przedsiębiorczość, bogactwo*, Wyższa Szkoła Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego, Warszawa 2006.

Kwiatkowski S. M. (red.), *Dobra gospodarka,* Wyższa Szkoła Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego, Warszawa 2006.

Kwiatkowski S. M., Bogaj A., Baraniak B., (red.), *Pedagogika pracy,* Wyd. Akademickie i Profesjonalne, Warszawa 2007.

Kwiek J., *Media a problem uzależnień,* w: Andrzejewska A., Bednarek J. (red.) *Cyberświat. Możliwości i ograniczenia*, Wyd. Akademickie „Żak", Warszawa 2009.

Laska E.I., *Samokształcenie dorosłych czynnością podmiotową*, w: Fabiś A. (red.), *Wyzwania współczesnej edukacji dorosłych*, t. 1, Górnośląska Wyższa Szkoła Pedagogiczna, Mysłowice-Zakopane 2004.

Lewowicki T., *Problemy kształcenia i pracy nauczycieli*, Instytut Technologii Eksploatacji – PIB, Warszawa–Radom 2007.

Lewowicki T., Grabowska B. (red.), *Społeczności pogranicza: wielokulturowość, edukacja*, Uniwersytet Śląski. Filia WSP ZNP, Cieszyn-Warszawa 1996.

Lewowicki T. i in. (red.), *Edukacja wobec ładu globalnego*, Wyd. Akademickie „Żak", Warszawa 2002.

Lewowicki T., Siemieniecki B. (red.), *Rola i miejsce technologii informacyjnej w okresie reform edukacyjnych Polsce,* Wyd. Adam Marszałek, Toruń 2002.

Lewowicki T., Ogrodzka-Mazur E., Szczurek -Boruta A. (red.), *Praca nauczyciela w warunkach wielokulturowości: studia i doświadczenia z pogranicza polsko-czeskiego*, Wyd. Adam Marszałek, Toruń 2008.

Lewowicki T., Siemieniecki B. (red.), *Współczesna technologia informacyjna i edukacja medialna*, Wyd. Adam Marszałek, Toruń 2005.

Lewowicki T., Szczurek-Boruta A., Grabowska B. (red.), *Przemiany społeczno-cywilizacyjne i edukacja szkolna: problemy rozwoju indywidualnego i kształtowania się tożsamości,* Oficyna Wydawnicza „Impuls", Kraków 2005.

Lewowicki T., Szczurek-Boruta A., Grodzka-Mazur E. (red.), *Teorie i modele badań międzykulturowych*, Uniwersytet Śląski, Filia WSP ZNP, Cieszyn–Warszawa 2006.

Lewowicki T., Urban J. (red.), *Edukacja międzykulturowa na pograniczach w pierwszych latach rozszerzonej Unii Europejskiej – teoria i praktyka*, „Gnome", Katowice 2007.

Lewowicki T., Siemieniecki B. (red.), *Współczesna technologia informacyjna i edukacja medialna*, Wyd. Adam Marszałek, Toruń 2008.

Lewowicki T., Siemieniecki B. (red.), *Media w edukacji. Szanse i zagrożenia*, Wyd. Adam Marszałek, Toruń 2008.

Lewowicki T., Siemieniecki B. (red.), *Media w procesie informacyjno-komunikacyjnym*, Wyd. Adam Marszałek, Toruń 2008.

Lewowicki T., Siemieniecki B. (red.), *Kształcenie na odległość w praktyce edukacyjnej,* Wyd. Adam Marszałek, Toruń 2009.

Lewowicki T., Szlosek F. (red.), *Kształcenie ustawiczne do wielokulturowości,* Instytut Technologii Eksploatacji – PIB, Radom 2009.

Łaszczyk J., *Elektroniczne media jako środek stymulowania rozwoju intelektualnego*, w: Tanaś M. (red.), *Kultura i język mediów,* Oficyna Wydawnicza „Impuls", Kraków 2007.

Łaszczyk J., *Psychologiczne i społeczne zagrożenia związane z zastosowaniem mediów i technologii informacyjnej w edukacji*, w: Tanaś M. (red.), *Pedagogika @ środki informatyczne i media*, WSP ZNP, Oficyna Wydawnicza „Impuls", Kraków 2007.

Łaszczyk J. (red.), *Komputer w kształceniu specjalnym: wybrane zagadnienia,* WSiP, Warszawa 1998.

Łaszczyk J. (red.), *Pedagogika czasu przemian*, ZM WSPS, Warszawa 1999.

Łaszczyk J., Jabłonowska M. (red.), *Uczeń zdolny wyzwaniem dla współczesnej edukacji*, APS, Warszawa 2008.

Nalaskowski S., *Metody nauczania*, Wyd. Adam Marszałek, Toruń 1997.

Niemierko B., *Pomiar wyników kształcenia*. WSiP, Warszawa 1999.

Niemierko B., *Między oceną szkolną a dydaktyką*, WSiP, Warszawa 2001.

Okoń W., *Wprowadzenie do dydaktyki ogólnej*, Wyd. Akademickie „Żak", Warszawa 2003.

Półturzycki J., *Dydaktyka dorosłych*, WSiP, Warszawa 1991.

Półturzycki J., *Akademicka edukacja dorosłych.* Uniwersytet Warszawski, Warszawa 1994.

Półturzycki J., *Dydaktyka dla nauczycieli*. Wyd. Adam Marszałek, Toruń 1999.

Rozmysłowicz P., *Kompetencje medialne nauczyciela*, w: Żegnałek K. (red.), *Kompetencje współczesnego nauczyciela*, WSP TWP, Warszawa 2008.

Siemieniecka D., *Technologia informacyjna a twórczość*, w: Siemieniecki B. (red.), *Pedagogika medialna*,, t. II, Wyd. Naukowe PWN, Warszawa 2007.

Siemieniecka D. (red.), *Współczesne konteksty edukacyjne technologii informacyjnej,* Wyd. Adam Marszałek, Toruń 2009.

Siemieniecki B., *Komputer w diagnostyce i terapii pedagogicznej,* Wyd. Adam Marszałek, Toruń 1966.

Siemieniecki B., *Komputery i hipermedia w procesie edukacji dorosłych*, Wyd. Adam Marszałek, Toruń 2001.

Siemieniecki B., Lewandowski W., *Internet w szkole*, Wyd. Adam Marszałek, Toruń 2001.

Siemieniecki B., *Technologia informacyjna w polskiej szkole. Stan i zadania,* Multimedialna Biblioteka Pedagogiczna, Wyd.

Adam Marszałek, Toruń 2003.

Siemieniecki B., *Rola i miejsce technologii informacyjnej w okresie reform edukacyjnych w Polsce. Kognitywistyka edukacyjna marzenia czy rzeczywistość?,* w: Lewowicki T., Siemieniecki B. (red.), *Rola i miejsce technologii informacyjnej w okresie reform edukacji w Polsce,* Wyd. Adam Marszałek, Toruń 2003.

Siemieniecki B., *Badania nad możliwościami i ograniczeniami e-learningu w edukacji,* w: Siemieniecki B. (red.), *Kształcenie na odległość w świetle badań i analiz,* Wyd. Adam Marszałek, Toruń 2005.

Siemieniecki B., *Media a patologie*, (w:) Siemieniecki B. (red.), *Pedagogika medialna*, t. 1, Wyd. Naukowe PWN, Warszawa 2007.

Siemieniecki B., *Taksonomie zastosowań technologii informacyjnej w edukacji*, w: B. Siemieniecki (red.), *Pedagogika medialna*, Wyd. Naukowe PWN, Warszawa 2007.

Siemieniecki B. (red.), *Pedagogika medialna*, t. 1-2, Wyd. Naukowe PWN, Warszawa 2007.

Singer P., *Jeden Świat. Etyka globalizacji,* KiW, Warszawa 2006.

Skrzydlewski W., *Technologia kształcenia. Przetwarzanie informacji. Komunikowanie.* UAM, Poznań 1990.

Skrzypczak J., *Film dydaktyczny w szkole wyższej*. PWN, Warszawa 1985.

Skrzypczak J., *Popularna encyklopedia mass mediów,* UAM, Poznań 1999.

Smirnowa H., *Kompetencje emocjonalne dzieci*, „Edukacja i Dialog" 8/2000.

Sobczak J., *Dylematy społeczeństwa informacyjnego*, w: Sokołowski M. (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI wieku*, PWSZ, Elbląg 2006.

Sobkowiak B., *Komunikowanie społeczne*, w: B. Dobek-Ostrowska (red.), *Komunikowanie i jego podział*, Uniwersytet Wrocławski, Wrocław 2007.

Sokołowski M., *Teoria i praktyka edukacji medialnej: modele, konteksty, interpretacje*, „Kastalia", Olsztyn 2002.

Sokołowski M. (red.), *Oblicza Internetu. Internet w przestrzeni komunikacyjnej XXI wieku*, PWSZ, Elbląg 2006.

Sokołowski M. (red.), *Internet w przestrzeni komunikacyjnej XXI wieku,* PWSZ, Elbląg 2006.

Sokołowski M. (red.), *(Kon)teksty kultury medialnej: analizy i interpretacje,* t. 1, Uniwersytet Warmińsko-Mazurski, Olsztyn 2007.

Sokołowski M. (red.), *Kulturowe kody mediów. Stan obecny i perspektywy rozwoju,* Wyd. Adam Marszałek, Toruń 2008.

Sokołowski M. (red.), *Media i społeczeństwo*, Wyd. Adam Marszałek, Toruń 2008.

Sokołowski M. (red.), *Oblicza Internetu. Opus Universale. Kulturowe, edukacyjne i technologiczne przestrzenie Internetu,* Państwowa Wyższa Szkoła Zawodowa, Elbląg 2008.

Solarczyk-Ambrozik E., *Kształcenie ustawiczne w perspektywie globalnej i lokalnej. Między wymogami rynku a indywidualnymi strategiami edukacyjnymi,* Uniwersytet im. Adama Mickiewicza, Poznań 2004.

Sonczyk W., *Media w Polsce. Zarys problematyki,* WSiP, Warszawa 1999.

Sordylowa B., *Informacja naukowa w Polsce. Problemy teoretyczne, źródła, organizacja*, Ossolineum, Wrocław 1987.

Sorlin P., *Media w Polsce: zarys problematyki*, Wyd. Astrum, Wrocław 2001.

Sozański J., *Prawo Wspólnot i Unii Europejskiej*, WSHiP, Warszawa 2004.

Sozański J., *Europejskie standardy ochrony praw człowieka*, PWSBiA, Warszawa 2004.

Sozański J., *Prawa człowieka w systemach prawnych Wspólnot i Unii Europejskiej*, Wyd. Iris, Warszawa-Poznań 2008.

Społeczeństwo informacyjne w liczbach 2009, MSWiA, Warszawa 2009.

Społeczeństwo informacyjne. Wykorzystanie technologii informacyjno-telekomunikacyjnej w 2006 r., Warszawa 2006.

Steinbrink B., *Multimedia u progu technologii XXI wieku*, Markt & Technik, Warszawa 1993.

Stępień R., *O potrzebie kształcenia nauczycieli,* „Edukacja dla Bezpieczeństwa", 5/2005.

Stochmiałek J. (red.), *Problemy współczesnej edukacji w niemieckich i polskich opracowaniach*, Instytut Technologii Eksploatacji, Warszawa-Radom 1995.

Stokłosa J., Biliński T., Pankowski T., *Bezpieczeństwo danych w systemie informatycznym*, Wyd. Naukowe PWN, Warszawa 2001.

Straszak A., *Sieciowa infrastruktura edukacyjna społeczeństwa informacyjnego*, w: Lewowicki T., Siemieniecki B., *Rola i miejsce technologii informacyjnej w okresie reform edukacji w Polsce*, Wyd. Adam Marszałek, Toruń 2003.

Strategia e-Polska – Plan działań na rzecz rozwoju elektronicznej administracji (eGovernment) na lata 2005—2006. Ministerstwo Nauki i Informatyzacji, Warszawa 2004.

Strategia państwa polskiego w dziedzinie mediów elektronicznych na lata 2005—2020, KRRiT, 26 sierpnia 2005.

Strategie reform oświatowych w Polsce na tle porównawczym: zbiór studiów, ELIPSA, Warszawa 1999.

Strebe M., *Firewall, Ściany ogniowe*, MIKOM, Warszawa 2000.

Strykowski W., *Audiowizualne materiały dydaktyczne. Podstawy kształcenia multimedialnego*, PWN, Warszawa 1984.

Strykowski W., *Media i edukacja medialna w tworzeniu współczesnego społeczeństwa,* w: Strykowski W., Skrzydlewski W. (red.) *Media i edukacja w dobie integracji*, Wyd. eMPi², Poznań 2002.

Strykowski W., *Kompetencje medialne: pojęcia, obszary, formy kształcenia,* w: Strykowski W., Skrzydlewski W.(red.), *Kompetencje medialne społeczeństwa wiedzy,* Wyd. eMPi², Poznań 2004.

Strykowski W., Skrzydlewski W. (red.), *Dokąd zmierza technologia kształcenia.* UAM, Poznań 1993.

Strykowski W. (red.), *Media a edukacja. Międzynarodowe Konferencje*. Wyd. eMPi², Poznań 2006.

Strykowski W. (red.), *Scenariusze zajęć edukacji czytelniczo-medialnej,* UAM, Poznań 2002.

Strykowski W., Zając A. (red.), *Nowoczesna technika w kulturze i oświacie. Komputery – – audio-wideo – TVSAT – multimedia – infrostrady.* UAM w Poznaniu, WSP w Rzeszowie, Tarnów 1996.

Suchodolski B., *Wychowanie mimo wszystko*, WSiP, Warszawa 1990.

Suchodolski B. (red.), *Model wykształconego Polaka*, Ossolineum, Wrocław 1980.

Suchodolski B., *Przedmowa*, w: Peccei A., *Przyszłość jest w naszych rękach*, PWN, Warszawa 1987.

Sullivan-Traino M., *Infostrada*, READ ME, Warszawa 1995.

Surina I., *Konstruowanie społeczności wirtualnych w systemie internetowej komunikacji. Możliwości i zagrożenia,* w: Nowak J. (red.), *Meandry wykluczenia społecznego*, WSP TWP, Warszawa 2008.

Symonides J. (red.), *Human Rights: International Protection, Monitoring, Enforcement*, Aldersot-Burligton USA-Singapore-Sydney 2003.

Szlosek F. (red.), *Edukacja nauczycielska,* Instytut Technologii Eksploatacji, Radom 1998.

Szlosek F. (red.), *Kształcenie nauczycieli a reforma systemu edukacji w Polsce*, Instytut Technologii Eksploatacji, Radom 2000.

Szlosek F., Czarnecki K.M., (red.), *Badanie – dojrzewanie – rozwój (na drodze do doktoratu),* Instytut Technologii Eksploatacji, Radom-Piotrków Trybunalski 2002.

Tanaś M., *Edukacyjne zastosowania komputerów,* Wyd. Akademickie „Żak", Warszawa 1997.

Tanaś M., *Edukacyjne konsekwencje rozwoju środków informatycznych*, w: Kwiatkowska H., Szybisz M. (red.), *Edukacja i dialog w świecie przyszłości*, Wyższa Szkoła Humanistyczna, Pułtusk 2003.

Tanaś M. (red.), *Pedagogika @ środki informacyjne i media*, Oficyna Wydawnicza „Impuls", Warszawa–Kraków 2004.

Tanaś M., (red.) *Technologia informacyjna w procesie dydaktycznym*, MIKOM, Warszawa 2005.

Tanaś M., *Wychowanie a media*, w: Siemieniecki B. (red.), *Pedagogika mediów*, Wyd. Adam Marszałek, Toruń 2006.

Tanaś M. (red.), *Kultura i język mediów*, Oficyna Wydawnicza „Impuls", Kraków 2007.

Wenta K., *Samokształcenie w społeczeństwie ponowoczesnym,* w: Pająk K., Zduniak A. (red.), ELIPSA, Warszawa-Poznań 2003.

Wenta K., *Ewaluacja i innowacja w edukacji obywatelskiej,* w: Grzesiak J. (red.), *Ewaluacja i innowacje edukacji,* PWSZ, Konin 2007.

Wenta K., *Manipulacja we wzorze osobowym,* (w:) Siemieniecki B. (red.), *Manipulacja – media – edukacja*, Wyd. Adam Marszałek, Toruń 2007.

Wieczorkowski K., *Zasady dydaktyki ogólnej, w kształceniu na odległość*, w: Lewowicki T., Siemieniecki B. (red.), *Rola i miejsce technologii informacyjnej w okresie reform edukacyjnych w Polsce*, Wyd. Adam Marszałek, Toruń 2002.

Zaczyński W.P., *Uczenie się przez przeżywanie. Rzecz o teorii wielostronnego kształcenia,* WSiP, Warszawa 1990.

Żegnałek K. (red.), *Kompetencje współczesnego nauczyciela*, WSP TWP, Warszawa 2008.

Żygulski K., *Globalne problemy współczesnego świata*, Fundacja Innowacja, Warszawa 1999.

METODY KSZTAŁCENIA PRACOWNIKÓW SŁUŻB SPOŁECZNYCH

ZAGROŻENIA CYBERPRZESTRZENI:
PRZEWODNIK DLA RODZICÓW

Velta Lubkina
Gilberto Marzano

„To złoty wiek organizowania się. Jedno Internet zmienił na zawsze, mianowicie względny koszt zebrania grupy ludzi w jednym miejscu, aby pracowali nad wspólnym celem. Może to zjawisko nie zawsze dobre (ułatwia to życie wszelkiej maści zbirom, rasistom i świrom), ale zmieniło ono fundamentalnie przebieg gry". (Cory Doctorow, For the Win, 2010)

1 WPROWADZENIE

Celem niniejszego artykułu jest wyznaczenie dobrych praktyk, które powinni stosować rodzice w celu ochrony swoich dzieci przed zagrożeniami cyberprzestrzeni.

2 Podkreśla się, że przynajmniej początkowo rodzice postrzegają Internet jako przydatne narzędzie w odrabianiu lekcji przez ich dzieci[1]. W oczach rodzica telefony komórkowe jawią się jako urządzenia pomagające zapewnić bezpieczeństwo ich pociech, które mogą zadzwonić do domu w nagłym przypadku. Natomiast zarówno dzieci, jak i młodzież, postrzegają Internet, telefony komórkowe oraz powiązane z nimi technologie jako niezbędne elementy ich życia społecznego. Wielu rodziców napotyka trudności związane z użytkowaniem nowych technologii i nie rozumie związanego z nimi ryzyka. Natomiast dla dzieci i młodzieży nowe technologie istnieją od zawsze, zatem ich użytkowanie jest dla nich czymś naturalnym, w przeciwieństwie do wielu rodziców, którzy szczerze przyznają, że to właśnie od dzieci czerpią całą wiedzę na temat Internetu i związanych z nim technologii.

3 Obecnie rodzice powinni opanować do perfekcji nowe technologie oraz sprawować kontrolę nad nimi, jeśli chcą, żeby ich dzieci mogły bezpiecznie serfować w sieci.

[1] Por. Kowalsky R. M., Limber S. P., Agatstone P. W., *Cyberbullyiung: Bulletyn in the Digital Age*, Willey -Blackwell, 2012.

4 PODSTAWY BEZPIECZEŃSTWA W SIECi

Dostawcy oprogramowania komputerowego, jak Microsoft i Google, dają swoim użytkownikom szereg porad na temat bezpieczeństwa.

5 Strona Internetowa Google zaleca:

Istnieje mnóstwo fascynujących rzeczy, jakie można robić online, ale Internet może być momentami również przerażający. Podobnie jak w realnym świecie należy dbać o bezpieczeństwo. Bez względu na to, czy jesteś nowym użytkownikiem czy starym wyjadaczem, dobrze być na bieżąco z najlepszymi praktykami dotyczącymi dzielenia się danymi i przeglądania stron. Znajdziesz tutaj rady, jak być bardziej bezpiecznym w sieci oraz przegląd narzędzi Google służących ochronie bezpieczeństwa.

6 Google oferuje porady na temat:

- haseł,
- oszustw,
- ochrony urządzeń,
- korzystania z zabezpieczonych sieci,
- unikania wyłudzenia informacji,
- sprawdzania ustawień Gmaila,
- bezpieczeństwa podczas zakupów,
- blokowania ekranu,
- narzędzi Google służących ochronie bezpieczeństwa.

7 Natomiast Microsoft oferuje wiele darmowych aplikacji ochrony rodzicielskiej pozwalających kontrolować używanie komputera przez dziecko: odwiedzane strony internetowe, używane programy, czas spędzony przed komputerem. Są to w szczególności:

- **blokowanie stron** – możesz blokować strony odwiedzane przez dzieci, a tym samym być pewnym, że odwiedzają jedynie strony stosowne do ich wieku,

blokować pobieranie plików oraz decydować o tym, jakiego rodzaju treści filtry będą blokować. Możesz również blokować lub zezwalać na korzystanie z poszczególnych stron. Więcej informacji w sekcji Ograniczaj treści oglądane przez dzieci w sieci;

- **ograniczanie czasu** – możesz ograniczyć czas, na jaki dzieci mogą się logować do komputera. Ograniczenia czasowe mogą dotyczyć określonych godzin, a jeśli już wcześniej się zalogowały, zostaną wówczas automatycznie wylogowane. Możesz wyznaczyć różne dozwolone pory logowania się każdego dnia tygodnia. Więcej informacji w sekcji Kontrola korzystania z komputera;
- **kontrola dostępu do gier** – możesz wybrać gry odpowiednie do wieku, rodzaj treści jakie zostaną zablokowane, zdecydować czy chcesz zablokować czy zezwolić na określone lub gry bez ratingu. Więcej informacji w sekcji Określ, w jakie gry dzieci mogą grać;
- **zezwolenie lub zablokowanie poszczególnych programów** – możesz zabronić dzieciom korzystania z konkretnych programów. Więcej informacji w sekcji Zabroń dzieciom korzystania z konkretnych programów[2].

8 Microsoft radzi wykonanie czterech kroków w celu ochrony prywatności i bezpieczeństwa dzieci podczas korzystania z komputera:[3]:

- krok 1. Zdecyduj, co twoje dziecko może i czego nie może przeglądać w Internecie,
- krok 2. Wzmocnij ochronę i prywatność,
- krok 3. Monitoruj dzieci, gdy są one online,
- krok 4. Przypominaj dzieciom, żeby nie rozmawiały z nieznajomymi online,

9 Inne sugerowane przez Microsoft istotne środki ostrożności dotyczące bezpieczeństwa korzystania z sieci w domu wyrażają się hasłami:

- Chroń swój komputer.
- Chroń wrażliwe dane.
- Twórz mocne hasła i zachowaj je dla siebie.
- Dbaj o swoją reputację w sieci.
- Rozważnie korzystaj z portali społecznościowych.
- Podejmuj dodatkowe środki zapobiegawcze chroniące dzieci online.

10 Istnieje wiele produktów komercyjnych, dzięki którym można zarządzać korzystaniem z Internetu oraz chronić przed nieodpowiednimi treściami i zagrożeniem ze strony portali społecznościowych, nieznajomych i innymi. Jednym z najbardziej popularnych jest McAfee Family Protection (cena 49,99 USD na trzy komputery) produkowany przez McAfee, największą firmę na świecie tworzącą zabezpieczenia. Pozwalają one na[4]:

- ochronę dzieci przed nieodpowiednimi treściami,
- zarządzanie dostępem dzieci do odpowiednich nagrań na YouTube,
- zarządzanie czasem, jaki dzieci spędzają online,
- zarządzanie dostępem do komunikatorów,
- korzystanie z pozytywnych elementów portali społecznościowych,
- zabezpieczanie informacji dotyczących twojej rodziny,
- zapewnienie bezpieczeństwa twoim dzieciom online,
- natychmiastowe powiadamienie o zagrożeniu, o którym możesz porozmawiać z dzieckiem,

[2] http://windows.microsoft.com/en-US/windows-vista/Set-up-Parental-Controls, data dostępu: 7.02.2013.

[3] http://www.microsoft.com/security/family-safety/childsafety-steps.aspx, data dostępu: 7.02.2013.

[4] http://home.mcafee.com/store/family-protection, data dostępu: 8.02.2013.

- dostęp do odpowiednich dla wieku twojego dziecka filmów,
- zabezpieczenie przed słuchaniem utworów, w których używany jest wulgarny język.

11 Kolejnym produktem dla ochrony rodzicielskej jest CyberPatrol (cena 39,95 USD na trzy komputery), który zezwala na blokowanie stron pornograficznych i innych nieodpowiednich treści, ustalanie limitów czasowych dla gier komputerowych i korzystania z Internetu, kontrolowanie dostępu do gier i komunikatora etc.[5].

12 Magazyn „PC" dostarcza aktualne zestawienie i ocenę produktów w Parental Control & Monitoring[6].

13 **UZALEŻNIENIE OD KOMPUTERA: PRAKTYCZNE ŚRODKI ZAPOBIEGAWCZE**

Margaret A. Shotton (1989) stawia pytanie, czy należy mówić o uzależnieniu od komputera (ang. *computer addiction*) czy raczej zależności od komputera (ang. *computer dependence*). Analizuje użycie obu sformułowań i dochodzi do wniosku, że poprawna definicja nadmiernego korzystania z komputera to zależność od komputera. Niektórzy naukowcy używają terminu użytkowanie problematyczne (ang. *problematic usage*)[7] (Yee, 2006). Jednak wyrażenie uzależnienie od komputera wstępuje najczęściej. Wikipedia przedstawia taką właśnie definicję[8]:

14 Uzależnienie od komputera jest chorobą psychiczną spowodowaną nadmiernym używaniem komputera do takiego stopnia, że ma ono negatywny wpływ na życie codzienne. Nadmierne używanie może prowadzić do problemów w interakcjach społecznych, zaburzeń nastroju, osobowości, etyki zawodowej, związków, procesów myślowych lub zaburzeń snu.

15 Badania przeprowadzone na Uniwersytecie Stanforda dowodzą, że mężczyźni są podatni na uzależnienie od gier wideo[9]. Psychoterapeuta Shavaun Scott zauważył, że osoba uzależniona od gier komputerowych prowadzi niejako podwójne życie: pierwotne i wtórne. Życie pierwotne to rzeczywistość, w której żyjemy. Natomiast życie wtórne to świat wirtualny, w którym toczy się gra. Doktor Scott stwierdza, że problemy pojawiają się wtedy, gdy uzależniony zaczyna być tak pochłonięty drugim życiem, że zaniedbuje obowiązki prawdziwego życia[10].

16 **ZWIĄZEK GIER WIDEO Z UZALEŻNIENIEM OD KOMPUTERA**

17 K. Dini, psychiatra i autor popularnej książki dotyczącej uzależnienia od gier, zauważa że mimo iż zwyczajowe granie może wskazywać na brak rozrywki w społeczeństwie, nadmierne granie może prowadzić do lub ujawnić chorobę[11].

---

5 http://www.cyberpatrol.com/home/, data dostępu: 8.02.2013.

6 patrz http://www.pcmag.com/category2/0,2806,1639158,00.asp, data dostępu, 8.02.2013)

7 Yee N., *The Psychology of Massively Multi-User Online Role-Playing Games: Motivations, Emotional Investment, Relationships and Problematic Usage*, w: Schroeder R. & Axelsson A. (Eds.), *Avatars at Work and Play: Collaboration and Interaction in Shared Virtual Environments,* London, Springer-Verlag, 2006, pp. 187—207

8 http://en.wikipedia.org/wiki/Computer_addiction, data dostępu: 8.02.2013.

9 Brandt M., *Video Games Activate Reward Regions of Brain in Men More than Women*, Stanford study finds. Stanford Med website, http://med.stanford.edu/news_releases/2008/february/videobrain.html, February 8 2008; retrieved: 9 of February 2013.

10 Wywiad z Shavaunem Scottem, Youtube, http://youtube.com/watch?v=8U1T9ZumALk&feature=related, data dostępu: 9.02.2013.

11 D. Kourosh, *Video Game Play and Addiction: a Guide for Parents*, Bloomington, iUniverse Inc, 2008

18 Kolejnym istotnym pytaniem jest zdefiniowanie granicy, kiedy można mówić o uzależnieniu od komputera.

19 Generalnie uzależnienie od komputera niczym nie różni się od innych form uzależnienia. Jedzenie, robienie zakupów czy uprawianie seksu są zupełnie normalnymi czynnościami. Dlaczego zatem niektórzy mają skłonność nadmiernego angażowania się w nie? Zwykle osoby uzależnione cechuje jakiś stopień predyspozycji – biologicznej, psychologicznej lub często kombinacji obydwu. D. Kourosh tłumaczy to na przykładzie braku umiaru w wypadku gier komputerowych:

> „które mogą stanowić przeciwwagę dla braków w innych sferach życia gracza. Świat wirtualny może w pewnym stopniu stanowić substytut braków w życiu osobistym, zawodowym czy edukacji. Jednak taki sposób rekompensowania może prowadzić do pogłębiania się deficytów w życiu realnym, co prowadzi do powstania cyklu podobnego w przypadku każdego uzależnienienia, czy to od jedzenia, zakupów czy seksu"[12].

20 Nadmierne używanie komputera może przekształcić się w uzależnienie, jeśli towarzyszą temu negatywne skutki. D. Angres i K. Bettinardi podkreślają, że uzależnienie stanowi nieprzerwane używanie substancji lub zachowania wpływające na zmianę nastroju mimo negatywnych skutków:

> „System nagradzania wspólny zapamiętywaniu, uczeniu się, motywacji, kontroli i podejmowaniu decyzji charakteryzuje również nałogi (s. 696)[13]".

21 Korzystanie z komputera czy granie w gry wideo przeradza się w nałóg, jeśli ma charakter ekstremalny, kompulsywny i urasta do rangi problemu w życiu codziennym: niekoniecznie wszystkie osoby korzystające z komputera czy grające w gry wideo uzależnią się od nich.

22 Istnieje wiele sposobów zapobiegania uzależnieniu od komputera. Najprostszym z nich jest ograniczanie czasu spędzonego przed komputerem, ale istotna jest również wiedza dotycząca wykorzystywania sieci oraz znajomość świata gier komputerowych.

23 Rodzice wyposażeni są w środki ograniczające używanie komputera, ale muszą również stosować środki zapobiegawcze, np. kontrolowanie gier komputerowych. Dobrym sposobem jest granie z dziećmi i w ten sposób regulowanie czasu poświęconego na tę czynność.

24 Rodzice powinni potrafić rozpoznać symptom kompulsywnego grania w celu zapobiegania uzależnieniu. Muszą oni edukować dzieci na tematy dotyczące zagrożeń związanych z uzależnieniem od komputera, np. wzrost masy ciała, spadek sprawności fizycznej, izolacja społeczna. Istnieje wiele problemów natury zdrowia fizycznego utożsamianych z uzależnieniem od gier, jak brak higieny osobistej, syndrom suchego oka, bóle pleców oraz migreny. Ponadto, nadużywanie Internetu może się przyczynić do powstawania depresji i zaburzeń snu.

25 Najlepszym, co możemy zrobić, jest edukowanie rodziców i przede wszystkim zapobieganie uzależnieniu od gier. Rodzice muszą być w stanie ograniczać zwyczaje związane z graniem.

26 Czytanie i dyskusja z dzieckiem dotycząca powieści Cora Doctorowa *For the Win* może również odegrać pozytywną rolę. Powieść Doctorowa opowiada o wzroście wirtualnej ekonomii, do którego prowadzą gry RPG, w które gra wielu graczy online (MMORPG). Główne postacie Mathew, Wei Dong i Mala mieszk

[12] Tamże, s. 46

[13] D. H. Angres, K. Bettinardi-Angres, *The Disease of Addiction: Origins, Treatment and Recovery*, "Dis Mon", 54/2008, 10, pp. 696–721

kają w różnych częściach świata, a mimo to łączą je gry komputerowe i są od nich uzależnieni.

27 OCHRONA PRZED CYBERPORNOGRAFIĄ

Pramod K. Nayar zauważa, że na cyberpornografię składają się zarówno wartości społeczne (włączając normy i prawa), jak również technologie (odbiór na żywo, ang. webcasting, przesyłanie strumienia wideo).

28 Termin cyberpornografia zawiera nowe aspekty:

- komercjalizacja i normalizacja aktów/zachowań stygmatyzowanych na rynkach tradycyjnych (to drugie sprowadziło pornografię do podziemia);
- pojawienie się zjawiska związanego z wyzwolonym wyrażaniem samego siebie oraz grupowym uprawomocnieniem (co można określić jako wzrost ekspresyjnej seksualności);
- nowy związek między producentem i konsumentem, w którym na podstawie informacji zwrotnej (zwanej „czego chcą konsumenci") rozwijane są nowe techniki i prezentowane treści;
- redefinicja pornografii samej w sobie jako formy rozrywki, funkcji edudacyjnej i stylu życia.

29 Kolejnym agrumentem, który należy rozważyć, jest rozróżnienie pomiędzy cyberseksem i cyberpornografią. Leila Green sądzi, że definicje cyberseksu i cyberpornografii różnią się od siebie, zaś cyberpornografia może być postrzegana jako rodzaj cyberseksu[14]. Ponadto, cyberseks zawiera w sobie również erotyczne interakcje za obopólną zgodą partnerów łączących się za pomocą kamery i innych urządzeń elektronicznych.

30 Pornografia w Internecie stanowi szczególnie trudny problem, gdyż tradycyjne koncepty publicznej/prywatnej przestrzeni niekoniecznie pokrywają się z cyberprzestrzenią. Konsumpcja pornografii za pośrednictwem komputera jest dalece prywatną aktywnością, mającą miejsce nie tylko w domowym zaciszu (boksu/pokoju w pracy), ale również w warunkach wyizolowanej, efemerycznej relacji pomiędzy użytkownikiem i ekranem komputera. Jednocześnie jest to konsumpcja publiczna, gdyż treści te rozprzestrzeniają się na liczne strony, przekraczają granice w sensie fizycznym, gdzie inne formy pornografii, takie jak księgarnie czy kina, znacznie łatwiej identyfikować i regulować[15].

31 Ważnym odniesieniem dotyczącym pornografii w cyberprzestrzeni i ochrony dzieci jest publikacja Służby Badawczej Kongresu Stanów Zjednoczonych zatytułowana *Cyberporn, Protecting Our Children from the Back Alleys of the Internet*.

32 Oprogramowanie do kontroli rodzicielskiej jest środkiem pozwalającym chronić nasze dzieci przed cyberprzestrzenią. Mimo wszystko najważniejsze, by rodzice edukowali się na temat funkcjonowania Internetu. Ponadto, powinni dzielić się ze swoimi dziećmi wiedzą na temat tego, jak w bezpieczny sposób wyszukiwać informacje, jak przez przypadek nie wejść na strony o treściach pornograficznych, a w szczególności jak dzieci powinny się zachować, gdy mimo wszystko znajdą się na takiej stronie.

[14] B. Cronin, E. Davenport, E. Zones: *Positioning Pornography in the Digital Economy*, "The Information Society", 17/2001, 1, s. 33–48

[15] R. K. Westheimer, Sex for dummy, John Wiley & Sons, 2011

33 PODSUMOWANIE – ZALECENIA

WHO@ (Working to Halt Online Abuse)[16] wydała następujące zalecenia w celu bezpiecznego korzystania z sieci:

- używaj neutralnego płciowo loginu/adresu e-mail;
- używaj darmowego konta e-mail jak Hotmail (www.hotmail.com) lub YAHOO! (www.yahoo.com) w przypadku nowych grup/list mailingowych, czatowania, IM, e-maili od nieznajomych, forów dyskusyjnych, wypełniania formularzy i innych form aktywności online;
- nie podawaj swojego głównego adresu e-mail nieznajomym (patrz wyżej);
- nie zamieszczaj zbyt wiele informacji w swoim profilu, w szczególności na stronach sieci społecznych. Zwracaj uwagę na to co zamieszczasz!
- zmień swoje ustawienia, tak by twój profil mogły oglądać jedynie osoby znajome/przyjaciele, którym na to zezwalasz;
- obserwuj przez jakiś czas nowe grupy, fora, chatroomy, zanim włączysz się do dyskusji;
- jeśli już jesteś uczestnikiem, bądź ostrożny – pisz tylko to, co powiedziałbyś w kontakcie osobistym;
- nie bądź zbyt łatwowierny online – nie ujawniaj informacji osobistych dopóki naprawdę nie będziesz ufał drugiej osobie;
- instynkt może w pierwszej chwili podpowiadać obronę – nie rób tego – tak zwykle zaczyna się prześladowanie w sieci;
- nie daj się nabrać na wiadomości e-mail (ang. phishing) informujące o tym, że twoje konto zostało zablokowane lub wymaga aktualizacji – to wyłudzanie informacji!

34 Dodatkowe zalecenia są następujące:

- e-maile możesz przesyłać dalej dopiero po uzyskaniu zgody autora oryginalnej wiadomości;
- otwieraj jedynie wiadomości od osób, które znasz i nigdy nie odpowiadaj na nękanie/podejrzane wiadomości;
- nie zamieszczaj swoich zdjęć online bez zgody osoby dorosłej;
- nigdy nie zamieszczaj zdjęć swoich przyjaciół bez ich zgody;
- edukuj przyjaciół na temat zagrożeń cyberprzestrzeni.

35 Jeśli otrzymasz wiadomości mające na celu zastraszenie:

- zachowaj wszystko! Nie usuwaj wiadomości, lecz umieść je w osobnym folderze na twoim dysku twardym, dyskietce, innym nośniku i zachowaj wydruk;
- skontaktuj się z policją, z Wydziałem Wsparcia do Zwalczania Cyberprzestępczości lub kimś, kto zajmuje się przestępstwami w sieci.

36 Kilka wskazówek dotyczących ochrony naszych dzieci:

doradzaj im, dawaj pozytywne, aktywne wsparcie. Zachęcaj do zgłaszania aktów przemocy;

- zapewnij, że nie ograniczysz dostępu do komputera, telefonu lub innych technologii;
- działaj natychmiast. Nie czekaj, by się przekonać, czy przemoc się skończy i zgłoś incydent w szkole lub online;
- szukaj znaków przemocy w sieci (np. gdy dziecko wydaje się niespokojne, kiedy jest online);
- nie odpowiadaj na zaczepki telefoniczne/esemesowe/online: przestępcy czekają na reakcję;
- trzymaj komputer w centralnym miejscu. Jest to istotne zwłaszcza w wypadku nastolatków.

[16] WHO@ (http://www.haltabuse.org/) jest najstarszą organizacją bezpieczeństwa online pomagającą dorosłym ofiarom cyberstalkingu.

37 Inne wskazówki zostały zebrane w broszurze *Child Safety on the Information Highway* wydanej przez Narodowe Centrum ds. Zaginionych i Wykorzystywanych Dzieci (NCMEC), która zawiera kilka przydatnych rad:

- wyznacz reguły korzystania z komputera przez twoje dziecko i omów je z nim;
- nie pozwól na to, by twoje dziecko ujawniało w sieci informacje osobiste, takie jak adres, numer telefonu lub nazwa szkoły;
- nie pozwól dziecku na organizowanie spotkań w sieci z nieznajomymi lub na to, by wysyłało swoje zdjęcia;.
- każ dziecku natychmiast zgłosić otrzymanie niepokojącej wiadomości.

BIBLIOGRAFIA:

Angres D. H., Bettinardi-Angres K., *The Disease of Addiction: Origins, Treatment and Recovery*, "Dis Mon", 54/2008, 10, pp. 696–721.

Brandt M., *Video Games Activate Reward Regions of Brain in Men More than Women*, Stanford study finds. Stanford Med website, <http://med.stanford.edu/news_releases/2008/february/videobrain.html>, February 8 2008; retrieved: 9 of February 2013.

Cronin B., Davenport E., Zones E.: *Positioning Pornography in the Digital Economy*, "The Information Society", 17/2001, 1, pp. 33–48.

Green L., *The Internet: An Introduction to New Media*, Oxford, Berg, 201.

Kourosh D., *Video Game Play and Addiction: a Guide for Parents*, Bloomington, iUniverse Inc, 2008.

Kowalsky R. M., Limber S. P., Agatstone P. W., *Cyberbullying: Bullying in the Digital Age*, Wiley-Blackwell, 2012 (second edition).

Nayar P. K., *An Introduction to New Media and Cybercultures*, Chicester, Wiley-Blackwell, 2010.

Shotton M. A., *Computer Addiction? A Study of Computer Dependency*, London, Taylor & Francis Ltd, 1989.

United States Congress Research, Cyberporn, Protecting Our Children From the Back Alleys of the Internet, Joint Hearing Before the Subcommittee on Basic Research and the Subcommittee on Technology of the Committee on Science, U.s. House of Representatives, One Hundred Fourth Congress, 2010 (First Session, July 26, 1995).

Westheimer R. K., *Sex for dummy*, John Wiley & Sons, 2011.

Yee N., *The Psychology of Massively Multi-User Online Role-Playing Games: Motivations, Emotional Investment, Relationships and Problematic Usage*, w: Schroeder R. & Axelsson A. (Eds.), *Avatars at Work and Play: Collaboration and Interaction in Shared Virtual Environments,* London, Springer-Verlag, 2006, pp. 187—207.

ZAGROŻENIA SPOŁECZNE CYBERPRZESTRZENI
DOŚWIADCZENIA ŁOTEWSKIE

Velta Lubkina, Gilberto Marzano

1 WPROWADZENIE

Niniejsze opracowanie jest skróconym raportem z badania przeprowadzonego przez Juliję Drebeinikę, studentkę czwartego roku studiów kierunku Edukacja i projektowanie Rezeknes Augstskola.

2 ORGANIZACJA BADANIA

Badanie zostało przeprowadzone w 2010 roku, w gimnazjum w Rezekne, przy pomocy ankiety i wywiadów. Ankieta została sporządzona przy współpracy z nauczycielami.

Metoda: ankieta, wywiad

Liczba ważnych wypełnionych ankiet: 107 (uczniowie w wieku 6–8 lat oraz nastolatki)

Wywiady: 5 (nauczyciele)

Cel: weryfikacja poziomu zagrożenia uzależnienia od komputera i próba wynalezienia środków zapobiegawczych

3 PODSUMOWANIE I ANALIZA WYNIKÓW ANKIETY

DOSTĘP DO KOMPUTERA

Większość uczniów (89%) używa komputera w domu, podczas gdy 56% korzysta z komputera u przyjaciół. Natomiast 35% korzysta z komputera dostępnego w szkole, a 19% respondentów zaznaczyło odpowiedź „inne", zaznaczając, że np. korzysta z komputera w miejscu pracy rodziców.

Uczniowie mają łatwy dostęp do komputera, ale korzystają z niego bez nadzoru rodzicielskiego. Wielu z nich używa komputera u przyjaciół i do komunikacji z nimi.

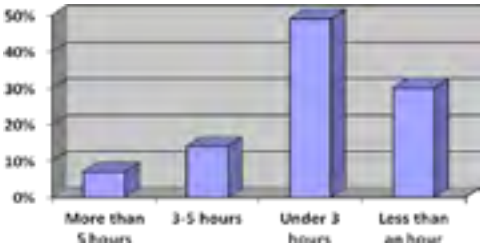
4 CZĘSTOTLIWOŚĆ KORZYSTANIA Z KOMPUTERA

70% uczniów korzysta z komputera codziennie, podczas gdy 26% używa go 2–3 razy w tygodniu, natomiast 3% - raz w tygodniu. Jedynie 1% korzysta z komputea 2–3 razy w miesiącu. Biorąc pod uwagę fakt, że ponad połowa ankietowanych uczniów przyznaje codzienne korzystanie z komputera, istnieje możliwość występowania przypadków uzależnienia w badanej grupie.

5 CZAS SPĘDZANY PRZED KOMPUTEREM

Ilość czasu spędzanego przed komputerem ilustruje Wykres 1.

Wykres 1. Czas spędzany przed komputerem



Źródło: opracowanie własne

Z podanych odpowiedzi wynika, że mniej niż 30% uczniów spędza mniej niż godzinę przy komputerze, 49% spędza 3 godziny, 14% 3–5 godzin, natomiast 7% powyżej 5 godzin. Tym samym ryzyko występowania zagrożenia uzależnienia od komputera wydaje się być oczywiste.

6 CEL KORZYSTANIA Z KOMPUTERA

65% respondentów używa komputera do nauki i wyszukiwania informacji, 33% do wysyłania e-maili, 24% do czatowania, 69% do odwiedzania portali społecznościowych.

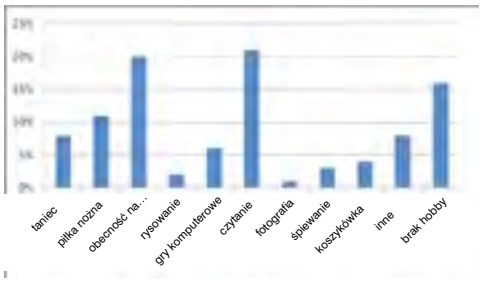
61% gra na komputerze, natomiast 71% przy jego pomocy pobiera muzykę i filmy. Należy przy tym podkreślić, że gry komputerowe, czatowanie i inne formy roz-

rywki mogą prowadzić do zależności od komputera.

7 PASJE/HOBBY NASTOLATKÓW

Wykres 2 przedstawia, jak uczniowie spędzają swój czas wolny.

Wykres 2. Hobby nastolatków



Źródło: opracowanie własne

Reasumując: 84% uczniów ma jakieś hobby, np. taniec, książki, koszykówka itd., podczas gdy 16% nie ma żadnego hobby. Dla 6% hobby stanowią gry komputerowe. Jednak należą oni do mniejszości, gdyż większość uczniów preferuje inne formy aktywności.

8 DOMOWE OBOWIĄZKI NASTOLATKÓW

Wykres 3. Zaangażowanie w prace domowe

Źródło: opracowanie własne

Większość nastolatków pomaga przy pracach domowych, takich jak zmywanie naczyń (33%), sprzątanie pokoju (75%), opieka nad bratem lub siostrą (7%). Wykres 3. dowodzi, że uczniowie nie są zbytnio zaangażowani w prace domowe.

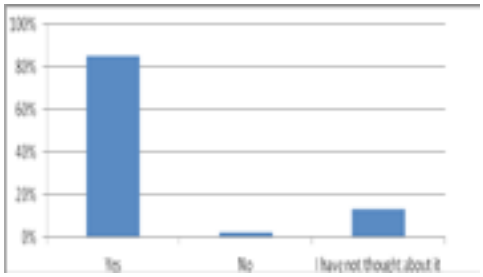
9 Z CZYM NASTOLATKI SPOTKAŁY SIĘ W INTERNECIE

56% nastolatków przyznaje, że często są świadkami prześladowania w sieci. 39% otrzymało nieprzyjemne wiadomości lub ogłoszenia, podczas gdy 27% przyznaje się do bólu pleców i oczu, jeśli zbyt wiele czasu spędzi przed komputerem. 29% uczniów zaniedbuje swoją pracę domową, spędzając wiele czasu w Internecie, 34% używa komputera jedynie w celu serfowania po Internecie, 20% zdradza prywatne informacje nieznajomym, takie jak nazwisko, numer telefonu, adres, etc. Zdarza się że uczniowe (7%) opuszczają szkołę, ponieważ spędzają cały wieczór w Internecie, natomiast 1% zupełnie zaniedbuje swoje obowiązki.

10 ŚWIADOMOŚĆ NASTOLATKÓW DOTYCZĄCA UZALEŻNIENIA OD KOMPUTERA

Badanie zweryfikowało rozumienie zagrożenia uzależnienia od komputera spowodowanego nadmiernym używaniem komputera. Wyniki przedstawia Wykres 4.

Wykres 4. Świadomość nastolatków dotycząca uzależnienia od komputera



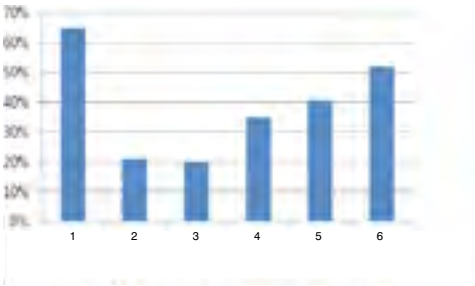
Źródło: opracowanie własne

Odpowiedzi pokazały, że 85% nastolatków zdaje sobie sprawę i zgadza się z faktem, że nadmierne korzystanie z komputera może prowadzić do problemów w szkole i wpływać na relacje z rówieśnikami i rodziną, 2% wierzy, że skutkiem może być uzależnienie. Część respondentów (13%) nie ma zdania na ten temat.

15 **PROBLEMY POWODOWANE NADMIERNYM KORZYSTANIEM Z KOMPUTERA**

Wielu uczniów jest zdania, że nadmierne korzystanie z komputera (patrz: wykres 5.) może prowadzić do problemów zdrowotnych (41%), braku czasu (52%), sporów z rodzicami (65%), absencji w szkole (21%), pogorszenia relacji z przyjaciółmi (20%), problemów w komunikacji (35%).

Wykres 5. Problemy powodowane nadmiernym korzystaniem z komputera



legenda: 1-konflikty z rodzicami, 2-nieobecność w szkole, 3-pogorszenie relacji z przyjaciółmi, 4-problemy w komunikacji, 5-problemy zdrowotne, 6-brak czasu

Źródło: opracowanie własne.

12 **INTERPRETACJA WYWIADÓW Z NAUCZYCIELAMI**

Poniższe zestawienie jest wynikiem wywiadów przeprowadzonych z pięcioma nauczycielami.

Okazuje się, iż nauczyciele byli dobrze poinformowani na temat problemów związanych z uzależnieniem od komputera. Zwykle zgadzali się ze stwierdzeniem, że nadmierne korzystanie z komputera prowadzi do absencji w szkole, braku motywacji do nauki, braku udziału w lekcjach, odmiennego zachowania i problemów w komunikacji.

13 Nauczyciele podkreślają, iż nadmierne używanie komputera wpływa negatywnie na nastawienie nastolatków do ich obowiązków, wywołuje spadek umiejętności uczenia się oraz zakłóca procesy edukacyjne. Niektórzy dysponują szeroką wiedzą dotyczącą uzależnienia od komputera, jednak istnieją tacy nauczyciele, którzy mają jedynie powierzchowne informacje na ten temat i nie są w stanie zapewnić niezbędnego wsparcia i zapobiegać problemom.

Dwóch nauczycieli wyszło z inicjatywą mającą na celu przyciągnięcie uwagi uczniów do zagrożeń związanych z uzależnieniem od komputera. Jeden zasugerował zwiększenie liczby zajęć informatycznych. Nauczyciel informatyki zaproponował, że poprowadzi lekcje dotyczące zagrożeń związanych z komputerem.

Nauczyciele podkreślali potrzebę istnienia broszur, materiałów informacyjnych, reklam, nagrań wideo na temat zagrożenia nadmiernym korzystaniem z komputera. Zasugerowali również stworzenie audycji w radiu i telewizji na ten temat.

Nauczyciele sugerowali:
- wykłady na temat różnych form uzależnienia od komputera, ich charakterystyki, przyczyn i skutków;
- omówienie tego problemu na lekcjach edukacyjnych dotyczących zdrowia;
- prowadzenie dyskusji z nastolatkami i ich rodzicami;
- prowadzenie lekcji na temat zagrożeń związanych z nadmiernym korzystaniem z komputera.

14 **Badanie sugeruje następujące inicjatywy w celu ograniczenia zagrożenia uzależnieniem od komputera:**
- stworzenie zaleceń dla nauczycieli, pracowników społecznych, psychologów;
- edukacja nastolatków, rodziców, nauczycieli na temat zapobiegania uzależnieniu od komputera;
- stworzenie grup wsparcia;
- wskazanie lektur i innych materiałów przydatnych w zrozumieniu problemów spowodowanych nadmiernym korzystaniem z komputera;
- zaproponowanie alternatywnych spo-

sobów spędzania czasu wolnego;
- seminaria dla rodziców nastolatków;
- gry i zajęcia sportowe;
- gry fabularne (RPG) w szkole.

15 PODSUMOWANIE

- większość uczniów jest świadoma tego, że nadmierne korzystanie z komputera może prowadzić do uzależnienia;
- większość nastolatków uważa, że korzysta z komputera w sposób rozważny, nie narażając się na ryzyko uzależnienia, ale istnieje wysokie prawdopodobieństwo, że przynajmniej 1% z nich należałoby uznać za uzależnionych. Nastolatki korzystają z komputera w różnych celach, głównie dla rozrywki, co może prowadzić do nadmiernej fascynacji komputerem;
- większość uczniów korzysta z komputera codziennie;
- nauczyciele wierzą, że nadmierne korzystanie z komputera w negatywny sposób wpływa na aktywność uczniów;
- są trudności w realizacji szkolnych inicjatyw dotyczących ryzyka uzależnienia od komputera;
- potrzeba udzielania rad nastolatkom na temat poprawnego korzystania z komputera;
- potrzeba wsparcia nauczycieli zaleceniami i radami praktycznymi dotyczącymi zapobiegania zagrożeniu uzależnieniem się od komputera przez nastolatki.

Załącznik:

Poniżej znajduje się kwestionariusz sporządzony w celu zbadania skali uzależnienia od komputera wśród studentów.

Zaznacz miejsca, w których używasz komputera (możesz zaznaczyć więcej niż jedną odpowiedź)

- ☐ w domu
- ☐ w szkole
- ☐ u przyjaciół
- ☐ inne

Jak często korzystasz z komputera?

- ☐ codziennie,
- ☐ niemalże codziennie
- ☐ 2–3 razy w tygodniu
- ☐ raz w tygodniu
- ☐ 2–3 razy w miesiącu
- ☐ rzadziej niż raz w miesiącu

W jakim celu zwykle korzystasz z komputera? (możesz zaznaczyć więcej niż jedną odpowiedź)

- ☐ wyszukiwanie informacji
- ☐ nauka
- ☐ kontakty (czat, Skype)
- ☐ odwiedzanie portali społecznościowych
- ☐ gry
- ☐ odbieranie e-maili
- ☐ pobieranie muzyki, filmów etc.
- ☐ inne

Czy masz pasję, hobby? Jakie?

_____

_____

_____

Jakie są twoje obowiązki w domu? (możesz zaznaczyć więcej niż jedną odpowiedź)

- ☐ gotowanie
- ☐ zmywanie naczyń
- ☐ opiekowanie się bratem/siostrą
- ☐ sprzątanie pokoju
- ☐ wynoszenie śmieci
- ☐ nie mam obowiązków
- ☐ inne

Z czym spotkałeś się w Internecie? (możesz zaznaczyć więcej niż jedną odpowiedź)

- ☐ zdjęcia lub gry, w których ktoś uderza lub atakuje innych
- ☐ otrzymujesz pogróżki
- ☐ bolą cię plecy, oczy etc., jeśli siedzisz przy komputerze przez dłuższy czas
- ☐ zdarza się, że nie wykonujesz swoich zadań, ponieważ zbyt wiele czasu spędzasz serfując w Internecie
- ☐ czasami masz jedynie ochotę serfować w Internecie
- ☐ ujawniasz poufne informacje dotyczące ciebie, twojej rodziny nieznajomym (numer telefonu, adres, etc.)
- ☐ czasem opuszczasz lekcje w szkole, ponieważ poprzedniego dnia do późna serfowałeś w Internecie
- ☐ inne

Czy zdajesz sobie sprawę że nadmierne używanie komputera może prowadzić do uzależnienia?

- ☐ tak
- ☐ nie
- ☐ nigdy się nad tym nie zastanawiałem/am

Do jakich problemów może prowadzić nadmierne używanie komputera? (możesz zaznaczyć więcej niż jedną odpowiedź)

- ☐ konflikty z rodzicami
- ☐ nieobecność w szkole
- ☐ pogorszenie relacji z przyjaciółmi
- ☐ problemy w komunikacji
- ☐ problemy zdrowotne
- ☐ brak czasu
- ☐ inne

Dziękujemy za wypełnienie ankiety!

DOŚWIADCZENIA
WDRAŻANIA PROGRAMÓW DOTYCZĄCYCH ZAGROŻEŃ CYBERPRZESTRZENI WŚRÓD PRACOWNIKÓW SOCJALNYCH W POLSCE

Łukasz Tomczyk

1 WPROWADZENIE

Niniejsze opracowanie jest studium przypadku szkoleń z zakresu bezpieczeństwa dzieci i młodzieży w sieci zrealizowanych w ramach zadań własnych Miejskiego Ośrodka Pomocy Społecznej w Cieszynie. Prezentowany kurs został w praktyce zaimplementowany w ramach spotkań, w których uczestniczyli pracownicy socjalni, pedagodzy, osoby zaangażowane w lokalne środowisko organizacji pozarządowych. Poniższy program szkolenia był nastawiony na pracę indywidualną, przy jednoczesnym wykorzystaniu doświadczeń zgromadzonych osób. Pierwsza partia szkoleń odbyła się na początku maja 2012 r., sukces przedsięwzięcia przyczynił się do podjęcia dalszych szkoleń, tym razem w ramach cyklicznego programu realizowanego przez MOPS w Cieszynie, jakim jest Szkoła Wczesnej Profilaktyki[1].

3

Szkolenie obejmowało 6 godzin dydaktycznych[2] w sali komputerowej z dostępem do Internetu. Każdy z uczestników miał pełne prawa administracyjne umożliwiające instalowanie dodatkowego oprogramowania w systemie operacyjnym. Ponadto prowadzący zajęcia posiadał rzutnik multimedialny wraz z głośnikami. Głównym celem zajęć było zapoznanie pedagogów oraz pracowników socjalnych ze współczesnymi zagrożeniami wynikającymi z upowszechnienia nowych mediów wśród dzieci i młodzieży.

4 CELE SZKOLENIA

obejmowały m.in.:

1. ukazanie istoty funkcjonowania nowych mediów w aspekcie negatywnych pochodnych wynikających ze swoistości urządzeń mikroelektronicznych;
2. identyfikację nowych trendów w wykorzystywaniu komputera osobistego oraz Internetu wśród dzieci i młodzieży;
3. zaprezentowanie typologii aplikacji rozrywkowych wykorzystywanych najczęściej przez uczniów w różnych grupach wiekowych;
4. ukazanie roli komputera i Internetu w zaspokajaniu potrzeb dzieci i młodzieży w różnych fazach rozwojowych;
5. poznanie aktualnych zagrożeń związanych z nowymi mediami, oddziaływujących bezpośrednio i pośrednio na dzieci i młodzież;
6. nabycie kompetencji technicznych pozwalających na rozpoznawanie treści szkodliwych dostępnych w Internecie oraz w urządzeniu lokalnym;
7. zapoznanie się z technikami diagnozy uzależnienia od Internetu;
8. poznanie psychologicznych następstw wynikających z nadużywania i nieprawidłowego wykorzystywania Internetu oraz różnych typów gier;
9. ukształtowanie umiejętności weryfikacji komputera osobistego pod kątem legalności oprogramowania oraz charakteru przechowywanych danych;
10. zapoznanie się z metodami przeciwdziałania zachowaniom stwarzającym zagrożenie;
11. orientację w technicznych sposobach zabezpieczenia komputera osobistego przed treściami szkodliwymi;
12. poznanie prawnych następstw związanych z cyberprzestępstwami;
13. ukazanie roli osób znaczących (rodziców, rodzeństwa, opiekunów, nauczycieli) we współdziałaniu z dzieckiem na płaszczyźnie edukacji medialnej;

[1] Więcej na temat wydarzenia: *17 szkoła wczesnej profilaktyki* http://www.cieszyn.pl/files/Szkola%20Wczesnej%20Profilaktyki_2012%5B1%5D.pdf

[2] Z doświadczeń prowadzącego wynika jednak, że liczba 6 godzin jest niewystarczająca ze względu na rozległość tematyczną materiału. W trakcie zrealizowanych szkoleń uczestnicy otrzymali dodatkowe informacje w postaci prezentacji multimedialnej oraz hiperłączy, z którymi mogli się zapoznać w ramach samokształcenia.

14. zaznajomienie się z metodami działań edukacyjno-wychowawczych sprzyjających kształtowaniu prawidłowych postaw względem nowych mediów u dzieci i młodzieży.

5 REALIZACJA SZKOLENIA – POSZCZEGÓLNE ETAPY

Szkolenie rozpoczynało się od zapoznania się z doświadczeniami kursantów dotyczącymi bezpieczeństwa dzieci i młodzieży w sieci. Każdy z uczestników prezentował swoje potrzeby w zakresie wiedzy i umiejętności odnoszących się do prawidłowego korzystania z nowych mediów.

6 Kolejno kursanci mieli do wykonania zadanie związane z ukazaniem bezpośredniego i pośredniego oddziaływania nowych mediów na dzieci, młodzież i dorosłych. Grupę podzielono na trzy zespoły, każdy z nich otrzymał dużą planszę z flipcharta, na której miał wypisać, w jaki sposób media oddziaływują w sposób bezpośredni i pośredni (ukryty, z opóźnionym skutkiem, nie wprost). Zespoły w trakcie wykonywania zadania miały odnieść się do wybranej kategorii wiekowej w ciągu 10 minut, a następnie przy omawianiu wskazań podkreślano elementy wspólne i różnicujące pokolenia. Rozważania zostały uzupełnione typologią M. Prenskey'a odnośnie podziału społeczeństwa na cyfrowych autochtonów i imigrantów.

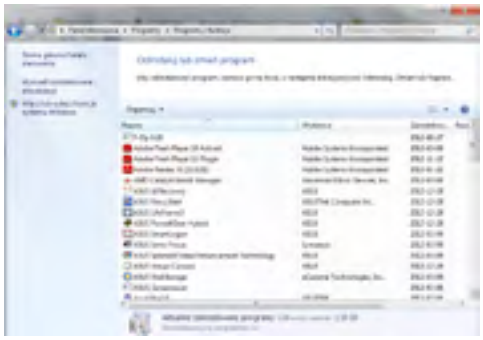
Tabela 1. Cyfrowi imigranci vs. cyfrowi autochtoni

Mają problemy ze zrozumieniem wirtualnej powierzchni widocznej przez okienko ekranu przesuwane nad nią.	Potrafią wyobrażać sobie i rozumieć wirtualną powierzchnię widzianą przez okienko przesuwanego nad nią ekranu.
Potrafią wyobrażać sobie i rozumieć treść długiego, linearnego tekstu czytanego z książki.	Mają problemy ze zrozumieniem długiego i skomplikowanego tekstu.
Lepiej rozumieją tekst drukowany.	Z powodzeniem czytają z małego ekranu.
Przedkładają tekst nad obraz i dźwięk.	Przedkładają obraz i dźwięk nad tekst.
Preferują linearne myślenie i szeregowe przetwarzanie informacji.	Preferują swobodny (hipertekstowy i hipermedialny) dostęp oraz równoległe przetwarzanie informacji.
Preferują cierpliwość, systematyczność i oczekiwanie skumulowanych, odroczonych rezultatów.	Preferują akcydentalne, krótkotrwałe uczenie się, eksperymentowanie, wielozadaniowość, oczekują szybkich efektów.
Wykorzystują podstawowe, standardowe funkcje posiadanych urządzeń mobilnych analogiczne do tradycyjnych. Traktują nowe technologie nieufnie.	Odkrywają wszystkie funkcje posiadanych urządzeń, wymyślają nowe ich zastosowania. Traktują nowe technologie kreatywnie, ufnie. Posiadane urządzenia mobilne traktują jak przedmioty bardzo osobiste.

Źródło: Hojnacki L., *Pokolenie m-learningu – nowe wyzwanie dla szkoły*, „E-mentor", 1(13)/2006., s. 26

7 Następne zadania były ściśle związane z użyciem komputera osobistego. Poproszono kursantów o uruchomienie komputera osobistego i wskazanie, w jaki sposób sprawdzić jego zawartość pod kątem zainstalowanych programów oraz użytkowania przeglądarki internetowej. Kursanci mieli za zadanie wybrać z listy programy komputerowe uważane za szkodliwe oraz wskazać gry komputerowe.

Obrazek 1. Panel sterowania



Źródło: widok ze strony

8 Ponadto kursanci zapoznali się z możliwością opcji historia stron w przeglądarce internetowej. Równocześnie omówiono zagadnienie technologii „cookies", a także zagadnienia anonimowości w sieci na przykładzie adresów IP (http://adres-ip.eu/index.php?ip=detect).

Obrazek 2. Sprawdzanie adresu IP

Źródło: widok ze strony

9 Zadanie dla uczestników:

- sprawdzenie historii odwiedzin sprzed tygodnia,
- usunięcie historii odwiedzin z wybranego dnia.

10 Uczestnicy szkolenia mieli także okazję zapoznać się z programem służącym monitorowaniu aktywności użytkowania komputera i Internetu w sposób zaawansowany. Ze strony producenta (http://www.visikid.pl) pobrano bezpłatną wersję testową oprogramowania i zainstalowano w komputerze. Instalacja aplikacji wymagała od uczestników pełnego dostępu do systemu operacyjnego oraz posiadania aktywnej skrzynki pocztowej.

11 Oczywiście twórcy programu podkreślają na swojej stronie internetowej, że „jeżeli rodzice poświęcają dzieciom odpowiednio dużo czasu, rozmawiają z nimi i objaśniają im świat, prawdopodobnie narzędzie do kontroli rodzicielskiej nie będzie im potrzebne. Niestety, bardzo wielu rodziców nie jest w stanie spędzać z dziećmi tyle czasu, ile powinni. Co nie znaczy, że nie obchodzi ich dobro własnych dzieci. Takim rodzicom Viskid z pewnością pomoże". Ponadto na stronie zadano pytanie, czy oprogramowanie Viskid jest w stanie zastąpić rozmowy edukacyjne i uświadamiające z dzieckiem? Projektanci aplikacji podkreślają, że „wręcz przeciwnie – ma je prowokować. Jeżeli rodzic uznaje, że dziecko korzysta z komputera w nieodpowiedni sposób, musi z nim o tym porozmawiać, wyjaśnić i skłonić do zmiany zachowania. W naszym programie do kontroli rodzicielskiej nie ma magicznego przycisku »blokuj«, bo to nie jest metoda wychowania dziecka"[3].

12 Viskid jest typem programowania, które nie blokuje stron internetowych, lecz jedynie pozwala na monitoring następujących parametrów pracy użytkownika:

- czas korzystania z komputera i Internetu,
- adresy odwiedzanych stron www,
- kategoria odwiedzanych stron www,
- rodzaj uruchamianych aplikacji na komputerze.

13 Aplikacja pozwala na monitorowanie maksymalnie trojga użytkowników, pierwsze raporty są dostępne już po pięciu minutach od wgrania programu do komputera i zalogowaniu się w panelu rodzica na stronie internetowej. Informacja o aktywności dziecka w sieci jest wysyłana, także w formie raportów, na podane w trakcie rejestracji konto rodzica.

Obrazek 3. Panel administracyjny programu Viskid

Źródło: widok ze strony

[3] *Kontrola rodzicielska,* http://www.visikid.pl/.

14 Zadanie dla uczestników:

- przed przerwą pedagodzy i pracownicy socjalni mają za zadanie przejrzeć kilka stron internetowych,
- po przerwie kursanci wymieniają się swoimi loginami i hasłami do programu Viskid, aby sprawdzić zdalnie aktywność w sieci innego użytkownika,
- zadanie to ma na celu ukazanie, iż wykorzystanie komputera można mierzyć z innego komputera podłączonego do Internetu.

15 Zadanie dla uczestników:

- opracowanie w grupach zasad kontroli rodzicielskiej,
- opracowanie sposobu korzystania z komputera (czas, pora korzystania, dni tygodnia, inne aktywności, rodzaje instalowanego oprogramowania i przeglądanych stron internetowych) dla:
  - dzieci w wieku przedszkolnym,
  - dzieci uczęszczających do szkoły podstawowej,
  - gimnazjalistów,
  - osób w wieku ponadgimnazjalnym,
  - dorosłych.

16 Całość rozważań jest podsumowana dyskusją, w jaki sposób osoby znaczące (rodzice, pedagodzy, pracownicy socjalni) mogą kreować bezpieczne środowisko dla młodszych w obszarze użytkowania nowych mediów. Poszczególne fragmenty szkolenia wzbogacane były o materiały multimedialne opracowane w ramach projektu SheepLive (http://pl.sheeplive.eu). Materiały zawierają kilkanaście kreskówek w różnych wersjach językowych służących jako wizualna pomoc, dająca możliwość omówienia różnorodnych e-zagrożeń. W ramach projektu opracowano następujące filmy, które są dostępne bezpłatnie w sieci: Bez kożuszka (publikacja nagich zdjęć i nagrań w Internecie), Nie tańcz z wilkami (wykorzystywanie fotografii i nagrań wideo w Internecie), Tajemniczy przyjaciel (grooming), Białe owce (dyskryminacja i rasizm w Internecie), Dziewięćdziesiąt dziewięć (łańcuszki szczęścia), Bekanie (Internet zawsze pamięta twoje błędy z przeszłości), Mała miss (anoreksja, internetowe przepisy na urodę), Zemsta (prześladowanie w Internecie – cyberstalking), Papla (wyłudzanie danych osobowych i informacji majątkowych – phishing), Karnawałowa maska (naśladowanie idoli w niebezpiecznych scenach), Tysiąc przyjaciół (wirtualne przyjaźnie), Maskarada (nigdy nie wiesz, kto jest po drugiej stronie), Ręce do góry (używanie wulgarnego języka i gestów), Druga strona (równość społeczna), Zagraniczni mobilni (szanuj prywatność swoich znajomych, etykieta w komunikacji telefonicznej), Sztuczne ognie (ryzyko związane z produkcją i stosowaniem materiałów wybuchowych), Gruby kark (cyberprzemoc), Komórkomania (uzależnienie od telefonów komórkowych, etykieta w komunikacji telefonicznej), Prezenty (zakupy online – kupuj tylko wtedy kiedy cię na to stać), Śnieżna gra (nagrywanie brutalnych i poniżających scen – happy slapping), Ubłocone głowy (uzależnienie od gier komputerowych).

17 **Projekt SheepLive**

Obrazek 4. Projekt SheepLive

Źródło: materiały FDN

Kolejne zadanie związane z bezpiecznym użytkowaniem mediów elektronicznych dotyczy pobrania i zainstalowania programu Beniamin, który jak zaznaczają autorzy aplikacji „jest programem zapewniającym bezpieczny dostęp do zasobów sieci Internet. Blokuje dostęp do stron, zgodnie z ustawieniami ustalonymi przez osobę nadzorującą komputer oraz ogranicza dostęp do wybranych funkcjonalności (np. komunikatory, listy dyskusyjne, ściąganie plików z sieci, poczta e-mail, zarządzanie dostępem do serwisów video i społecznościowych). System śledzi strony internetowe, które odwiedza użytkownik oraz jego działania w sieci, pod kątem dostępu do niepożądanych treści, na przykład stron o tematyce erotycznej. Program powstał pierwotnie z myślą o najmłodszych użytkownikach Internetu, jednak dzięki rozbudowanej konfiguracji może być również użyty w firmach i instytucjach do aktywnego kontrolowania dostępu do sieci”[4].

18 **Zarządzanie programem Beniamin**

Obrazek 5. Program Beniamin

Źródło: strona programu Beniamin

19 Sam program umożliwia blokadę różnych typów stron internetowych oraz dostępu do wybranych usług typu: e-mail, komunikatory. W panelu konfiguracyjnym dostępne są również opcje umożliwiające:

- wyświetlenie własnego komunikatu na zablokowanej stronie,
- wykonywanie zrzutów ekranowych w określonym przedziale czasowym (np. co minutę wraz z ich archiwizacją),
- przeglądanie ścisłego raportu odwiedzanych stron oraz uruchomionych aplikacji wraz z możliwością eksportu,
- wpisywanie adresów URL na tzw. „czarną listę”, dzięki czemu dane strony zostaną zablokowane w przeglądarce, pomimo że nie są umieszczone w bazie programu jako nieodpowiednie dla użytkowników,
- umieszczenie adresów URL na tzw. białej liście, przez co wybrane strony diagnozowane przez program jako destrukcyjne będą wyświetlane,
- ograniczanie dziennego limitu korzystania z Internetu oraz pór korzystania z sieci,
- tworzenie własnej definicji słów, które będą blokowane,
- blokadę opcji systemowych, takich jak: korzystanie z urządzeń przenośnych typu pendrive, uruchamianie panelu sterowania i innych.

20 Kontrola czasu korzystania z sieci w aplikacji Beniamin

Obrazek 6. Kontrola czasu korzystania z sieci

Źródło: strona programu Beniamin

21 Następnie prowadzący szkolenie poprosił uczestników o wymienienie kategorii gier komputerowych, jakie znają kursanci. Wszystkie wskazania zostały zapisane na flipcharcie. W dalszym etapie pedagodzy i pracownicy socjalni mieli za zadanie wypisać na swoich kartkach znane tytuły gier. Kolejnym krokiem było wypisanie rozrywkowych aplikacji w widocznym miejscu.

[4] *Beniamin – aktywna kontrola Internetu* http://www.beniamin.pl/index.php?option=com_content &view =article&id=175&Itemid=213, (dostęp: 20.02.2013).

Każdy z kursantów otrzymał zadanie sprawdzenia wymienionych tytułów w systemie PEGI (http://www.pegi.info/pl/). W trakcie analizy gier omówiono klasyfikację oraz etykiety odzwierciedlające zawartość gier komputerowych zgodnych z PEGI.

22 **System klasyfikacji PEGI**

23 Korzystając z możliwości, jakie oferuje metodyka szkoleń zgodna z systemem „blended learning", w ramach której jak podkreśla L. Eger należy dążyć do tego, aby kursanci nie tylko opanowali podstawowe zagadnienia, lecz również aby skutecznie zostali zmotywowani do dalszych działań w wymiarze praktycznym[5] zaprezentowano uczestnikom portal Fundacji Dzieci Niczyje (http://www.fdn.pl/kursy/). Każdy z kursantów otrzymał następujące zadania:

1. utworzyć własne konto jako użytkownik „Dorosły"
2. zalogować się do portalu;
3. uruchomić jeden z kursów;
4. zastanowić się nad wykorzystaniem niniejszej platformy we własnej pracy zawodowej.

24 Dalsze zadanie polegało na tym, że każdy z kursantów kolejno w ramach „giełdy pomysłów" podzielił się z innymi uczestnikami kursu możliwościami zastosowania poznanej platformy zdalnego nauczania w pracy z młodzieżą, tudzież z rodzicami uczniów i podopiecznych. Oceniono również estetykę wykonania strony internetowej, zawartość merytoryczną oraz łatwość obsługi interfejsu.

25 Platforma edukacyjna Dziecko w sieci

26 Całość działań praktycznych została uzupełniona o wyniki badań dotyczących psychospołecznego funkcjonowania dzieci i młodzieży w przestrzeni nowych mediów przy wykorzystaniu raportów:

- L. Kirwil i zespół, *Polskie dzieci w Internecie: Zagrożenia i bezpieczeństwo* – część 21 – Częściowy raport z badań EU Kids Online przeprowadzonych wśród dzieci w wieku 9–16 lat i ich rodziców,
- J. Czapiński, T. Panek (red.), *Diagnoza Społeczna*, Rada Monitoringu Społecznego, Warszawa,
- Instytut Kultury Miejskiej, *Dzieci sieci – kompetencje komunikacyjne najmłodszych*, Gdańsk,
- A. Wąsiński, Ł. Tomczyk – *Zjawisko netoholizmu w woj. śląskim*, Wyższa Szkoła Administracji w Bielsku-Białej,
- A. Garapich, *Popularność witryn wśród dzieci 7–14,* badania Gemius,
- Norton Online Family Reports.

27 Ostatnie z zagadnień poruszonych w trakcie kursu dotyczyło tematyki warezu. Uczestnicy mieli za zadanie dowiedzieć się przy wykorzystaniu sieci, czym jest warez.[6] Następnie prowa-

[5] L. Eger, *Technologie vzd lávání dosp lých*, Západo eská univerzita v Plzni, Plze 2005, s. 30

[6] Najczęściej użytkownicy analizując zagadnienie warezu korzystali ze strony „Wikipedii", gdzie ten typ działań definiuje się jako: „w żargonie komputerowym zbiorcze określenie rozmaitego rodzaju produktów komputerowych czy licencji. Określenie to dotyczy głównie płatnego zamkniętego oprogramowania i zmodyfikowanych wersji oprogramowania (shareware, adware), rozpowszechnianych nielegalnie, szczególnie po usunięciu zabezpieczeń przed kopiowaniem. Czasem stosuje się je także

dzący poprosił o zalogowanie się w wybranym serwisie oraz odszukanie płyt CD ulubionych artystów w formie cyfrowej oraz oprogramowania typu systemy operacyjne oraz pakiety biurowe. Po zakończeniu tychże czynności podjęto dyskusję nad prawnymi aspektami pobierania i udostępniania utworów objętych ochroną własności intelektualnej.

28 PODSUMOWANIE

Uczestnicy szkolenia uzyskali możliwość oceny prowadzącego poprzez wypełnienie anonimowej ankiety w bezpłatnym systemie www.ebadania.pl gdzie wzięte zostały pod uwagę następujące elementy szkolenia: jasność przekazywania informacji, użyteczność informacji, poziom merytoryczny, komunikatywność oraz propozycje nowych tematów związanych z zagrożeniami generowanymi przez cyfrową sieć.

29 W trakcie realizacji ćwiczeń zaproponowanych w szkoleniu wielokrotnie pojawiał się wniosek prowadzący do tego, że pośród wielu kwestii związanych z zagadnieniem użytkowania mediów elektronicznych, główny problem pedagogiczny dotykający przede wszystkim rodziców, jak i w dużym stopniu nauczycieli, oscyluje wokół pytania w jaki sposób osiągnąć równowagę pomiędzy naturalną chęcią zaspokajania potrzeb zabawowych wśród dzieci i młodzieży za pomocą Internetu a rozsądnym i bezpiecznym korzystaniem z niego? A. Olczak i R. Olczak proponują dwa typy rozwiązań:

1. techniczne – programowe metody ochrony dzieci przez zagrożeniami:
   a. filtry rodzinne umieszczone w serwisach internetowych,
   b. programy rodzicielskiej kontroli (Beniamin, Cenzor, Motyl).
2. pedagogiczne – głównie poprzez nawiązanie kontaktu z podopiecznym:
   a. dyskusja z dzieckiem na temat szkodliwych treści związanych z grami,
   b. stawianie granic zapisanych w umowie pomiędzy dzieckiem a dorosłym.

30 Najskuteczniejszym typem rozwiązań zarówno w domu jak i szkole jest zintegrowanie działań technicznych oraz pedagogicznych w celu zapewnienia dziecku jak największego komfortu w trakcie korzystania z sieci. Z racji cech rozwojowych, determinowanych wiekiem, nie wszystkie sposoby przeciwdziałania proponowane w powyższym podziale okażą się rozwiązaniami skutecznymi. Wypracowanie złotego środka, ze względu na szereg indywidualnych oraz środowiskowych czynników, z punktu psychopedagogicznego jest niestety działaniem skazanym na niepowodzenie. Wytworzenie nawyków prawidłowego korzystania z nowych mediów jest procesem wielostronnym, w którym powinni uczestniczyć świadomie rodzice, a także inne podmioty odpowiedzialne za wychowanie (babcie, dziadkowie, szkoła, rodzeństwo).

do innych materiałów dystrybuowanych z naruszeniem praw autorskich – takich jak muzyka, filmy czy e-booki. Jest to także nazwa sposobu udostępniania plików innym użytkownikom poprzez dzielenie ich na małe części (np. przy wykorzystaniu archiwizatora RAR lub ZIP) i umieszczanie na darmowych serwerach FTP/HTTP lub SMTP/POP3 (Peer2Mail)".

31 Pytania i zadania kontrolne

1. System PEGI:
   a. umożliwia szybkie sprawdzenie zawartych w grze treści,
   b. jest płatny,
   c. jest dostępny online,
   d. uwzględnia wszystkie gry.

2. Zainstalowane oprogramowanie w komputerze jest możliwe do sprawdzenia:
   a. w panelu sterowania,
   b. na pulpicie,
   c. w menu start,
   d. można korzystać z różnego rodzaju oprogramowania, również nie instalując go.

3. Dobrze zabezpieczony komputer wymaga oprogramowania typu:
   a. Firewall,
   b. program antywirusowy,
   c. pliki cookies,
   d. program demo.

4. Program kontroli rodzicielskiej typu Beniamin umożliwia:
   a. samoistne wyłączenie komputera o zaprogramowanej porze,
   b. blokowanie stron o charakterze erotycznym,
   c. udostępnianie możliwości korzystania z Internetu o określonej porze,
   d. blokowanie dostępu do serwisów społecznościowych.

5. Adres IP:
   a. służy identyfikowaniu osób w sieci Internet,
   b. jest niepowtarzalny,
   c. jest archiwizowany przez providerów internetowych,
   d. jest możliwy do maskowania poprzez technologię proxy.

6. Termin warez oznacza:
   a. nielegalne oprogramowanie,
   b. oprogramowane możliwe do zainstalowania w celach edukacyjnych,
   c. serwis internetowy udostępniający zazwyczaj adresy URL do plików z nielegalnym oprogramowaniem,
   d. jest to rodzaj gry online dostępnej bez rejestracji w serwisie internetowym.

BIBLIOGRAFIA:

Eger L., *Technologie vzdelávání dospelých*, Západoceská univerzita v Plzni, Plzen 2005.

Hojnacki L., *Pokolenie m-learningu – nowe wyzwanie dla szkoły*, „E-mentor", 1(13)/2006.

Olczak A., Olczak R., *Dziecko w Internecie – zagrożenia i ochrona*, http://www.ap.krakow.pl /ptn/ref2005/olczak.pdf, data dostępu: 20.02.2013.

Pyżalski J., *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Wyd. Impuls, Kraków 2012.

Tomczyk Ł., *Nowe media a funkcjonowanie dzieci i młodzieży w środowisku rodzinnym oraz rówieśniczym*, w: Stanek J., Zając W. (red.), *Współczesna rodzina. Dylematy teorii i praktyki pedagogicznej*, Wyd. WSP TWP, Warszawa 2011.

Tomczyk Ł., *Małoletni cyberhomo ludens – gry online jako podstawowa forma aktywności dzieci i młodzieży w Internecie*, w: Zieliński Z. (red.), *Rola informatyki w naukach ekonomicznych i społecznych. Innowacje i implikacje interdyscyplinarne*, Tom 2/2010, Wyższa Szkoła Handlowa, Kielce 2010.

Wąsiński A., Tomczyk Ł., *Aktywność młodzieży oraz rola rodziców w przestrzeni mediów sieciowych w perspektywie zagrożeń netoholizmem na przykładzie badań własnych*, w: Zieliński Z. (red.), *Rola informatyki w naukach ekonomicznych i społecznych. Innowacje i implikacje interdyscyplinarne*, t. 1, Wyższa Szkoła Handlowa, Kielce 2011.

PRZYKŁADY/PRZYPADKI

Anna Andrzejewska

1 **CYBERPRZEMOC**

Pierwsze doniesienia medialne dotyczące zjawiska przemocy rówieśniczej w sieci pojawiły się na początku lat 2000. Były to m.in. przypadek japońskiego ucznia nagranego w krępującej sytuacji w szatni szkolnej kamerą w telefonie komórkowym, sprawa zdjęcia amerykańskiej uczennicy, której fotografia przerobiona została na zdjęcie pornograficzne czy głośna historia filmu, w którym chłopiec z Kanady nieporadnie odgrywa scenę walki z filmu „Gwiezdne Wojny".

2 W Polsce głośno o problemie przemocy rówieśniczej z użyciem mediów elektronicznych zrobiło się wraz z historią gdańskiej gimnazjalistki, która popełniła samobójstwo w efekcie przemocy doznanej ze strony rówieśników. W historii ważną rolę odegrało nagranie aktu krzywdzenia dziewczyny kamerą w telefonie komórkowym.

3 Następnym przykładem cyberprzemocy było stworzenie przez 16-letniego gimnazjalistę z Opola witryny internetowej poświęconej w całości dręczeniu bezdomnego mieszkańca miasta. Strona zawierała m.in. filmy robione mu za pomocą telefonu komórkowego i agresywne wpisy.

4 Inny przykład to głośna sprawa uczniów gimnazjum w Czarnkowie, którzy założyli internetowe forum dyskusyjne, na którym drwili z kolegów, których nie darzyli sympatią.

5 Kolejnym przejawem cyberagresji była historia dwóch 15-letnich gimnazjalistów, którzy w Internecie zamieszczali wulgarne pogróżki pod adresem księdza z jednej z parafii w Tychach. Policja zlokalizowała szkolny komputer, na którym dokonywano wpisów, a ustalenie ich autorów nie było trudne. Przerażeni uczniowie tłumaczyli, że był to niewinny żart.

6 Poniżej przedstawiono fragment kolejnych wypowiedzi przypadkowych internautów na temat aktów przemocy w Internecie. Zilustrują one, jak cyberprzemoc jest postrzegana przez nich. Wypowiedzi są dosłowne z zachowaniem żargonu, ortografii, stylu.

Cyberprzemoc? – pierwsze słyszę...
Po raz pierwszy spotkałem się z tym terminem. Zacząłem chodzić po Internecie od 2 lat i pierwszy raz o tym słyszę. Nigdy jeszcze z takim czymś się nie spotkałem.
slawio14@vp.pl , 18.08.2007 13:34

Cyberprzemoc? – pierwsze słyszę...
Jeśli chcesz się z tym spotkać, zapraszam na czat: Dla 20 latków i zobaczysz jak jeden z czatowników znany jako bodzio, ale ma tych nicków mnóstwo. Często wchodzi jednocześnie pod kilkoma nickami i obraża innych, zwłaszcza kobiety. Praktycznie nie ma dnia by nie wpadał i nie bluzgał, robi screny z priv i pokazuje na ogólnym. Szykanuje te osoby by w końcu wycofały się z bywania w ty pokoju. Trwa to od dłuższego czasu bo czuje się bezkarny, jest przeświadczony, ze nikt mu nic nie zrobi i z tego co widać ma racje – ma się dobrze od dłuższego czasu, a ludzie odchodzą, czy tak powinno być? TO jest czatowy tyran , każdy go tu ma dość.
~dz.r , 19.08.2007 13:57

Trzeba być naprawdę wrażliwym żeby to kogoś ruszyło...
zatem gratuluję Ci szczęścia, bo ja to przeżyłam i najgorszemu wrogowi nie życzę... ku przestrodze uczciwych ludzi jak ktoś miał taki problem lub nadal ma chętnie poradzę co zrobić aby pozbyć się dręczyciela.
SUGAR_ona , 18.08.2007 14:53

Trzeba być naprawdę wrażliwym żeby to kogoś ruszyło...
reflektujesz na fajny seks?
~mario , 19.08.2007 19:49

atakowanie komputerów Nielegalne instalowanie na zaatakowanych komputerach oprogramowania do zbierania informacji osobistych, zainstalowanych programach, używanych hasłach. Takie działanie jest pod kara pozbawienia wolności włącznie. Strzeż się hackerze !~Prawo , 19.08.2007 16:41

Cyberprzemoc Przemoc to nie żadna przemoc tylko zabicie czasu gnębiąc jakiś ćwoków lub jakieś panienki.
P r z e m o c _ M a m _ W _ s o b i e , 19.08.2007 13:24

nękanie Na nękanie w necie trzeba sobie zasłużyć. Kto nie ma sobie nic do zarzucenia nie musi się obawiać niczego...prawda?
~anita7 , 19.08.2007 10:54

XP a co tutaj więcej trzeba klikać – kto ma słabą psyche to i w realu ma kłopoty, życie jest piękne ale krótkie i brutalne-niestety.
beata.sc@onet.eu,18.08.2007 3:49

przemoc w internecie kiedyś ktoś powiedział że słowem można zabić-czy ludzkość zrezygnowała z mówienia? To samo z Internetem gooniec@vp.pl , 18.08.2007 18:02

Przemoc wirtualna, konsekwencje w realu. Internet jest tylko środkiem. Znam przypadek gimnazjalistki z naszej miejscowości, która musiała zmienić szkołę z powodu cyberprzemocy. Sprawcy wcale nie są anonimowi, ale to Ona straciła szansę na normalne życie i „przyjaciół" (dziękuję za takich), którzy stanęli po stronie oprawców. Fajne społeczeństwo... Nie ma co... Nie wspominając o mniej drastycznych przypadkach, kiedy jakaś firma traciła swą pozycję, czy klientów z powodu internetowych plotek. Te rzeczy istniały, tylko środek się zmienił... stąd może większa skala rażenia.
~Elle , 17.08.2007 17:07

konwersacja Prawdą jest, że Internet uzależnia, i dużo czasu spędzamy przy nim czasu, ale ma wielkie plusy doskonała forma kontaktowania się z ludźmi na całym świecie. Właśnie poznałam mężczyznę przez Internet, cudownego faceta z Anglii. Lecę do niego za miesiąc.
pozdrawiam Marzena
majka75@op.pl , 18.08.2007 14:17

Brak anonimowości przed niczym nie chroni. Bo czym jest obecność w sieci? To zwykle IP kompa. W przeciętnej kawiarence czy z telefonu na kartę, można nadal się ukryć i psocić. To jest zawsze kwestia ludzkiej przyzwoitości i naszego stosunku do zła. To walka stara jak świat, tylko narzędzia się zmieniły..:)
kod2kat , 17.08.2007 16:32

7 UZALEŻNIENIE OD GIER

Maciek, lat 11. Uzależnienie chłopca zaczęło się, kiedy kolega pożyczył mu płytę z grą *xxxx*. Stało się to początkiem uzależnienia od komputera, a dokładnie od tej gry. Płyta ta trafiła do Maćka przypadkiem, a została w jego życiu do dzisiaj.

8 Fascynacja *xxxx* ogarnęła też młodszego brata. Zdarzało się, że grał w nią późną nocą, bo wtedy nikt mu nie przeszkadzał i mógł bez prze-

szkód zatracić się w wirtualnym świecie. Wielokrotnie na tym tle dochodziło do kłótni między rodzeństwem. Posiadając tylko jeden komputer, chłopcy nie mogli grać jednocześnie. Zwłaszcza że Maciek potrafi niezwykle długo grać w mecze. Świat gry komputerowej potrafił przenosić do rzeczywistości. Często rozmawiał z młodszym bratem o tym jak np. zakończył się mecz, jakiego kupił piłkarza, a jakiego sprzedał, jak rozwijała się jego kariera. Czasem gdy rodzice nie pozwalali mu grać, wpadał w złość i okropnie się denerwował. Zachowywał się jak zupełnie obcy człowiek. Poświęcał bardzo mało czasu na naukę, tracąc go na grę, co odbijało się na ocenach. Trudno było wyegzekwować od niego jakiekolwiek obowiązki. Często też spóźniał się na posiłki. Kiedy grał, nic nie widział poza grą i potrafił zrezygnować z wielu rzeczy. Najgorsze w tym jest chyba to, że nie widział swojego uzależnienia.

9 **Jakub lat 16.** Mieszka na wsi pod Warszawą. Ma starszą siostrę. Rodzice zawsze dbali o należytą opiekę nad dziećmi, a jednocześnie wymagali, aby wykonywały one sumiennie swoje obowiązki. Tak wyglądała sytuacja do momentu zmiany szkoły przez Jakuba i zakupu komputera. Chłopak wykorzystywał nowe urządzenie bardzo dobrze. Komputer zwiększył efektywność nauki i skrócił znacząco czas potrzebny na wykonanie niektórych zadań. Tak było do momentu, gdy odkrył gry komputerowe online, które początkowo traktował jak rozrywkę w czasie wolnym.

Z upływem czasu komputer i gry zaczęły wypełniać każdą wolną chwilę, coraz rzadziej spotykał się ze znajomymi. Stopniowo coraz więcej czasu poświęcał grom, a coraz mniej nauce. Opuścił się w nauce. Co prawda nie było trudności w zaliczaniu klas, ale z piątkowego/czwórkowego ucznia stał się nagle trójkowym/dwójkowym. Rodzice rozmawiali z chłopcem, podejrzewając, że za dużo czasu spędza przed ekranem komputera. Chłopak, broniąc się, stwierdził, że materiał w szkole jest coraz trudniejszy. Gdy został mu ograniczony dostęp do komputera, zaczął spędzać czas u znajomych, którzy mają komputer, albo w kawiarenkach internetowych. Zaczęły się nieobecności w szkole. Terapią szokową było powtarzanie czwartej klasy technikum.

10 **Łukasz, lat 17.** W dzień swoich 15 urodzin dostał od kolegi grę komputerową *YYYYYYY.* Jeszcze wtedy nikt nie zdawał sobie sprawy, że chwilowa radość może kiedyś przerodzić się w nieszczęście jego i jego najbliższych. Zaczęło się niewinnie. Otrzymany prezent należało przecież wypróbować. Najpierw była chęć poznania reguł i zasad, stworzenie własnego bohatera i w końcu rozpoczęcie gry, która spodobała się Łukaszowi już od pierwszej chwili. Stopniowo coraz więcej czasu spędzał przed komputerem, gra coraz bardziej go wciągała, przykuwając do komputera na wiele godzin. Zaczęło się liczyć tylko to, aby zrealizować postawione w grze zadania, przejść na kolejny poziom doświadczenia jednostki i odnaleźć jak najlepsze rzeczy do umundurowania dla swojego bohatera. Każdy zabity potwór i przejście do kolejnego miasta budziły radość i satysfakcję Łukasza, natomiast niepowodzenie – złość i rozpoczęcie po raz kolejny próby zabicia stwora.

Tracił przy tym poczucie czasu i do późnych godzin nocnych walczył o to, czego za pierwszym razem nie udało mu się zdobyć. Nie interesowały go już inne formy aktywności, każdą wolną chwilę spędzał przy komputerze. Czynności, które do tej pory sprawiały mu dużą frajdę, przestały go interesować. Nie wychodził już grać z kolegami w piłkę nożną, zrezygnował nawet z treningów ping-ponga, na które zostawał zawsze po piątkowych zajęciach wychowania fizycznego. Myślał tylko o tym, by jak najszybciej wrócić do

swojej ulubionej gry. Jak tylko wchodził do domu po szkole, rzucał plecak w kąt i siadał przed monitorem. Prace domowe schodziły na dalszy plan, często w ogóle nie były odrabiane. Nic i nikt nie był w stanie odciągnąć Łukasza od komputera. Zapominał nawet, że jest głodny. Posiłki znacznie ograniczał, jadł tylko podczas gry. Do kuchni przychodził nie po to, by zjeść wspólnie z rodzicami niedzielny obiad, ale by jak najszybciej zabrać swój talerz i udać się z nim do swojego pokoju, gdzie znajdował się komputer. Mówił, że musi dokończyć ważną pracę na zajęcia szkolne. Umiejętnie manipulował rodzicami. Potrafił wmówić im konieczność korzystania z komputera i znacznie zaniżyć rzeczywisty czas spędzany na grze.

Kiedy rodzice zorientowali się, że ich syn jest uzależniony od gry komputerowej, było już za późno na dyskusje, groźby czy pogadanki wychowawcze.

11 SEKSTING

Pierwszą powszechnie znaną „ofiarą" sekstingu była licealistka Jessie Logan. Nastolatka przesłała swoje nagie zdjęcie chłopakowi, który po rozstaniu z Jessie rozpowszechnił je. Dziewczyna zaczęła być prześladowana przez rówieśników (przezwiska, wypraszanie z imprez z okazji rozdania dyplomów). Nastolatka zdecydowała się nawet na wystąpienie w programie telewizyjnym, by przestrzec inne nastolatki przed rozsyłaniem swoich roznegliżowanych zdjęć. Niestety dziewczyna nie poradziła sobie z tą sytuacją i 3 lipca 2008 roku popełniła samobójstwo.

12 Monika, 21-letnia studentka na jednym z forów internetowych podzieliła się swoją historią z sekstingem.
„Wydawało mi się, że będę z Tomkiem do końca życia. Planowaliśmy wiele razy wspólną przyszłość, ustalaliśmy liczbę dzieci i nawet urządzaliśmy wirtualnie nasze mieszkanie. Byłam absolutnie i święcie przekonana, że spotkałam właśnie tego jednego, jedynego mężczyznę mojego życia. Raz po imprezie poszliśmy do łóżka i zgodziłam się, żeby Tomek nakręcił komórką filmik, kiedy mu robię... (intymne zbliżenie przyp. red.) Ot, niewinny wygłup, myślałam sobie. Kilka dni później nakryłam go w łóżku z moją przyjaciółką, historia jak z tzawego romansidła, klasyka gatunku. Niewiele myśląc wywaliłam go z mieszkania, które razem wynajmowaliśmy. Groził mi, bezczelny gnojek. Byłam twarda i nieustępliwa. Choć bardzo cierpiałam, wiedziałam dobrze, że nie wolno mi znów się z nim wiązać, bo skoro zdradził mnie raz, będzie mnie zdradzał w przyszłości. Obiecywał, że się zemści. Nie brałam jego słów na poważnie, bo co on takiego mógł mi zrobić, myślałam sobie? Okazało się, że może mi zrobić bardzo wiele złego. Zamieścił w sieci film. Ten film! Do tego imię, nazwisko, adres i numer telefonu! Kiedy to zobaczyłam, poczułam się tak, jakby właśnie skończyło się moje życie. Nie wiedziałam, co robić. Do kogo zwrócić się o pomoc? Bardzo się wstydziłam. Chyba nawet nie do końca potrafię opisać, co czułam. Mówić, że to upokorzenie, to mało, za mało. To było coś znacznie większego, straszniejszego. Przez kilka dni nie wychodziłam z domu. Nie miałam nawet siły wstać z łóżka. Bałam się iść do sklepu na dole, bo wyobrażałam sobie, że znajomy sprzedawca widział ten film. Jacyś napaleni zboczeńcy wysyłali mi na komórkę fotografie swoich penisów, bo myśleli, że jestem prostytutką... Przez jakiś czas poważnie rozważałam samobójstwo. Wreszcie odważyłam się i poprosiłam o pomoc mamę. Na szczęście mam do niej zaufanie. Umierałam ze wstydu, kiedy jej o tym mówiłam. Ale powiedziałam. Potrzebowałam pomocy. Inaczej bym chyba zwariowała. Od tamtej historii minął rok. Ciągle uciekam, zmieniam miejsca zamieszkania i ciągle wydaje mi się, że jestem rozpoznawana. Że nawet ludzie, którzy mijają mnie na ulicy dobrze wiedzą, kim jestem i co robię. Że

myślą, że jestem prostytutką. Nienawidzę mężczyzn. Nienawidzę siebie za to, że byłam tak głupia i naiwna. Nienawidzę Internetu. Tamten fatalny filmik wciąż krąży po sieci, ciągle na niego trafiam. Ciągle piszę do różnych adminów, żeby go usunęli, ale nie zawsze się udaje. Raz nawet znalazłam go na stronach placówki naukowej na Grenlandii, na serwerze na Bahamach... Nad tym się nie da zapanować. Film ma swoje życie, zupełnie niezależne ode mnie”[1].

13 Przypadek Moniki nie jest odosobniony. Takich historii ku przestrodze można znaleźć wiele i nie tylko w Internecie. Można być zarówno ofiarą sekstingu jak i celowym wykonawcą.

14 Poniższe przykłady dobitnie ilustrują, jak wielka niefrasobliwość ludzi może doprowadzić do nieprzewidywalnych przykrych konsekwencji:

15 „Marta jest studentką, podobnie jak jej chłopak. Woli nie podawać miasta, ani nazwy uczelni. Zgadza się na rozmowę tylko dlatego, żeby przestrzec wszystkich przed z pozoru tylko niewinnymi zabawami w wysyłanie rozbieranych zdjęć. Sama je sobie zrobiła i sama je wysłała. Lubi swoje ciało, jeździ konno i pływa. Z ówczesnym chłopakiem była od trzech lat. Kiedyś nakręcili film ze swoim udziałem – na pamiątkę, żeby zobaczyć jacy byli piękni, kiedy będą starzy. Nie pomyślała wtedy, że może nie będą starzeć się razem. Film jest na szczęście u Marty. Prawie rok temu wysłała chłopakowi swoje nagie zdjęcie, widać na nim tylko jej piersi i twarz. Podpisała: Na zawsze Twoje. I ten właśnie MMS trafił do wszystkich znajomych chłopaka Marty, w większości ich wspólnych znajomych” (www.efs.razem.pl).

„Załamaniem psychicznym swoją naiwność przypłaciła 16-latka z Oświęcimia. Dziewczyna na czacie nawiązała kontakt z 20-latkiem. Prowadzili miłą rozmowę, nastolatka zaufała mężczyźnie, o którym wiedziała tylko tyle, że mieszka w okolicach Krakowa. Kiedy wirtualny chłopak poprosił ją, żeby wykonała i przesłała mu kilka nagich zdjęć, zrobiła to bez zastanowienia. Mężczyzna niemal natychmiast umieścił je na jednym z seksualnych serwisów społecznościowych. Informacja o zdjęciach szybko dotarła do kolegów ze szkoły. Dziewczynka przeżyła szok. Przestraszyła się reakcji rodziców i wychowawców. Bała się, że zostanie skarcona za kontakty z dorosłym mężczyzną i skasowała wszystkie informacje, które mogły pomóc policji w ustaleniu sprawcy” (www.efs.razem.pl).

16

17 „Pewien 45-latek wyszukiwał swoje ofiary przez ogłoszenia w gazetach i Internecie. Interesowały go poszukujące pracy, potrzebujące pożyczki lub szukające kontaktu w celach matrymonialnych. Zgłaszał się do nich jako pracodawca, pożyczkodawca czy kandydat na męża. Potem prosił o przesłanie intymnych zdjęć, w konkretnych pozycjach. Gdy dostawał zdjęcia, dla kobiet zaczynał się horror. Groził, że skompromituje je, publikując zdjęcia. W zamian za bezpieczeństwo miały mu płacić. I niektóre regularnie płaciły. Inne wykorzystywał seksualnie (http://policyjni.gazeta.pl).

12 PRZYKŁADY STALKINGU

Julita otrzymywała SMS-y takiej treści: „Myślisz, że okręcisz mnie wokół palca i zostawisz? Grubo się mylisz! Postaram się, żebyś mnie bardzo mocno znienawidziła”. Julita jest kobietą, jakich tysiące. Była ofiarą natrętnego wielbiciela. Dostawała mnóstwo niechcianych wiadomości z wyznaniami miłości lub groźbami po tym, gdy postanowiła zakończyć związek.

[1] http://www.kafeteria.pl/przykawie/obiekt.php?id_t=1062, (data dostępu: 22.01.2012).

11 Inny przykład stalkingu: Marta i Krzysztof. Już po rozstaniu Marta otrzymywała SMS-y takiej treści: „Zdrady nigdy ci nie wybaczę ani nie zapomnę. Wiem już, z kim się spotykasz. Ale ciebie to będzie bardziej boleć niż mnie" albo takie: „Taka jak ty zdarza się raz na milion, dlatego nie umiem przestać cię kochać i nigdy nie odpuszczam. Nawet jakbym poszedł siedzieć, to i tak wyjdę i będzie tak samo. Ja nigdy nie rezygnuję i nie wybaczam" – odgrażał się. Następnie żądał spotkania, wspólnego spędzania czasu. Szantażował, że opublikuje w Internecie jej nagie zdjęcia lub roześle je znajomym. Wszystko to zrobi, jeśli kobieta nie będzie się z nim dalej spotykać.

11 „Jadę po ciebie z kosą i oszpecę ci buźkę. Będę to robił najdłużej, jak się da, żebyś krzyczała, żebyś czuła tragiczny ból. A na koniec obsypię ci te rany solą" – pisał do innej ofiary stalkingu natrętny adorator. 21-letni Adrian Z., który nie mógł się pogodzić, że rówieśniczka go rzuciła. Poznali się w 2009 r. Dziewczyna stwierdziła, że ten związek nie ma przyszłości. Innego zdania był Adrian. Gdy ta odmawiała spotkania, w wymyślnych groźbach straszył swoją sympatię okaleczeniem. „Wiem, gdzie pracujesz. Wiem, gdzie mieszkasz. Nie bądź zdziwiona, jak ktoś cię odwiedzi. Jestem chłopak bez serca i nie mam litości. Suk…, już jesteś skończona" – groził Julicie. Zakazał jej też kontaktu z policją. Dziewczyna nie wytrzymała jednak presji i pod namową koleżanki zgłosiła się na komisariat.

Zdarzenia, których dotyczy proces, miały miejsce na początku stycznia 2010 roku[2].

[2] Źródło: http://przemocwsieci.cba.pl/ (data dostępu: 12. 08.2010).

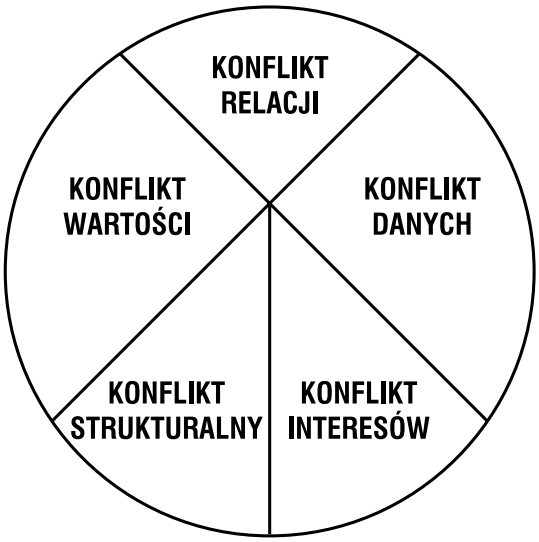
ROZWIĄZYWANIE
KONFLIKTÓW, MEDIACJE I NEGOCJACJE

Joanna Lizut

1 WPROWADZENIE

Celem tej części opracowania jest dostarczenie wiedzy na temat pracy w sytuacji konfliktu i wskazanie technik mediacji i negocjacji z uwzględnieniem specyfiki i trudności tego typu pracy. Dodatkowo zaproponowane w części praktycznej przykłady ćwiczeń i tematów do dyskusji pozwolą uczestnikom szkoleń wzmocnić swoje kompetencje w zakresie rozwiązywania konfliktów, nauczyć się radzenia sobie w trudnych sytuacjach i osiągnąć lepszą współpracę z klientem.

Schemat 1. **Podstawowe typy konfliktów wg Ch.Moore'a**



Źródło: Ch. Moore, cyt. za: A. Cybulko, *Konflikt*, w: E. Gmurzyńska, R. Morka (red.), *Mediacje, Teoria i praktyka*, Oficyna Wolters Kluwer Business, Warszawa 2009, s. 57.

2 **Do podstawowych rodzajów konfliktów zaliczamy**[1]:

3 **konflikt danych** – występuje wówczas, kiedy strony konfliktu nie dysponują potrzebnymi danymi, mają różne, błędne, niepełne informacje lub odmiennie je interpretują. Może to prowadzić do narastania negatywnych nastawień, przede wszystkim ze względu na trudności w komunikacji i brak zaufania. Zwłaszcza w sytuacji, gdy strony oskarżają się o zatajenie danych, celowe wprowadzanie w błąd, konflikt może ulec eskalacji;

4 **konflikt relacji** – związany jest z silnymi, trudnymi emocjami przeżywanymi w relacji z drugą osobą. Może pojawiać się wówczas, gdy nie ma obiektywnych powodów do konfliktu, ale relacje opierają się na stereotypowym postrzeganiu strony przeciwnej;

5 **konflikt wartości** – ma swoje źródło w odmiennych systemach wartości, różnych światopoglądach czy uznawanych systemach zasad. Jest tym silniejszy, iż bardziej sztywne są opinie stron, które nie dopuszczają odmienności przekonań, co skutecznie blokuje współpracę;

6 **konflikt strukturalny** – przyczyną tego typu konfliktów są rozmaite czynniki zewnętrzne. Spór np. wynika z faktu ograniczonych zasobów, wadliwej struktury organizacji, błędnie pełnionych ról, ograniczeń czasowych. Zrozumienie,

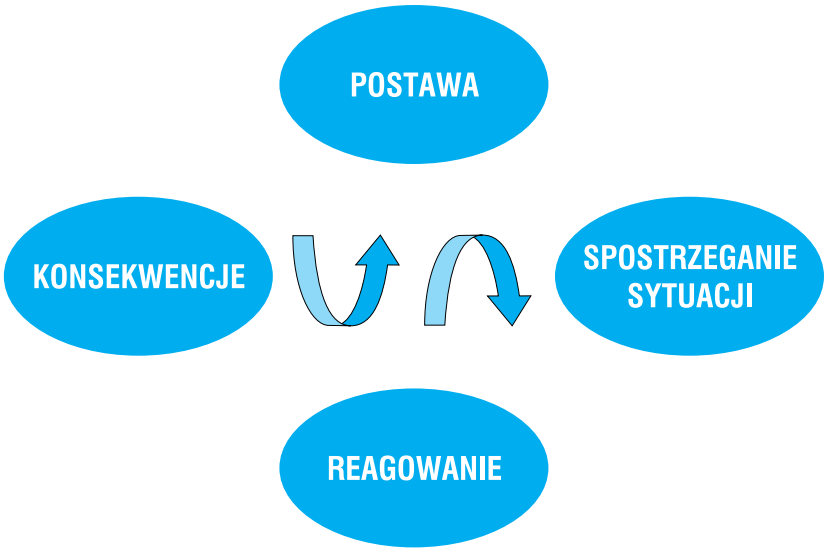
[1] A. Cybulko, *Konflikt*, w: E. Gmurzyńska, R. Morka (red.), *Mediacje, Teoria i praktyka*, Oficyna Wolters Kluwer Business, Warszawa 2009, s. 57–58.

że źródła konfliktu tkwią poza jednostkami, może doprowadzić do wspólnego poszukiwania konstruktywnego rozwiązania;

7 **konflikt interesów** – jest związany z niemożnością realizacji potrzeb czy osiągnięcia celów. Wywołany jest współzawodnictwem stron o dobra i możliwość zaspokojenie potrzeb.

8 Trudności w rozwiązywaniu konfliktów mają swoje źródła w fakcie „tkwienia" w cyklu konfliktu, co powoduje jego eskalacje. Jedynie przerwanie cyklu może doprowadzić do konstruktywnego/efektywnego rozwiązania konfliktu.

CYKL KONFLIKTU:
Schemat 2. Cykl konfliktu



Źródło: Polskie Centrum Mediacji, http://pcm.szczecin.eu.interia.pl/konflikt.html data dostępu: 25.02.2013.

9 **Elementy cyklu konfliktu:**

Postawy – stałe, pozytywne lub negatywne oceny świata, siebie, innych ludzi, obiektów lub pojęć powstałe w toku doświadczeń, dzięki którym łatwiej jest ustosunkować się do otaczającej rzeczywistości i reagować na nią. Postawy moją też swoje odniesienie do sytuacji konfliktu. Postawy powodują pewne wyuczone zindywidualizowane sposoby postrzegania sytuacji trudnych;

10 **Spostrzeganie** – opiera się na konkretnych, przypisanych jednostce postawach i powoduje, że obserwując jakieś sytuacje zauważamy wybiórczo tylko te elementy, które „pasują" do naszych postaw. Jeśli pewne elementy sytuacji nie są zgodne z naszymi nastawieniami – modyfikujemy je w taki sposób, aby pasowały do „schematów", które posiadamy.

11 To, w jaki sposób spostrzegamy spór, niesie za sobą określone konsekwencje w naszych zachowaniach;

12 **zachowania/reagowanie** – indywidualne spostrzeganie sytuacji konfliktowej powoduje, że w stosunku do ludzi biorących w niej udział zachowujemy się w określony sposób, tzn. reagujemy na spór;

13 **konsekwencje** – kontrreakcja drugiej strony.

14 Konflikt można przerwać na każdym z tych etapów, choć to właśnie postawy w zasadniczy sposób wpływają na jego przebieg. Doświadczenia uczestników sporu determinują przebieg cyklu, tak go kształtując, że w praktyce utrwalają prezentowane pierwotne postawy. Osoba unikająca, czująca się skrzywdzona wynikiem poprzedniego sporu,

w kolejnym konflikcie będzie tak kierowała swoją relacją z drugą stroną, iż prawdopodobnie wzmocni pierwotne przekonania o destruktywnej naturze konfliktu.

12 Oprócz powtarzalnych elementów tworzących określony cykl, każdy konflikt ma też swoją dynamikę. W sytuacjach gdy występują trudności z usunięciem różnic między stronami, dochodzi do **eskalacji (nasilenia) konfliktu**. Objawia się to poprzez[2]:

- przechodzenie do coraz bardziej destrukcyjnych form walki,
- rozszerzanie zakresu konfliktu – przechodzenie do innych form konfliktu, włączanie kolejnych kwestii spornych,
- angażowanie coraz większych zasobów – czasu, pieniędzy,
- wciąganie kolejnych uczestników do konfliktu.

13 Do mechanizmów sprzyjających, przyczyniających się do eskalacji konfliktu zaliczamy:

1. **dysonans poznawczy** – chęć utrzymania równowagi pomiędzy przekonaniami a zachowaniami, zarówno własnymi jak i innych osób. Im bardziej chcemy przekonać oponenta, tym bardziej intensyfikujemy swoje zachowania, które mają do tego doprowadzić. Opór drugiej strony wywołuje negatywne emocje, które chcemy zniwelować, co paradoksalnie prowadzi do dalszego nasilenia nacisków i eskalacji konfliktu;
2. **pułapka zaangażowania** – im bardziej w coś się angażujemy, poświęcając swoją energię, czas czy pieniądze, tym trudniej jest nam zrezygnować. Stąd, im dłużej i bardziej intensywnie funkcjonujemy w sytuacji konfliktu, tym ciężej jest zaprzestać sporu, nawet wówczas, gdy nie przynosi on żadnych korzyści,
3. **dbałość o zachowanie twarzy** – większość osób cechuje niechęć do przyznania się do błędu;
4. **społeczna norma wzajemności** – opierająca się na zasadzie: „oko za oko, ząb za ząb", nakazująca odpłacać za wyrządzone krzywdy. Według tej reguły jesteśmy skłonni odwzajemniać się tym samym, co nas dotyka;
5. **złość** – odczuwane negatywne emocje prowadzą do wykrzywienia obrazu świata i zniekształcenia oceny zachowań, jak i samej osoby oponenta;
6. **zniekształcenie percepcji** – powiązane z poprzednią kategorią, prowadzi do przypisywania winy za konflikt przeciwnikowi i jego cechom, a nie np. czynnikom sytuacyjnym itp.

14 Wyróżnia się cztery podstawowe sposoby zachowania w sytuacji konfliktu, przyjmując za kryterium podziału stosunek do własnych interesów i interesów drugiej strony:

1. **wycofanie** – dla tej postawy charakterystyczna jest niska dbałość o interes własny i drugiej strony,
2. **uleganie** – przeważa interes drugiej strony nad interesem własnym,
3. **rywalizacja** – przedkładanie interesów własnych nad stosunkami z drugą stroną,
4. **współpraca** – poszukiwanie rozwiązania satysfakcjonującego obie strony i pozwalającego zaspokoić interesy obu stron[3].

15 **Wycofanie** – nie przynosi korzyści żadnej ze stron. Najczęściej występuje wówczas, gdy stronom nie zależy na rozwiązaniu sporu.

[2] J. Reykowski, *Konflikty polityczne,* w: K. Skarżyńska (red.), *Psychologia polityczna*, Poznań 1999, s. 179–181.

[3] A. Cybulko, *Konflikt*, w: E. Gmurzyńska, R. Morka (red.), *Mediacje, Teoria i praktyka*, Oficyna Wolters Kluwer Business, Warszawa 2009, s. 61–62.

Zachowania świadczące o wycofaniu:

ignorowanie – ostentacyjne niedostrzeganie konfliktu i przenoszenie uwagi drugiej strony na kwestie drugorzędne, poboczne;

odwlekanie – odraczanie poszukiwania rozwiązania w bliżej nieokreśloną przyszłość;

pokojowe współistnienie – pozorowanie współpracy, udawanie, że konflikt nie istnieje;

deprecjonowanie – odbieranie znaczenia drugiej stronie, pomniejszanie jej wartości, które ma na celu uniknięcie konfrontacji z powodu rzekomego braku partnera (partner niegodny);

reorientacja – poszukiwanie problemu zastępczego w miejsce faktycznego konfliktu;

separacja – całkowite uniknięcie podjęcia się poszukiwania rozwiązania sporu poprzez wyeliminowanie jednej ze stron.

Uleganie – rezygnacja z możliwości realizacji własnych interesów przez jedną ze stron sporu. Wybór takiej strategii jest charakterystyczny dla osób, które ponad osiągnięcie swoich interesów przekładają np. dobre stosunki z drugą stroną. Może jednak również występować wówczas, gdy strony charakteryzuje duża dysproporcja w zakresie wiedzy, kompetencji i umiejętności. Wówczas strona słabsza nie może się skutecznie przeciwstawić oponentowi.

Rywalizacja – strategia, której wybór jest charakterystyczny dla osób nastawionych na konfrontację i dążących do zrealizowania własnych celów. Wygrana jest istotniejsza niż dobre stosunki z drugą stroną.

Współpraca – interes własny i drugiej strony są równie ważne. Podobnie jak dobre relacje z oponentem. Strony sporu są gotowe zrezygnować z części swoich roszczeń, przede wszystkim pracując nad porozumieniem, które będzie satysfakcjonujące dla obu stron. Znalezienie wspólnego rozwiązania wymaga wysokich kompetencji komunikacyjnych i skłonności do kooperacji.

17 **DZIAŁANIA W SYTUACJI KONFLIKTU, KONSTRUKTYWNE POROZUMIEWANIE SIĘ:**

Konflikt jest szczególną sytuacją, która wymaga od jego uczestników szczególnego zaangażowania w proces komunikowania, który oznacza wymianę, łączność, rozmowę, porozumiewanie się, przekazywanie myśli, emocji między nadawcą i odbiorcą. Proces ten odbywa się na różnych poziomach oraz wywołuje określone skutki.

18 W trakcie tego procesu jego uczestnicy wywierają określony wpływ na drugą stronę. Znajomość reguł w tym zakresie pozwala na efektywniejsze osiąganie założonych celów i skuteczne negocjowanie stanowisk.

19 **Do najważniejszych reguł wywierania wpływu społecznego zalicza się**[4]:

regułę wzajemności – dążenie do rewanżowania się osobom, które wyświadczyły nam jakąś przysługę, ofiarowały prezent określonej wartości;

regułę kontrastu – polega ona na zmianie odbioru bodźców zależnie od kontekstu, w jakim są przedstawiane (na jakim tle są przedstawiane);

[4] K. Bargiel-Matusiewicz, *Negocjacje i mediacje*, Polskie Wydawnictwo Ekonomiczne, 2010, s. 25–37.

regułę ograniczonej dostępności – opiera się na tendencji do przypisywania większej wartości obiektom trudno osiągalnym, których liczba jest ograniczona;
regułę sympatii – znacznie łatwiej jest coś uzyskać, jeśli wzbudziło się sympatię u drugiej strony;
regułę dowodu społecznego – jesteśmy skłonni podejmować takie decyzje, które są zgodne ze zdaniem większości.
regułę autorytetu – odbiorcy komunikatu chętniej poddają się wpływowi osób czy instytucji, które w danych kręgach kulturowych, społecznych czy zawodowych uchodzą za autorytet i cieszą się wysokim prestiżem;
regułę zaangażowania/konsekwencji – powszechne wśród ludzi jest trzymanie się wcześniej podjętych decyzji.

20 MEDIACJE

Mediacja – pomoc neutralnej osoby trzeciej w dojściu do porozumienia między stronami konfliktu.

21 SPORY A NOWE TECHNOLOGIE

Online dispute resolution (ODR) – można rozumieć na dwa sposoby. Pojęcie to dotyczy rozstrzygania sporów wynikających z postępowania mającego miejsce w Internecie, np. spory e-commerce, jak i odnosi się do korzystania z internetowych technologii komunikacyjnych w samym procesie rozwiązywania sporu, nawet jeśli nie jest on związany z działaniami prowadzonymi w Internecie[5].

22 NEGOCJACJE

Negocjacje – rozwiązywanie konfliktu zaistniałego pomiędzy dwoma lub większą liczbą partnerów, podczas którego przeciwne strony modyfikują swoje potrzeby, aby dojść do możliwego do zaakceptowania porozumienia[6].

Wyróżnia się wiele stylów negocjacji, poniżej propozycja A. Olech wraz z zaleceniami dla negocjujących.

Zarówno w negocjajcjach jak i medjacjach zasadnicze znaczenie odgrywają umiejętności związane z umiejętnością otwartości i słuchaniu drugiej strony czyli tzw. aktywne słuchanie.

23 Korzyści płynące z aktywnego słuchania:

1. pozwala wytworzyć poczucie wzajemnego zaufania i przekonanie, iż jesteśmy akceptowani mimo różnicy zdań;
2. zachęca do większej otwartości, zwierzenia się ze wszystkich problemów, co być może uświadomi naszemu rozmówcy, gdzie tkwi źródło jego trudności;
3. pomaga rozmówcy na dokładne zanalizowanie i organizację swojej wypowiedzi, co zwiększa jego szanse na samodzielne rozwiązanie problemu;
4. umożliwia swobodne wypowiedzenie się na dany temat, „wyrzucenie" z siebie danego problemu, co zmniejsza napięcie psychiczne;
5. pozwala na konfrontację własnych wyobrażeń i ocen z opiniami drugiej osoby oraz ich korektę;
6. pozwala na uzyskanie informacji zwrotnych;
7. daje możliwość prześledzenia toku rozumowania drugiej strony, odmiennego sposobu myślenia i wnioskowania.

24 Zasady aktywnego słuchania:

1. akceptacja rozmówcy, przejawianie zainteresowania opiniami drugiej strony;
2. tolerancja dla emocji i zachowań drugiej strony;
3. okazywanie szacunku drugiej stronie;

[5] K. Mania, *Online Dispute Resolution – podstawowe zagadnienia*, http://arbitraz.laszczuk.pl/_adr/117/ODR_Online_Dispute_Resolution_-_podstawowe_zagadnienia.pdf, data dostępu: 20.02.2013.

[6] K. Bargiel-Matusiewicz, *Negocjacje i mediacje*, Polskie Wydawnictwo Ekonomiczne, 2010, s. 65.

4. utrzymywanie kontaktu wzrokowego, zachęcanie do rozmowy;
5. zadawanie dodatkowych pytań dotyczących tego, co mówi druga osoba;
6. powstrzymanie się od komentowania, udzielania rad;
7. cierpliwość, nieprzerywanie rozmówcy jego wypowiedzi.

25 PODSUMOWANIE

Znaczenie i zasady poprawnej komunikacji znajdują swoje zastosowanie także w wirtualnej przestrzeni. Niewątpliwie w sytuacji braku bezpośredniej styczności i anonimowości łatwiej eskalować konflikt. Niemniej wykorzystanie tej nowej przestrzeni dla kontaktów społecznych stwarza także możliwość do owocnej współpracy i na tych szansach warto się skupić.

Tabela 1: Style negocjacji

Negocjacje pozycyjne		**Negocjacje oparte na zasadach (problemowe)**
miękkie	**twarde**	
Uczestnicy są przyjaciółmi	Uczestnicy są przeciwnikami	Uczestnicy rozwiązują wspólny problem
Celem jest ugoda	Celem jest zwycięstwo	Celem jest rozsądny wynik uzyskany sprawnie i w dobrej atmosferze
Ustępuj dla podtrzymania kontaktów	Żądaj ustępstw jako warunku podtrzymania kontaktów	Oddzielaj ludzi od problemu
Traktuj problem i ludzi delikatnie	Bądź twardy wobec ludzi i problemu	Bądź delikatny wobec ludzi i twardy wobec problemu
Ufaj innym	Nie ufaj innym	Działaj niezależnie od zaufania
Łatwo zmieniaj stanowisko	Okop się na swoim stanowisku	Koncentruj się na zadaniu, a nie na stanowiskach
Składaj oferty	Stosuj groźby	Badaj stan interesów
Ujawnij dolną granicę tego, co możesz zaaprobować	Ukrywaj dolną granicę akceptacji	Unikaj formułowania dolnej granicy
Akceptuj jednostronne straty dla dobra porozumienia	Żądaj jednostronnych korzyści jako warunków prowadzenia rozmów	Opracuj możliwości korzystne dla obu stron
Szukaj jednego rozwiązania, akceptowanego przez drugą stronę	Forsuj jedno rozwiązanie, korzystne dla Ciebie	Szukaj wielu możliwości, wybierzesz jedną później
Nalegaj na zawarcie ugody	Nalegaj na przyjęcie twojego stanowiska	Nalegaj na przyjęcie obiektywnych kryteriów
Staraj się unikać walki woli	Staraj się wygrać walkę woli	Staraj się osiągnąć rezultaty oparte na obiektywnych kryteriach, niezależnych od subiektywnych życzeń
Poddawaj się presji	Wywieraj presję	Uzasadnij i bądź otwarty na uzasadnienia; ulegaj argumentom a nie presji

Źródło: A. Olech, *Praca w zespole-zespołowe rozwiązywanie problemów i konfliktów*,(w:) M. Bąkiewicz, M. Grewiński (red.), *Praca socjalna w środowisku lokalnym,* WSP TWP, Warszawa 2009, s. 60–61

ĆWICZENIA 45
ĆWICZENIA 46
ĆWICZENIA 47
ĆWICZENIA 48

BIBLIOGRAFIA:

Bargiel-Matusiewicz K., *Negocjacje i mediacje*, Polskie Wydawnictwo Ekonomiczne, 2010.

Bieńkowska E., *Poradnik mediatora*, Wydawnictwo Zrzeszenia Prawników Polskich, Warszawa 1999.

Gmurzyńska E., Morka R. (red.), *Mediacje, Teoria i praktyka*, Oficyna Wolters Kluwer Business, Warszawa 2009.

Gójska A., *Mediacja w rozwiązywaniu konfliktów rodzinnych*, Wydawnictwo C. H. Beck, Warszawa 2007.

Haeske U., *Konflikty w życiu zawodowym: mediacja i trening w rozwiązywaniu problemów*, Jedność, Kielce 2005.

Mania K., *Online Dispute Resolution – podstawowe zagadnienia*, http://arbitraz.laszczuk.pl/_adr/117/ODR__Online_Dispute_Resolution_-_podstawowe_zagadnienia.pdf data dostępu: 20.02.2013.

Nordhelle G., *Mediacja, Sztuka rozwiązywania konfliktów*, FISO.

Olech A., *Praca w zespole – zespołowe rozwiązywanie problemów i konfliktów*, w: Bąkiewicz M., Grewiński M. (red.), *Praca socjalna w środowisku lokalnym*, WSP TWP, Warszawa 2009.

Reykowski J., *Konflikty polityczne*, w: Skarżyńska K. (red.), *Psychologia polityczna*, Poznań 1999.

ĆWICZENIA

Marcin Bochenek, Piotr Bisialski,
Joanna Lizut, Martyna Różycka,
Anna Rywczyńska, Krzysztof Silicki,
Agnieszka Wrońska

ĆWICZENIA WPROWADZAJĄCE I INTEGRUJĄCE

Ćwiczenia mające zastosowanie do wszystkich modułów tematycznych, służące integracji grupy i wprowadzeniu zagadnień teoretycznych

ZAGROŻENIA ZDROWIA PSYCHICZNEGO I FIZYCZNEGO

Dolegliwości wzroku

Zespół RSI

Dolegliwości układu kostno-szkieletowego

Zespół uzależnienia od Internetu

Cyfrowa demencja

Cyberprzemoc

Samobójstwa

ZAGROŻENIA SPOŁECZNO-WYCHOWAWCZE

Pedofilia w sieci

Pornografia

Seksting

Sekty

Stalking

ZAGROŻENIA ZWIĄZANE Z UZALEŻNIENIAMI

Internet jako źródło informacji o substancjach psychoaktywnych

Uzależnienie od gier komputerowych

Infoholizm

CYBERPRZESTĘPCZOŚĆ I NADUŻYCIA

Portfel

Bezpieczne zakupy przez Internet

Rozumienie szyfrowania

Zjawisko phishingu

Bankowość elektroniczna

ĆWICZENIA WPROWADZAJĄCE

1 Odrywana wizytówka

Cel: poznanie uczestników spotkania.

Przebieg:

- Rozdaj uczestnikom kartki A4 (przecięte wzdłuż) i poproś o złożenie w harmonijkę, tak by powstało pięć równych części. Na każdej części powinno znaleźć się imię (ew. imię i nazwisko). Kartka harmonijka przyczepiona jest do ubrania za pomocą taśmy.
- Zadaniem uczestnika jest wybranie dowolnego rozmówcy oraz rozmowa na temat podany przez prowadzącego. Zakończeniem ćwiczenia jest wymiana wizytówek z ewentualnym uzupełnieniem o dane kontaktowe np. e-maili lub numerów telefonu (nie jest to obligatoryjne) i wybranie kolejnego rozmówcy.
- Tematy rozmów proponowane przez prowadzącego zmieniają się i mogą dotyczyć następującej tematyki: moja ulubiona potrawa, miejsce gdzie lubię spędzać czas wolny, hobby, zwierzęta w moim życiu.

2 Krzyżówka imion

Cel: poznanie imion uczestników spotkania.

Przebieg:

- Rozdaj uczestnikom kartki A4
- Pierwsze zadanie polega na napisaniu na arkuszu wyrazu, który kojarzony jest z Internetem (np. sieć, plik, Internet). Następnie uczestnicy po kolei wypisują swoje imiona, tak aby utworzyły krzyżówkę. Należy dopisać swoje imię, wykorzystując dowolną już napisaną literę (zarówno pionowo jak i poziomo).

3 Rysowana historia

Cel: poznanie uczestników spotkania, wprowadzenie w tematykę zajęć.

Przebieg:

Rozdaj uczestnikom kartkę A4. Poproś, by podzielili ją na cztery równe części.

Zadaniem uczestników jest przedstawienie na każdej części proponowanych przez prowadzącego informacji. Formą wypowiedzi są rysunki, symbole, znaki etc. bez używania pisma.

a	b
c	d

- Następnie uczestnicy w parach rozmawiają i opowiadają sobie wzajemnie o tym, co przedstawili na kartce. Modyfikacją może być próba odgadnięcia symboliki rysunku przez partnera rozmowy lub/i po wysłuchaniu informacji przekazaniu jej innej osobie z grupy.

Propozycje tematów do zilustrowania:

a. ulubione strony www/często przeglądane strony
b. cyberzagrożenia najbardziej groźne (moim zdaniem)
c. hobby offline
d. to, co zwykle mam na biurku z komputerem

4 Cebula

Cel: poznanie uczestników spotkania, wprowadzenie w tematykę zajęć.

Przebieg:

- Poproś uczestników, by ustawili się parami, twarzami do siebie, tworząc dwa koła: wewnętrzne i zewnętrzne.
- Prowadzący wydaje polecenia/tematy rozmów (propozycje poniżej).
- Po każdym wykonanym zadaniu prowadzący zmienia rozmówców poprzez przesuwanie koła wewnętrznego lub zewnętnznego o x osób, np. proszę, by osoby w kole zewnętrznym przesunęły się w lewą stronę o 5 osób lub osoby w kole wewnętrznym przesuną się w prawo o 3 osoby.
- Z nowym rozmówcą rozpoczynamy zadanie od powitania i przedstawienia się.

Propozycje zadań/tematów rozmów mogą dotyczyć podobnych zagadnień, jak w poprzednich ćwiczeniach lub być ściśle związane z tematyką zajęć, np.:

- Z jakimi cyberzagrożeniami spotykasz się najczęściej w swojej pracy zawodowej?
- Jak zareagujesz, gdy zobaczysz swoje zdjęcie, informację o sobie w Internecie w miejscach, w których ich nie zamieszczałeś/-łaś?
- Który program/rodzaj zajęć profilaktycznych jest Twoim zdaniem warty polecenia?

Tematy/zadania mogą mieć również charakter rozluźniający, relaksacyjny lub/i prowadzić do rozładowania napięć, stworzenia miłej atmosfery np. opowiedz rozmówcy wesołą historię, osoby w kole środkowym zamykają na chwilę oczy, podczas gdy partnerzy zmieniają 3 szczegóły swojego wyglądu.

5 Przypadkowe słowo

Cel: rozpoznawanie problemów i zjawisk dot. cyberzagrożeń, utrwalanie wiedzy, podsumowania.

Przebieg:

Propozycje tematów mogą dotyczyć szerokiego obszaru zagrożeń cyberprzestrzeni, zarówno tematów ogólnych jak i pytań szczegółowych obejmujących zagadnienia zagrożenia zdrowia psychicznego i fizycznego, zagrożenia społeczno-wychowawcze, zagrożenia związane z uzależnieniami, cyberprzestępstw oraz ochrony dzieci.

- Zapisz w widocznym miejscu problem, nad którym będzie pracować grupa.
- Przygotuj słownik/encyklopedię/ leksykon, dowolny tekst pisany lub kartki z przygotowanymi wyrazami. Nie powinny to być specjalnie dobrane wyrazy tzw. pasujące do tematu, ale wyrazy (najlepiej rzeczowniki), które prowokują wiele skojarzeń.
- Każdy uczestnik losuje wyraz oraz buduje skojarzenia dotyczące problemu, które wywołał wylosowany wyraz, analizuje, jakie pomysły, idee lub kierunki myślenia sugeruje.
- Można zapisać konkretne pomysły, rozwiązania powstałe pod wpływem skojarzeń z wyrazem przypadkowym i przedyskutować je w grupach i na forum.

1 1,2 … 4

Cel: utrwalenie umiejętności rozpoznawania symptomów zagrożeń zdrowia fizycznego.

Przebieg:

- Rozdaj uczestnikom kartki wg poniższego wzoru i poproś o uzupełnienie zgodnie z podanymi poleceniami.
- Poproś uczestników o dobranie się w pary, omówienie indywidualnie przygotowanych propozycji oraz wypracowanie wspólnej wersji.
- Połącz pary w zespoły czteroosobowe. Zadaniem zespołów jest przygotowanie propozycji dobrych praktyk oraz przedstawienie innym grupom.

Rodzaje / grupy zagrożeń zdrowia fizycznego	Syndromy występowania dolegliwości wzroku CVS (Computer Vision Syndrome)	Propozycje ćwiczeń

2 3

Diagram czy mapa

Cel: utrwalanie wiedzy, trening kreatywności.

Przebieg:

- Poproś uczestników o przedstawienie w dowolnej formie graficznej np. mapa myśli, schematy, diagramy) obszaru cyberzagrożeń zdrowia fizycznego.

4

Nadmierne korzystanie z Internetu

Cel: identyfikowanie pierwszych objawów nadmiernego korzystania z sieci.

Przebieg:

- Podziel grupę na kilkuosobowe zespoły. Rozdaj w grupach po sześć białych karteczek i poproś, aby wpisano na kartki rodzaje symptomów nadmiernego korzystania z sieci, a następnie aby ułożono z kartek piramidkę, w taki sposób, aby najtrudniejszy do zdiagnozowania, zdaniem grupy, symptom znalazł się na szczycie piramidki. W zespołach i na forum grupy przedyskutujcie poszczególne piramidki.

5 Myślące kapelusze

Cel: identyfikacja nowych zagrożeń nieprawidłowego wykorzystywania nowych technologii.

Przebieg:

Ćwiczenie wykorzystuje metodę Sześciu Myślących Kapeluszy Edwarda de Bono.

- Rozdaj uczestnikom kolorowe kartki, z których metodą origami przygotują sobie czapeczki – kapelusze. Dobrym sposobem jest również losowanie kolorów.
- Wyjaśnij, że kolor kapelusza będzie związany z wejściem osoby w rolę i określonym sposobem myślenia:
  - biały kapelusz -- wiązanie faktów i liczb,
  - czerwony kapelusz -- korzystanie z intuicji,
  - czarny kapelusz – obiektywna krytyka,
  - żółty kapelusz – logiczne konstruowanie,
  - zielony kapelusz – myślenie kreatywne i lateralne,
  - niebieski kapelusz – szerokie spojrzenie na problem.

Przedstaw problem, który będzie przedmiotem dyskusji i zapisz w widocznym miejscu:

Cyfrowa demencja oraz inne formy e-zagrożeń jako nowe następstwa nieprawidłowego użytkowania nowych mediów.

- Posadź uczestników w kręgu i daj czas na przygotowanie się do dyskusji i indywidualne szukanie argumentów zgodnie z kolorem kapelusza.
- Po nałożeniu przez uczestników kapeluszy rozpoczyna się dyskusja.

6 Wyszukiwarka na wesoło

Cel: trening kreatywności.

Przebieg:

- Zadaniem uczestników jest zapisanie na kartce w ciagu minuty jak najwięcej wyrazów rozpoczynających się na podaną przez prowadzącego literę np. a (arbuz, ananas, Ameryka itp.).
- Kolejne zadanie to zapisanie rzeczowników, które rozpoczną i zakończą się na wskazane przez prowadzącego litery np. k …….. t (kot, kojot, krawat itp.).
- Zadanie kończące to układanie zdań 3-, a później 4- i 5-wyrazowych na podane przez prowadzącego litery np. K…… s……..w…… (Kot strącił wazonik.)

7 Przemoc online

Cel: identyfikacja zjawiska cyberprzemocy oraz wskazywanie metod przeciwdziałania przemocy online**.**

Przebieg:

Podziel grupę szkoleniową na dwie mniejsze grupy. Poproś uczestników, aby każda z grup opracowała przypadek cyberprzemocy, a następnie przedstawiła go w formie teatralnej scenki sytuacyjnej. Kiedy obydwie grupy zaprezentują wybraną, przykładową sytuację związaną ze zjawiskiem cyberprzemocy rozpocznijcie dyskusję wokół tematów:

- w jaki sposób można było zapobiec tej sytuacji,
- jaka była rola oraz motywy poszczególnych osób (ofiara, agresor, świadek zdarzenia),
- w jaki sposób można zareagować oraz gdzie zwrócić się po pomoc w danym przypadku.

8 Dyskusja słoneczko

Cel: rozpoznawanie problemów i zjawisk, identyfikowanie oznak i powodów samobójstw.

Przebieg :

- Dyskusja słoneczko to odmiana dyskusji, w której uczestnicy w pierwszym etapie przedstawiają swoje opinie na małych kartkach papieru (każda opinia na oddzielnej kartce). Następnie układa się je w kręgu, przy czym powtarzające się opinie układamy tak, aby stworzyły promienie słoneczka.
- Zaproponuj problem: Czynniki, które wpływają na ryzyko popełnienia samobójstwa przez dojrzewającego nastolatka[1].
- Zadaniem uczestników jest przedstawienie swojej opinii na kartkach oraz ułożenie ich w kręgu. Opinie powtarzające się/zbliżone tworzą promienie. Zaproponowany układ jest odzwierciedleniem opinii grupy i prowadzi do dyskusji, która musi być zakończona podsumowaniem prowadzącego wskazującego prawidłowe rozwiązanie.
- Ćwiczenie może być kontynuowane pracą w grupach nad zagadnieniem zapobiegania zachowaniom samobójczym wśród młodzieży i/lub sposobami udzielenia pomocy.

[1] Więcej w rozdziale „**Zagrożenia zdrowia psychicznego i fizycznego**”

9 Konferencja prasowa

Cel: rozpoznawanie problemów i zjawisk – samobójstwa w Internecie.

Przebieg:

- Podziel grupę na 4–5 osobowe zespoły, których zadaniem będzie opracować historię nastolatka, który z powodów bezpośrednio lub pośrednio związanych z podejmowaniem aktywności w sieci podjął próbę samobójczą. W ćwiczeniu można wykorzystać również istniejące w mediach materiały.

Przykład: *Kolejna ofiara „terroru w sieci"? 12-latka popełniła samobójstwo* „12-letnia Rebecca S.popełniła samobójstwo w fabryce na Florydzie. Na jej profilach w serwisach Instagram i Ask.fm odnaleziono wpisy z obelgami i groźbami. Nie ma żadnych wątpliwości, że Rebecca była terroryzowana w sieci - mówi szeryf „fragm. art., źródło: http://www.tvn24.pl/wiadomosci-ze-swiata,2/kolejna-ofiara-terroru-w-sieci-12-latka-popelnila-samobojstwo,354823.html

- Pozostali uczestnicy wcielą się w rolę dziennikarzy zadających pytania, którzy szukają odpowiedzi na pytania, jak doszło do zdarzenia, czy i w jaki sposób można było uniknąć/zapobiec tej sytuacji, jaka była rola oraz motywy poszczególnych osób (ofiara, agresor, świadek), czy i ew. jakie są oznaki, kto i w jaki sposób może pomóc, w jaki sposób można zareagować oraz dokąd zwrócić się po pomoc w danym przypadku etc.

10 5 kroków

Cel: utrwalanie wiedzy dotyczącej zjawiska groomingu tj. uwodzenia dzieci przez Internet.

Przebieg:

- Podziel grupę na 5 grup roboczych. Poproś, aby grupy przygotowały opis charakterystycznych zachowań podczas etapów uwodzenia oraz spróbowały wypracować mechanizmy ochrony dziecka na każdym z etapów.

Grupa I – nawiązanie znajomości z dzieckiem
Grupa II – tworzenie relacji z dzieckiem
Grupa III – sprawdzanie ryzyka
Grupa IV – umocnienie relacji z dzieckiem
Grupa V – dążenie do spotkania
Poproś przedstawicieli grup, aby zaprezentowali wyniki swojej pracy [2].

[2] Więcej w rozdziale „**Zagrożenia społeczno-wychowawcze**" (*Pedofilia w sieci* A. Andrzejewska, J. Bednarek).

11 Plakat dla rodziców

Cel: utrwalenie informacji o czynnikach, które zwiększają ryzyko uwodzenia dzieci przez dorosłych.

Przebieg:

- Podziel grupę na 3–4 osobowe zespoły. Poproś, aby w grupach uczestnicy przygotowali plakat skierowany do rodziców o tym, kiedy dzieci są bardziej narażone na uwodzenie przez dorosłego.
- Poproś uczestników, aby w grupach przygotowali projekt ostrzeżenia zakładanego przed materiałami pornograficznymi dostępnymi w Internecie lub czasopismami o charakterze pornograficznym.

Modyfikacja**:**

- Poproś uczestników, aby wyszukali w Internecie strony, na których można zgłosić nielegalną pornografię publikowaną w Internecie.

12 Kampanie społeczne

Cel: utrwalanie wiedzy, trening kreatywności.

Przebieg:

- Przedyskutuj z grupą, jaki jest cel kampanii społecznych. Poproś uczestników, aby podali przykłady kampanii społecznych, które im się podobały i dlaczego oraz które z nich nie zrobiły wrażenia lub się im nie podobały i dlaczego.
- Poproś uczestników aby w 3–5 osobowych zespołach przygotowali założenia kampanii dotyczącej zjawiska sextingu (lub innych zagrożeń internetowych). Ważne, aby w projekcie kampanii znalazły się takie informacje, jak: cel kampanii, grupa docelowa, kanały komunikacji, wykorzystywane narzędzia (film, baner, plakat, reklama w prasie itp.).
- Poproś uczestników, aby znaleźli w Internecie przykłady kampanii społecznych (polskich i zagranicznych) związanych z obszarem cyberzagrożeń oraz bezpieczeństwa dzieci i młodzieży w Internecie. Wspólnie stwórzcie listę kampanii, które spotkały się z pozytywnym przyjęciem.

13 Powiem, pokażę

Cel: rozwijanie umiejętności prezentacji i graficznego przygotowania materiału prezentacyjnego.

Przebieg:

- Podziel grupę na mniejsze zespoły.
- Poproś, by każdy zespół przygotował, a następnie przedstawił na forum grupy kilkuplanszową prezentację na temat związany z wybranymi obszarami zagrożeń społeczno-wychowawczych.
- Zwróć uwagę na zasady dobrej prezentacji.

14 Co to jest stalking?

Cel: definiowanie pojęcia stalking.

Przebieg:

- Uczestników dzielimy na 4-osobowe grupy. Każdej z nich przydzielamy kartkę formatu A4. W środku arkusza uczestnicy wpisują wyraz stalking. Następnie poszczególne osoby (każda w innym rogu kartki) wpisują jedno zdanie, które się im kojarzy z wypisanym na środku kartki wyrazem.
- Po zakończeniu tej czynności kartkę należy obrócić zgodnie z ruchem wskazówek zegara. Następnie każdy dopisuje nowe zdanie, uzupełniające zdanie napisane wcześniej. Kartkę obracamy trzykrotnie, aby w każdym jej rogu uczestnik napisał swoje zdanie, które mu się kojarzy z wyrażonym w poprzednim zdaniu czy zdaniach poglądem pozostałych członków grupy.
- Przedstawiciele poszczególnych grup odczytują głośno zapisane zdania. Dyskutują w grupie.
- Ćwiczenie to pozwala na zebranie ciekawego materiału, który wymaga jednak dyskusji, omówienia, ew. korekty i podsumowania.
- Zakończeniem ćwiczenia jest wspólne zdefiniowanie pojęcia stalkingu[3].

[3] Więcej w rozdziale „**Zagrożenia społeczno-wychowawcze**" (artykuł *Stalking*).

15 Czerwone i czarne

Cel: rozpoznawanie problemów i zjawisk – stalking.

Przebieg:

- Przedstaw grupie problem: Najlepszym zabezpieczeniem przed stalkingiem jest zastosowanie narzędzi filtrujących lub blokujących połączenie z konkretną osobą.
- Rozdaj samoprzylepne kartki w dwóch kolorach.
- Zadaniem uczestników jest odpowiedź na dwa pytania, zapisanie na kartkach odpowiedzi, a następnie umieszczenie ich na przygotowanej planszy podzielonej na dwie części (plusy i minusy).
- Zakończeniem ćwiczenia jest zebranie opinii, dyskusja i podsumowanie dot. próby stworzenia procedury postępowania w przypadku stalkingu.

16 Substancje psychoaktywne

Cel: rozpoznawanie problemów i zjawisk – substancje psychoaktywne i dopingujące.

Przebieg:

Dopasuj do opisu substancji psychoaktywnej nazwę oraz objawy zażywania[4]

	Amfetamina	**a**	Charakteryzuje się silnym działaniem pobudzającym, wprowadza układ nerwowy w stan nadaktywności. Podana miejscowo wykazuje właściwości znieczulające, przez co znalazła zastosowanie w medycynie. Obecnie z powodu skutków ubocznych jest ona zastępowana przez nowe, mniej szkodliwe środki znieczulające. Pozostaje jednak wciąż wykorzystywana jako miejscowy środek znieczulający w okulistyce i otolaryngologii. Występuje pod postacią krystalicznie białego proszku. Zazwyczaj przyjmowana jest wziewnie do nosa, gdzie śluzówka wchłania ją niemal natychmiast, wywołując wpływ na ośrodki przyjemności w mózgu. Bywa też wcierana w środek małżowiny usznej lub dziąsła. Przyjmowana doustnie działa dużo słabiej, jednak znieczula błonę śluzową żołądka, przez co zanika uczucie głodu. Może być także palona poprzez dodanie jej do skrętów lub papierosów.	**X**	Działanie fizjologiczne: • opóźnia objawy zmęczenia, • zmniejsza potrzebę jedzenia i snu, • silnie rozszerza źrenice, zakłóca pracę serca, • prowadzi do pobudzenia psychoruchowego, • jest przyczyną wzrostu ciśnienia krwi i przyspieszenia oddechu, • zażycie większych dawek może spowodować wzrost temperatury ciała i drżenie mięśniowe. Pozornie pozytywnymi efektami działania, z powodu których młodzież sięga po tę substancję jest: odczucie silnej euforii, pobudzenie ruchowe i podniecenie seksualne, intensywne poczucie mocy fizycznej i umysłowej, zanik zdolności odczuwania przykrych wrażeń, poczucie wyższości i odsunięcie poczucia lęku. Zażycie powoduje również skrócenie czasu reakcji psychicznej – przyśpieszeniu ulegają procesy myślowe. Negatywne odczucia, z jakimi mogą spotkać się osoby przyjmujące to: niepokój i napięcie, bezsenność, załamanie nerwowe, urojenia o nieprzyjemnej treści oraz brak krytycyzmu co do własnych zachowań[2].
	Kokaina	**b**	Środek psychostymulujący, który powoduje długotrwałe pobudzenie. W ciągu ostatniego stulecia używana była w medycynie, jako środek odchudzający stosowany przez osoby otyłe, a także przez sportowców jako tzw. koks (doping). Pod inną nazwą – benzedryna, była stosowana w medycynie ok. 80 lat temu, do leczenia astmy oskrzelowej oraz napadowej senności. Amfetamina przyjmowana jest dożylnie, doustnie, palona i wdychana przez nos. Występuje w postaci bezwonnego proszku o gorzko-cierpkim smaku w kolorze od białego do ceglastego. Pobudzenie, które towarzyszy zażyciu amfetaminy może trwać od 2 do 3 godzin, w zależności od spożytej dawki[3].	**Y**	Objawy zażycia (działanie fizjologiczne): • rozszerzenie źrenic, • wzmożenie odruchów, • wzrost temperatury ciała, • pobudzenie i brak łaknienia, • szczękościsk, • nudności i wymioty, • odwodnienie, • kołatanie serca i tachykardia[4], • nagłe wzrosty ciśnienia i uderzenia krwi do głowy. Działanie zależy od nastroju i sytuacji osoby, która zażywa środek. Jeśli stan psychiczny osoby jest zły, może ulec pogorszeniu po jej zażyciu. Pozornie „pozytywnymi" skutkami zażycia są: euforia i przypływ energii, uczucie empatii i silnej więzi z otoczeniem, intensyfikacja przeżyć emocjonalnych, pobudzenie seksualne i zaostrzenie percepcji otoczenia. Do negatywnych oddziaływań możemy zaliczyć: napięcie emocjonalne, poczucie utraty kontroli, niepokój, który może przerodzić się w panikę, nadwrażliwość na bodźce zewnętrzne, nieprzyjemne halucynacje i depresję[5].

[4] Więcej w rozdziale „**Zagrożenia związane z uzależnieniami**" (*Internet jako źródło informacji o substancjach psychoaktywnych*)

	Ecstasy (MDMA)	**c**	Jest pochodną meskaliny – z jednej strony działa stymulująco na układ nerwowy, z drugiej posiada właściwości halucynogenne. W przeszłości środek ten miał zastosowanie w psychoterapii, co było związane z jego właściwościami wyzwalającymi empatię[6]. Tabletki są bardzo kolorowe lub też są to białe pastylki, które mają wytłoczone napisy lub wzorki (np. sierp, kot, ptak itp.).. „Jest to najczęściej mieszanka zawierająca kilka rodzajów środków psychoaktywnych o różnym składzie, jakości, oraz stężeniu"[7]. Wszystko to powoduje, że konsumenci sięgając po tę substancję grają w „rosyjską ruletkę".	**Z**	Objawy zażycia (działanie fizjologiczne): • brak apetytu, • jadłowstręt, • silne pobudzenie psychomotoryczne, • rozszerzenie źrenic, • przyspieszona akcja serca i szybki oddech, • podwyższone ciśnienie krwi, • częstsze wydalanie moczu, • uczucie suchości w ustach, • uszkodzenia szkliwa zębów. Efektem zażycia jest ogromny przypływ energii i znaczne podwyższenie nastroju, aż do euforii. Osoby będące pod wpływem tego narkotyku wykazują się wzmożoną aktywnością, której towarzyszy bezsenność. Mają polepszoną koncentrację i możliwość maksymalnego skupienia uwagi. Towarzyszy im poczucie pewności i mocy. Negatywnymi efektami działania są: drażliwość i agresywność, przymglona świadomość oraz wrażenie obecności insektów na skórze, tzw. formikacje[8].
	pochodne konopi indyjskich – **marihuana i haszysz**	**d**	W medycynie działanie THC[9] wykorzystywane jest do obniżenia ciśnienia śródgałkowego, działanie przeciwwymiotne i przeciwdrgawkowe. Jest suszem z kwiatostanu i liści, zawiera 0,5–5% THC. Również jest to żywica krzewu konopi, zawiera 2–19% THC. Największą zawartość THC (10–30%) zawiera olej haszyszowy powstały z rozpuszczonej żywicy konopi. Najczęstszą formą przyjmowania preparatów jest ich palenie[10].	**H**	objawy fizjologiczne: • wzrost ciśnienia krwi i przyśpieszone tętno, • pocenie się, • wysuszenie śluzówek jamy ustnej, niekiedy ataki kaszlu, • zwiększenie apetytu, • przekrwienie gałek ocznych, spojówek, czasami obrzęk powiek, • zawroty i bóle głowy, • zaburzenia pamięci, • zaburzenia koordynacji ruchowej, uwagi i możliwości uczenia się, • gorsza ogólna sprawność psychofizyczna. Odczucia po zażyciu są zależne od cech osobowości danej osoby, wielkości i drogi przyjętej dawki, stanu emocjonalnego w momencie przyjęcia, obecności innych osób oraz od współdziałania tego preparatu z innymi np. z alkoholem. Pozornie „pozytywnymi" aspektami zażywania jest: odprężenie i poczucie spokoju, zwiększenie poczucia przyjemności seksualnych, optymizm i podniesiona samoocena, wzrost wrażliwości zmysłów, zmiana poczucia mijającego czasu (mijający wolniej). Do negatywnych efektów ich działania możemy zaliczyć: skłonność do ulegania sugestiom, nieracjonalne myśli, zagubienie, zwiększone napięcie i niepokój, pogorszenie pamięci, apatia, lęki i urojenia oraz niemożność skupienia uwagi na wielu rzeczach naraz[11].

Prawidłowe odpowiedzi 1bZ, 3cY, 2aX, 4dH

[5, 6, 7, 9, 10, 11] zaczerpnięto z treści zawartych w publikacji

17 Metaplan

Cel: zbieranie informacji o przebiegu i wynikach określonego zjawiska.

Przebieg:

- Uczestników dzielimy na kilka grup 4–6 osobowych.
- Prowadzący zapisuje w widocznym miejscu temat/problem: *Internet jest źródłem informacji o substancjach odurzających i dopingujących*
- Uczestnicy pracują w grupach zgodnie ze schematem pytań:
  - Jak jest?
  - Jak powinno być?
  - Dlaczego nie jest tak, jak powinno być?
  - Wnioski

Warto posłużyć się arkuszem ułatwiającym zebranie wniosków

Internet jest źródłem informacji o substancjach odurzających i dopingujących	
Jak jest? Jak powinno być?	Jak powinno być?
Dlaczego nie jest tak, jak powinno być?	Wnioski:

18 W świecie gier

Cel: rozpoznawanie symptomów uzależnienia od gier komputerowych oraz utrwalenie wiedzy o rodzajach gier i oznaczeniach PEGI.

Przebieg:

- Przeczytaj uczestnikom poniższy cytat. Jest to wpis matki na forum poświęconym uzależnieniom:

  „Mój syn jest uzależniony od gier komputerowych, szczególnie od jednej, gra ze wszystkimi i rozmawia przez słuchawki, bywa, że nawet 10–14 godz. dziennie. Nic do niego nie dociera, nie szuka pracy, potrafi nie jeść cały dzień. Uważa, że jeśli nigdzie nie chodzi i nie używa żadnych używek, to nie ma problemu. Ostatnio powiedział, że jeśli to jest dla mnie problem, to skoczy z mostu i będę mieć kłopot z głowy. Sam nie podejmie leczenia, boję się coraz bardziej!!!!!!!!!!”

- Przedyskutuj z grupą, jakiego rodzaju gry należą do najbardziej uzależniających, zastanówcie się, jakie motywacje mogą spowodować przenoszenie życia do świata wirtualnego.
- Wybierz z grupy dwóch ochotników: jeden niech wcieli się w osobę uzależnioną od gier, drugi niech wcieli się w członka rodziny (rodziców, rodzeństwo) zaniepokojonego uzależnieniem i zmianą trybu życia. Niech w 5 minut pomyślą nad argumentami do rozmowy, a następnie przeprowadzą rozmowę mającą spowodować namówienie osoby uzależnionej do podjęcia terapii, uświadomienia sobie problemu. Pozostałe osoby z grupy mogą wspierać dyskutantów argumentami.
- Przedyskutujcie, na jakie cechy gry należy zwracać uwagę, chcąc kupić grę dziecku[6].

[6] Więcej w rozdziale „**Zagrożenia związane z uzależnieniami**” (artykuł *Gry komputerowe*).

19 Co Ty na to?

Cel: trening komunikacji, wymiana doświadczeń.

Przebieg:

- Poproś uczestników, by dobrali się w pary i rozdaj zestawy pytań/opisy sytuacji.
- Jedna osoba z pary wybiera pytanie/sytuację, zadaniem drugiej osoby jest udzielenie odpowiedzi.
- W kolejnej rundzie następuje zamiana ról w parach.

Uwaga: ćwiczenie można wykonać w większych grupach. Pozwala to na przedstawienie wielu rozwiązań oraz dyskusję.

Modyfikacje: przykłady/ opisy sytuacji podawane są przez uczestników grupy – w pierwszej fazie ćwiczenia każdy uczestnik tworzy pytanie/opisuje problem/sytuację na osobnej kartce.

Przykłady pytań/problemów/sytuacji, które można wykorzystać w ćwiczeniach:

- Jak się zachowasz, gdy dowiesz się, że 8-letnie dziecko Twoich sąsiadów, znanych Ci tylko z widzenia, jest aktywnym użytkownikiem portalu społecznościowego przeznaczonego dla młodzieży i dorosłych?
- Co powiesz matce 16-latka, która zgłosi Ci problem nadmiernego korzystania przez dziecko z komputera (dziecko codziennie prawie do rana gra w gry komputerowe)?
  Jak zareagujesz, gdy zobaczysz swoje zdjęcie, informację o sobie w Internecie w miejscach, w których ich nie zamieszczałeś/-łaś?
- Co zrobisz, gdy przedstawiciel rodziny, z którą współpracujesz powie, że znalazł w Internecie niepokojące go strony?

20 Kupuję w sieci

Cel: utrwalenie wiedzy o zasadach bezpieczeństwa podczas dokonywania zakupów przez Internet.

Przebieg:

- Podziel grupę na mniejsze 3–4 osobowe grupy robocze. Każda grupa niech wybierze produkt lub usługę, którą chce kupić. Z wykorzystaniem serwisów aukcji internetowych, porównywarek cen, niech w 15 minut wybierze najatrakcyjniejszą ofertę. Następnie niech sprawdzi usługodawcę pod kątem bezpieczeństwa (jakie sprzedawca ma opinie, czy strona jest właściwie zabezpieczona, czy cena jest realistyczna – nie jest zbyt zaniżona, czy nie istnieją jakieś ukryte płatności – np.: bardzo drogie koszty przesyłki).

- Przedyskutuj z grupą na podstawie dostępnych aktów prawnych, jakie prawa ma kupujący przez Internet i czym te prawa różnią się w stosunku do tradycyjnych form zakupów.

- Razem z grupą przygotujcie listę podstawowych zasad, którymi należy się kierować podczas zakupów przez Internet. Lista zasad powinna uwzględniać dobre praktyki dla całej rodziny – w tym określać zasady dokonywania mniejszych zakupów przez dzieci i młodzież.

21 Szyfrowanie

Cel ćwiczenia: rozróżnianie w najpopularniejszych przeglądarkach sesji szyfrowanych (bezpiecznych) – wykorzystywanych np. przy dokonywaniu transakcji w Internecie od zwykłych sesji http stosowanych przy przeglądaniu stron internetowych.

Potrzebny sprzęt i oprogramowanie: komputer z zainstalowanymi przeglądarkami: Internet Explorer, Firefox, Opera, Chrome.

Przebieg ćwiczenia: Łączenie się kolejno za pomocą wymienionych przeglądarek do określonego serwisu internetowego w celu zawarcia jakiejś transakcji i obserwowanie pojawienia się atrybutów świadczących o nawiązaniu bezpiecznej sesji (https).

Przykład: łączenie się do serwisu Allegro

1. Firefox – po wejściu na podstronę „moje Allegro", na której podaje się login i hasło pojawia się w pasku nawigacji przeglądarki zielona kłódka i nazwa bezpiecznego protokołu (https).

2. Internet Explorer

3. Opera

4. Chrome

Jeśli chcemy się dowiedzieć więcej szczegółów – klikamy na zieloną kłódeczkę:

22 Historie łudzące

Cel: rozumienie sposobów i zjawisk dotyczących wyłudzania informacji.

Przebieg:

- Dopasuj opis każdej z poniższych sytuacji do rodzaju zagrożenia, uzupełnij tabelę [7]

Zjawisko	Zdarzenie	wyjaśnienie
phishing		
pharming		
skimming		
Vishing		

Zdarzenia :

A:
Kasia bardzo się spieszyła, przed wyjazdem chciała opłacić rachunki. Gdy podłączyła się do sieci,przystąpiła do uregulowania należności przelewem internetowym. Żeby było szybciej, skorzystała z podpowiadacza. Odniosła wrażenie, że strona jej banku przeszła „mały lifting", jest lekko zmieniona. Prawie taka sama, ale… Nie było czasu na przyglądanie się. Kiedy podała numer z tokena, wyświetlił się jednak błąd i połączenie ze stroną banku zostało zerwane. Po kilku sekundach zalogowała się po raz kolejny i… zamarła: konto było puste. Ktoś przed chwilą dokonał przelewu całej kwoty na jakieś bliżej nieznane konto. Co się wydarzyło?

B:
Witek zawsze czyta wszystkie e-maile. Tego dnia otrzymał ich ponad pięćdziesiąt. Szczęśliwie nie wszystkie wymagały odpowiedzi. Ale jeden był ważny. Napisał do niego bank. W e-mailu pojawiła się informacja, że z powodów technicznych – przejścia na nowy, lepszy funkcjonalnie system informatyczny – tymczasowe logowanie odbywać się będzie poprzez podany w e-mailu link. Wystarczy „kliknąć" w podany link i przejść szybką procedurę weryfikacyjną. Witek z perfekcyjną dokładnością zastosował się do instrukcji. W końcu skrupulatność popłaca. Po kilku dniach okazało się jednak, że jego konto było mocno uszczuplone. Co się wydarzyło?

C:
Zosia miała dużo czasu na zrobienie przelewu drogą elektroniczną. Pamiętała, co przydarzyło się Kasi, dlatego dokładnie sprawdziła, czy adres www banku jest OK (znała go na pamięć). Strona banku nie budziła podejrzeń, wyglądała dokładnie tak samo jak zawsze, sprawdziła nawet, że kłódeczka w przeglądarce jest zamknięta, zatem wszystko jest w porządku. Niestety nie było. Gdy po kilku dniach zalogowała się po raz kolejny – zamarła: konto było puste. Co się wydarzyło?

D:
Zwyczajem Marii podczas turnusu wczasowego była popołudniowa kawa z deserem – za każdym razem w innym miejscu. Będę miała co opowiadać koleżankom po powrocie – myślała uradowana. W istocie … Opowieść głównie dotyczyła przypadku, który zdarzył się ostatniego dnia, kiedy to w uroczej kawiarence oddała kartę płatniczą pracownikowi obsługi. Ten wyszedł z kartą na zaplecze, jakiś czas nie wracał, tłumacząc się brakiem połączenia z bankiem. Wkrótce na koncie pojawił się debet. Co się wydarzyło?

E:
Zdzich otrzymał bardzo ważny e-mail, w którym bank prosił go o zadzwonienie pod numer 0-800…, pod którym powinien zaktualizować swoje dane konta bankowego. Zdzich po wykręceniu podanego w e-mailu numeru usłyszał automatyczną wiadomość. Poproszono go o podanie danych dostępowych do konta. Zdzich podał swój identyfikator i pełne hasło oraz numer telefonu komórkowego, którego używa do zatwierdzania transakcji online. W końcu jak bank prosi to znaczy, że to ważne. Po kilku dniach, gdy chciał dokonać przelewu – okazało się, że na koncie nie ma gotówki. Co się wydarzyło?

F:
Do Jacka zadzwoniono z banku z informacją, że zanotowano próbę nieautoryzowanego wykorzystania jego karty kredytowej. Mój bank jednak jest najlepszy – dba o mnie i moje finanse – pomyślał Jacek. Dowiedział się, że w celu wyjaśnienia sprawy istnieje natychmiastowa konieczność przejścia procedury weryfikacyjnej. Poproszono Jacka o podanie imienia, nazwiska, adresu, numeru karty kredytowej, daty ważności, kodu CVV jego karty oraz PIN-u. Jacek był zadowolony, że bank jest czujny, więc podał wszystkie wymagane dane. Po pewnym

[7] Więcej w rozdziale „**Cyberprzestępczość i nadużycia**" (artykuł *Zjawisko phishingu*)

czasie okazało się, że niestety nie mógł już zapłacić swoją kartą z powodu braku środków. Co się wydarzyło?

Zjawiska:
phishing, pharming, skimming, vishing

Wyjaśnienia, czyli co się wydarzyło:

1. W przypadku Kasi, w momencie w którym skorzystała z podpowiedzi co do adresu strony internetowej banku, nie zauważyła ona, że ten adres – choć łudząco podobny – nie był adresem banku. Np. jej bank elektroniczny używał adresu: Otobank.pl a Kasia zalogowała się na podstawioną stronę o adresie 0tobank.pl (zamiast dużej litery O – cyfra 0). Fałszywa strona wyglądała łudząco podobnie, Kasia nie miała czasu na dłuższe przyglądanie się. Gdyby była czujna, może zauważyłaby, że niektóre komunikaty na tej stronie były z błędami ortograficznymi czy stylistycznymi. Kasia nie sprawdziła także, czy w czasie logowania pojawiła się kłódeczka w przeglądarce internetowej oraz czy certyfikat tej strony należy do instytucji bankowej, w której Kasia ma konto. Kasia zalogowała się na podstawioną stronę pseudobanku i podała wszystkie dane potrzebne do wykonania transakcji. Także numer jednorazowego kodu z tokena, który otrzymała ze swojego banku. Intruzi przechwycili jej dane wraz z kodem/hasłem i natychmiast posłużyli się tymi informacjami, żeby dokonać nielegalnego przelewu z konta Kasi na konto w jakimś banku w innym kraju, z którego w łatwy sposób dokonali wypłaty. Kasia miała do czynienia ze zjawiskiem phishingu. Jej komputer był zawirusowany, więc przeglądarka podpowiedziała link do fałszywej strony, na której dokonano wyłudzenia danych konta i informacji autoryzującej transakcje.

2. Witek miał do czynienia ze zjawiskiem phishingu w połączenie ze spamem. Najpierw otrzymał w poczcie elektronicznej spam, który udawał, że pochodzi od banku, w którym Witek ma konto. Witek kliknął na link sugerowany w e-mailu i został skierowany na spreparowaną stronę www, na której dokonano wyłudzenia informacji bankowych od Witka, pod pozorem konieczności przejścia procedury weryfikacyjnej. Intruzi po otrzymaniu potrzebnych danych od Witka, dokonali nieuprawnionego wejścia na jego konto. Ponieważ Witek autoryzuje swoje transakcje za pomocą telefonu komórkowego (smartfona), intruzi zawirusowali jego smartfon, aby przejąć nad nim kontrolę w czasie dokonywania nielegalnych operacji na bankowym koncie Witka.

3. Zosia, mimo że wydawało się jej, iż była czujna i dokładnie sprawdziła, czy loguje się na stronę swojego banku (adres www był prawidłowy, wygląd strony nie budził podejrzeń, kłódeczka w przeglądarce była zamknięta) nie ustrzegła się przed zagrożeniem zwanym pharmingiem. Pharming występuje wtedy, kiedy użytkownik jest przekierowywany na fałszywą stronę banku zupełnie w sposób dla niego niezauważalny. Dzieje się tak wtedy, gdy np. komputer użytkownika jest zarażony szkodliwym oprogramowaniem (tzw. malware) lub systemy internetowe rozwiązujące nazwy domenowe są „zatrute" przez intruzów i kierują użytkowników Internetu na złe strony, nawet po wpisaniu w przeglądarkę prawidłowej nazwy internetowej banku. Zosia nie sprawdziła, czy certyfikat cyfrowy strony, na której dokonała logowania (uwierzytelnienia) należy do instytucji banku, w którym ma swoje konto bieżące. Gdyby to zrobiła, wykryłaby próbę oszustwa. Na fałszywej stronie banku intruzi wyłudzili od Zosi jej wszystkie dane konta bankowego oraz kod autoryzacji transakcji z tokena i dokonali nieuprawnionego przelewu z jej konta, podobnie jak w przypadku Kasi. Pharming można więc traktować jako zaawansowaną wersję phishingu.

4. Maria padła ofiara tzw. skimmingu. Nieuczciwy pracownik lokalu wyszedł z kartą płatniczą na zaplecze, gdzie dokonał nielegalnego skopiowania zawartości paska magnetycznego karty w celu wytworzenia kopii karty przez grupę przestępczą i późniejszego posługiwania się nią (np. robienia zakupów). Inną odmianą skimmingu jest instalowanie przez przestępców specjalnych nakładek na bankomaty, które sczytują z karty wszystkie dane, łącznie z PIN-em.

5. Zdzich padł ofiarą vishingu (w połączenie ze spamem). List e-mail, który wydawał się być informacją z banku, w rzeczywistości pochodził od przestępców chcących wyłudzić dane o koncie bankowym Zdzicha. Vishing może być połączeniem phishingu z oszustwem telefonicznym. Podany w e-mailu numer telefonu w rzeczywistości był przechwycony przez przestępców i służył do wyłudzenia informacji od Zdzicha. Na podstawie otrzymanych danych, przestępcy dokonali nielegalnych transakcji na koncie ofiary.

6. Jacek padł ofiarą vishingu. Przestępcy zadzwonili na numer telefonu Jacka, by wyłudzić informację, która pozwoliła im na dokonanie nielegalnych transakcji na jego koncie. Numer, z którego dzwoniono mógł się nawet prezentować jako numer należący do banku, w którym Jacek ma konto. Przestępcy bowiem, wykorzystując luki w systemach telefonii internetowej, podszyli się pod legalny bank. W tym wypadku nie został dodatkowo zastosowany klasyczny phishing (jak w przypadku Zdzicha). Odmianą tego przypadku jest także scenariusz, w którym fałszywy bank prosi o oddzwonienie na numer, który wygląda na prawidłowy numer banku.

23 Czy wiesz , że ...?

Cel: Wzbogacenie wiedzy dot. historii rozwoju bankowości elektronicznej w Polsce i na świecie.

Przebieg:
Rozdaj karty z quizem i instrukcją

QUIZ
Zadanie: Rozwiąż quiz. Sprawdź prawidłowe odpowiedzi.

1. Pierwszy bankomat uruchomiono:
a. w latach 60.
b. w latach 70.
c. w latach 80.

2. Pierwszy bankomat na świecie uruchomiono:
a. w Stanach Zjednoczonych
b. w Wielkiej Brytanii
c. w Japonii

3. Banki których europejskich krajów jako pierwsze świadczyły usługi bankowe poprzez Internet?
a. banki francuskie
b. banki szwajcarskie
c. banki fińskie i szwedzkie

4. W Polsce pierwszą formą bankowości elektronicznej były:
a. terminale płatnicze w punktach handlowo-usługowych
b. karty płatnicze
c. bankomaty

5. Świadczenie usług bankowości elektronicznej przez Internet w Polsce zaoferowano w roku:
a. 1998
b. 1992
c. 2001

6. Według danych ZBP i NBP za drugi kwartał 2012 roku z bankowości internetowej aktywnie korzystało:
a. około 8 milionów Polaków
b. ponad 10,7 miliona Polaków
c. poniżej 6 milionów Polaków

7. Na koniec II kwartału liczba bankomatów w Polsce wynosiła blisko 18 000.
a. fałsz, urządzeń było ok. 12 000
b. prawda, w tym okresie było 17 950 urządzeń

8. Za nieuprawnione transakcje dokonane kartą po jej zastrzeżeniu odpowiedzialność spoczywa na banku, pod warunkiem że:
a. karta klienta nie przekracza limitu 10 000 zł
b. klient nie zaniedbał swoich obowiązków – ochrony karty i kodów dostępu
c. karta należy do kategorii „złota karta"

9. Monitorowaniem rynku transakcji elektronicznych zajmują się:
a. Krajowa Izba Rozliczeń i Narodowy Bank Polski
b. Związek Banków Polskich i Ministerstwo Finansów
c. Narodowy Bank Polski i Związek Banków Polskich.

Odpowiedzi: 1a, 2a, 3c, 4c, 5a, 6b, 7b, 8b, 9c

24 Oszuści w Internecie

Cel: diagnozowanie oszustwa cybernetycznego oraz opracowanie dobrych praktyk.

Przebieg:

- Podziel grupę na zespoły. Przedstaw każdemu zespołowi wybrane problemy i poproś o omówienie/diagnozę problemu oraz zaproponowanie porad/informacji dla Pana Kowalskiego związanych z zagrożeniami oraz propozycję, co powinien zrobić, by nie stać się ofiarą.

- Poproś poszczególne zespoły, aby na forum zaprezentowały problem i jego rozwiązanie.

- Poproś uczestników o przedstawienie doświadczeń związanych z oszustwami internetowymi, z którymi się spotkali. Porozmawiajcie o dobrych rozwiązaniach.

Opisy zdarzeń:

Pan Kowalski otrzymuje e-mail z ofertą konkursu, w którym nagrodą jest nowy komputer/tablet tp.. w bardzo okazyjnej cenie. Aby wziąć udział w konkursie, należy wypełnić formularz zgłoszeniowy.

Pan Kowalski otrzymuje esemes z wiadomością informującą o wygranej przez niego dużej puli pieniędzy. Jedynym warunkiem jest odesłanie esemesa zwrotnego.

Pan Kowalski swobodnie serfując po Internecie, nagle otrzymuje komunikat na ekranie swojego komputera wystawiony przez policję, że został on zablokowany z powodu ściągania nielegalnych treści. W celu odblokowania komputera należy uiścić opłatę na określone konto.

Pan Kowalski serfuje swobodnie po Internecie, nagle na ekranie jego komputera pojawia się komunikat „Wygrałeś tablet/telefon lub inną bardzo atrakcyjną nagrodę". W okienku odliczany jest upływający czas na wpisanie swojego numeru telefonu komórkowego, który jest jedynym warunkiem odebrania nagrody.

Pan Kowalski posiadając konto na Allegro, otrzymał e-mail od administratora Allegro informującego, że jego konto zostało przejęte przez oszustów. Aby zapobiec konsekwencjom, niezwłocznie ma wypełnić formularz, w którym proszony jest o podanie starego hasła i wpisanie nowego.

Uwaga: Prowadzący lub uczestnicy mogą zaproponować inne sytuacje obrazujące zagrożenia związane z oszustwami internetowymi.

25

Bezpieczny komputer

Przebieg:

Rozdaj uczestnikom kartki zgodnie z poniższym wzorem. Zadanie może być realizowane indywidualnie lub zespołowo.

Lp.	Potencjalne zagrożenie	Zaznacz właściwy sposób rozwiązania	Dopisz propozycję dobrych praktyk
1.	E-mail, którego pochodzenia nie jesteśmy pewni	a. Należy odczytać wraz z załączonymi załącznikami b. Oznaczyć go jako SPAM c. Nie odczytywać załączników - skasować	
2	Link do strony www załączony np.: w e-mailu lub serwisie społecznościowym	a. Należy zwrócić uwagę na adres (link) strony, do której otrzymaliśmy link b. Klikamy na każdy link, ponieważ nie stanowi on zagrożenia c. Należy posiadać zawsze aktualny system antywirusowy i włączony Firewall	
3	Podłączanie dysku zewnętrznego do komputera	a. Każdorazowo należy wykonać skanowanie oprogramowaniem antywirusowym b. Dyski zewnętrzne nie są zagrożeniem dla komputera c. Nie należy podłączać dysków zewnętrznych niewiadomego pochodzenia	
4	Złośliwe oprogramowanie	a. Może propagować się przez zainfekowane strony www b. Propaguje się za pomocą sieci komputerowej c. Propaguje się za pomocą innych nośników np.: dysków zewnętrznych	
5	Nieaktualizowane oprogramowanie	a. Może być źródłem infekcji komputera b. Nie ma wpływu na bezpieczeństwo komputera c. Jest jedynym możliwym źródłem infekcji komputera	

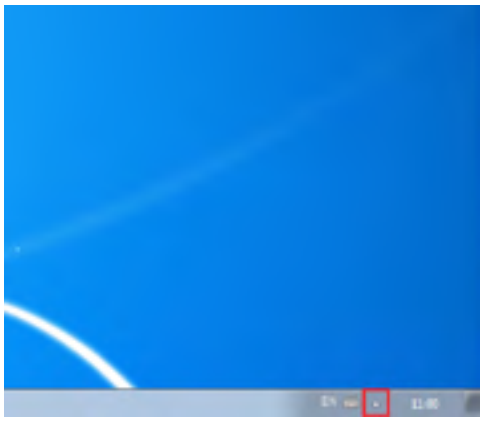
Odp: (1 - b,c), (2 – a,c) , (3 – a,c) , (4 – a,b,c), (5 - a)

26 Bezpieczne odłączanie dysków zewnętrznych USB

Cel: praktyczne ćwiczenia procedury bezpiecznego odłączania pamięci przenośnych od komputera.

Przebieg:
Jeśli chcesz uniknąć utraty danych podczas zapisywania lub nawet uszkodzenia systemu plików, dysków flash USB, należy zastosować odpowiednią sekwencję czynności przed fizycznym odłączeniem urządzenia od komputera. Dotyczy to wszystkich pamięci podłączanych do komputera przez port USB jak również karty SD. Sprawdź praktycznie, w jaki sposób należy bezpiecznie odłączyć od komputera dyski zewnętrzne. Poniżej przedstawiony został przykład z wykorzystaniem systemu operacyjnego Windows 7.

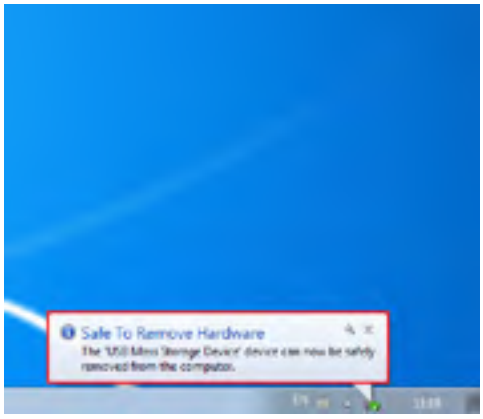
1. Kliknij małą strzałkę na pasku informacyjnym.



2. Kliknij polecenie w oknie dialogowym na następującą ikonę: **Bezpieczne usuwanie sprzętu i wysuwanie nośników.**

3. Kliknij na liście poniżej odpowiedni wpis na dysk USB.

4. Komunikat, że sprzęty mogą być usunięte. W tym momencie możesz bezpiecznie odłączyć swój dysk USB od komputera.



27 Ochrona przez botnetem

Cel: zabezpieczanie przez złośliwym oprogramowaniem.

Przebieg:

- Podziel grupę na dwa zespoły. Do zadań pierwszego zespołu należy przygotowanie w punktach informacji: W jaki sposób rozpoznać, czy komputer jest zarażony złośliwym oprogramowaniem? (wsparciem jest tekst w rozdziale Komputer).

- Drugi zespół poproś o przygotowanie odpowiedzi w punktach na pytanie:
  - W jaki sposób uniknąć złośliwego oprogramowania, które może podłączyć nasz komputer do botnetu? (wsparciem jest tekst w rozdziale Komputer).

- Zadaniem zespołów jest przedstawienie innym zebranych informacji na zadany temat. Informacje mogą być uzupełnione wskazówkami dobrych praktyk.

Podpowiedź do pytania 1: Nie zawsze jest łatwo rozpoznać, czy komputer został zarażony złośliwym oprogramowaniem, a tym samym, czy jest podłączony do botnetu. Jeśli działa wolniej niż zazwyczaj, zawiesza się, czy często przestaje odpowiadać, może to oznaczać, że został on zarażony. Te same symptomy mogą jednak też wskazywać na problem z oprogramowaniem lub sprzętem, które nie mają nic wspólnego ze złośliwym oprogramowaniem.

Podpowiedź do pytania 2:
Zainstaluj oprogramowanie antywirusowe i antyszpiegujące z zaufanego źródła.
Aktualizuj całe oprogramowanie (system operacyjny, przeglądarka, etc.).
Używaj bezpiecznych haseł i zachowaj je w tajemnicy.
Nigdy nie wyłączaj Twojego firewalla.
Ostrożnie używaj pamięci flash.

28

Podstawowe informacje przy łączeniu się do sieci Wi-Fi.

Cel: zachowanie bezpieczeństwa przy łączeniu się do nieznanych sieci Wi-Fi.

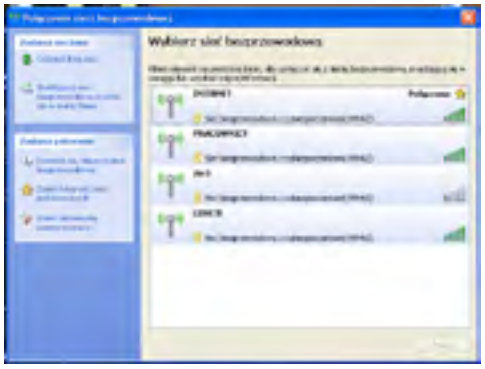
Przebieg:

Do przeprowadzenia ćwiczenia potrzebne jest urządzenie mobilne np. laptop z bezprzewodową kartą sieciową (obsługującą standard 802.11 – nazywaną Wi-Fi) lub telefonu komórkowego. W zależności od systemu operacyjnego w pasku Windows pojawi się ikonka sieci bezprzewodowych.

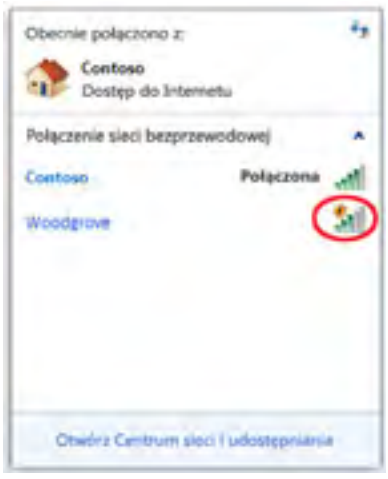
Po kliknięciu na ikonkę pojawi się lista dostępnych sieci Wi-Fi w zasięgu Twojego komputera.

Do najważniejszych informacji, na jakie należy zwrócić uwagę należą:

1. Nazwa sieci (inaczej SSID)
2. Sposób zabezpieczenia sieci (np.: WPA 2)
3. Poziom sygnału (wyrażony w postaci słupków)



Pamiętaj: W miarę możliwości należy łączyć się z sieciami wymagającymi klucza zabezpieczeń sieciowych lub zabezpieczonymi w inny sposób, na przykład certyfikatem. Informacje są przesyłane w takich sieciach w postaci szyfrowanej, co może pomóc w chronieniu komputera przed nieautoryzowanym dostępem. Jeżeli w oknie Połącz z siecią zostaną wyświetlone dostępne sieci bezprzewodowe, te z nich, które nie zostały zabezpieczone, będą oznaczone ikoną żółtej tarczy.



29 ANTYWIRUS/ANTYSPAM

Cel: utrwalenie wiedzy dotyczącej znajomości podstawowych pojęć dotyczących cyberzagrożeń.

Przebieg:
Rozdaj karty z quizem i instrukcją

QUIZ
Zadanie: Rozwiąż quiz. Sprawdź prawidłowe odpowiedzi

1. SPAM to?
   a. Niechciane lub niepotrzebne wiadomości elektroniczne
   b. Program szpiegujący
   c. Program, który podszywa się pod inne programy
   d. Szkodliwe oprogramowanie, które aby istnieć potrzebuje tzw. nosiciela

2. Aby komputer był chroniony przed szkodliwym oprogramowaniem powinien posiadać aktualny/ą?
   a. Program antywirusowy
   b. Zaporę ogniową
   c. Program antywirusowy i zaporę ogniową
   d. Bazę wirusów

3. Co to jest wirus komputerowy?
   a. Programy mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera.
   b. Plik pobrany z Internetu
   c. Określenie oznaczające usterkę komputera
   d. Zbiór fałszywych danych

4. Czym jest botnet
   a. Niechcianą pocztą przysyłaną na skrzynkę e-mail
   b. Siecią komputerową podłączoną do Internetu
   c. Grupą komputerów zainfekowanych złośliwym oprogramowaniem
   d. Oprogramowaniem antywirusowym

5. Funkcję ochrony dzieci przed nielegalnymi treściami w Internecie realizuje:
   a. Antywirus/Antyspam
   b. Firewall
   c. Program szyfrujący dane na dysku
   d. Programy „Filtry Rodzinne”

Odp: 1a, 2c, 3c, 4a, 5d

30

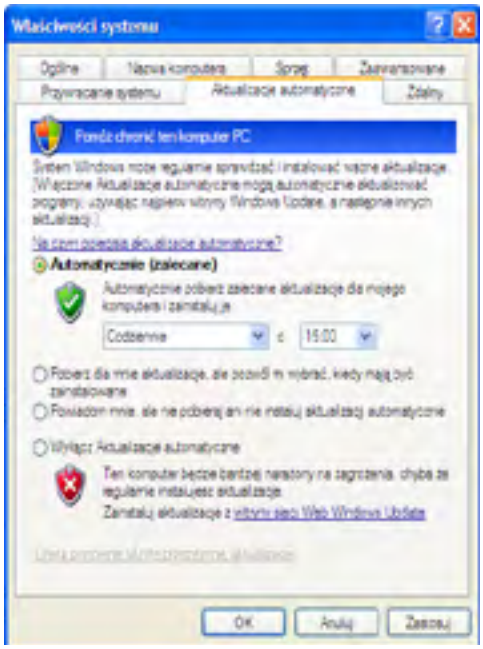
Nazwa:

Czy jesteś aktualny?

Cel: Celem ćwiczenia jest praktyczne sprawdzenie, czy na naszym komputerze system operacyjny i podstawowe programy takie jak przeglądarka, czytnik plików PDF oraz program antywirusowy mają włączone opcje bieżących aktualizacji (automatyczne, bądź ręczne).

Przebieg: Do wykonania ćwiczenia użytkownik musi dysponować komputerem z systemem operacyjnym Windows wraz z jedną z przeglądarek IE, Firefox, Chrome, Opera, programem odczytu plików PDF (Acrobat Reader) i systemem AV (antywirus). Kolejno przechodzimy z uczestnikami ćwiczenia przez odpowiednie procedury w konfiguracji komputera, aby uzyskać wiedzę o stanie aktualizacji.

1. **System operacyjny**
   W panelu sterowania Windows widzimy ikonkę System. Po kliknięciu w nią pojawia się informacja, jakiej wersji oprogramowania systemowego używa nasz komputer. Po kliknięciu w zakładkę „Aktualizacje automatyczne" widzimy okno, które informuje, czy i w jaki sposób dokonywane są aktualizacje. Do wyboru mamy takie możliwości:
   - aktualizacje automatyczne (zalecane przez producenta), z możliwością wybrania dogodnej pory użytkownika (np. codziennie o godz. 15)
   - pobieranie bez automatycznej instalacji (użytkownik decyduje każdorazowo, kiedy nastąpi instalacja),
   - tylko powiadomienie o istniejącym uaktualnieniu (bez pobrania i instalacji),
   - wyłączenie automatycznych aktualizacji (w dalszym ciągu będzie możliwe pobranie ręczne aktualizacji z witryny Windows Update).



Jeśli więc miałeś wybraną opcję „Automatyczne aktualizacje", to znaczy, że twój system operacyjny Windows jest aktualny.

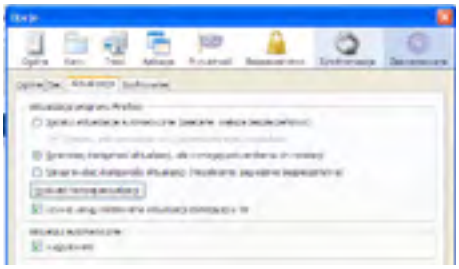
UWAGA: Producenci nie aktualizują swoich systemów w nieskończoność. Jeśli pojawia się nowa wersja danego systemu (np. Windows 7), to aktualizacje poprzednich wersji (np. Windows XP) po kilku latach się kończą – w tym wypadku jest to kwiecień 2013 – i użytkowanie starych systemów wiąże się z bardzo dużym zagrożeniem. Tak naprawdę jest nieakceptowane i należy przeinstalować system na nowy lub zaopatrzyć się w nowy komputer.

2. **Przeglądarka (na przykładzie Firefox)**
   Twórcy przeglądarki Firefox dbają o uaktualnienia. Od czasu do czasu na ekranie pojawia się po prostu okienko z informacją, że dostępna jest kolejna aktualizacja bezpieczeństwa.

Kiedy chcemy sprawdzić, jakiej wersji przeglądarki używamy, wystarczy kliknąć w pasku głównym na „Pomoc" a nastepnie zakładkę „O programie Firefox". Pojawi się okienko jak poniżej.

Widać, że proponowana aktualizacja zmieni używaną przez nas wersję 18.0.2 na wersję 19.0.

A jeśli chcemy mieć pewność, czy aktualizacje będą nadchodziły, wystarczy sprawdzić w menu przeglądarki: „Narzędzia" -> „Opcje" -> „Zaawansowane"



3. **Czytnik plików PDF (Acrobat Reader)**
   Pliki w formacie PDF są coraz bardziej popularnym sposobem prezentowania treści w witrynach internetowych oraz jako załączniki poczty elektronicznej. Nie wszyscy wiedzą, że w takim dokumencie także mogą gnieździć się wirusy[8]. Należy dbać więc, aby nasz program odczytujący pliki PDF (w tym przypadku Acrobat Reader) był zawsze aktualny.

Jak sprawdzić, czy nasz program jest aktualny? Po uruchomieniu Acrobat Readera należy w głównym pasku Menu aplikacji wybrać zakładkę „Pomoc" a następnie „Sprawdź uaktualnienia". Otrzymamy okienko, przykładowo, takie jak poniżej:
Możemy się więc dowiedzieć, że powinniśmy zezwolić na pobranie zalecanej aktualizacji ze strony producenta, a następnie dokonać instalacji uaktualnienia.

4. **Program antywirusowy**
Istnieje bardzo wiele programów antywirusowych. Na często zadawane pytanie: który program jest lepszy, a który gorszy można odpowiedzieć nieco przewrotnie: najgorszy jest ten, który nie jest aktualizowany, bo nie posiada aktualnej bazy wzorców wirusów i innego szkodliwego oprogramowania.
Programy antywirusowe zwykle same informują poprzez pojawianie się odpowiednich komunikatów na ekranie, że wystąpił problem z aktualizacjami.
Aby przekonać się, czy twój program AV ma aktualną bazę wirusów – kliknij w ikonkę tego programu, którą zwykle możesz znaleźć w dolnym pasku ekranu komputera i przeczytaj dokładnie, co jest napisane w okienku informacyjnym. Zwykle jest to napisane na tyle jasno, że łatwo się zorientować, kiedy (jaka data) była ostatnia aktualizacja oprogramowania, kiedy nastąpiło ostatnie skanowanie komputera (czyli poszukiwanie wirusów na komputerze czy tablecie oraz czy wykryto jakieś szkodliwe oprogramowanie).
Jeśli jakieś komunikaty będą budziły twoją wątpliwość – zwróć się do kogoś, kto jest biegły w administrowaniu komputerem.

[8] *Złośliwe pliki PDF* http://www.cert.pl/news/1961)

31 Kopie zapasowe

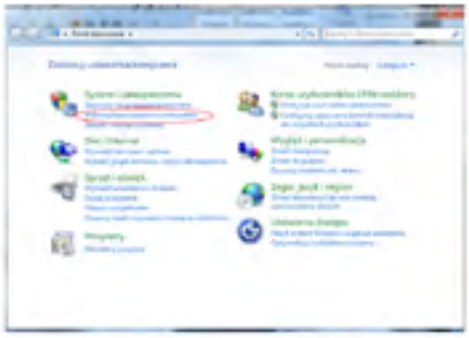
Cel: praktyczna ilustracja przykładu tworzenia kopii zapasowych w środowisku komputera z systemem operacyjnym Windows 7. Bazą teoretyczną ćwiczenia jest rozdział „Kopie zapasowe" w dziale „Komputer".

Przebieg: Na dowolnym komputerze (tutaj z systemem Windows7) tworzymy z uczestnikami ćwiczenia kopie zapasowe cennej zawartości dysku, a następnie odtwarzamy pliki z kopii.

1. **Tworzenie kopii zapasowych**

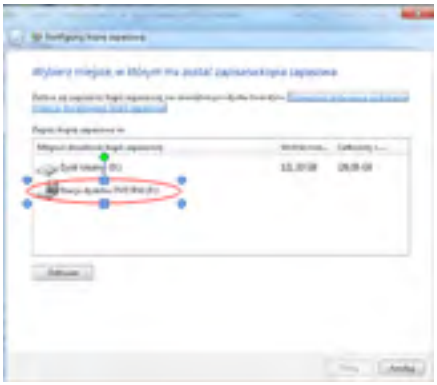
   Kopie zapasowe powinniśmy wykonywać na zewnętrzych nośnikach, takich jak dyski podłączane poprzez port USB, pendrive'y czy płyty DVD RW. Pojemność podłączonego nośnika powinna wystarczać do składowania plików, które zamierzamy umieścić na kopiach zapasowych. Jeśli cała zawartość nie mieści się na jednym nośniku, system poprosi o włożenie kolejnego nośnika w trakcie wykonywania kopii. W pierwszym kroku należy więc podłączyć zewnętrzny dysk lub pendrive.

   Następnie: w Panelu sterowania w sekcji „System i zabezpieczenia" istnieje opcja „Wykonaj kopię zapasową komputera".

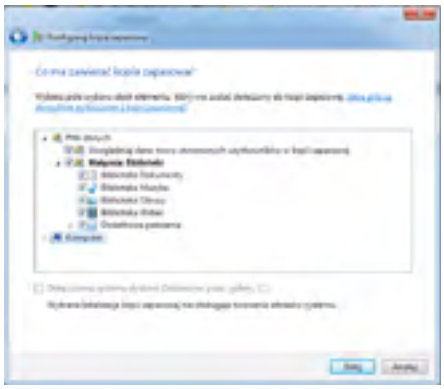


Następnie należy podążać za kolejno rozwijającymi się okienkami, aby:

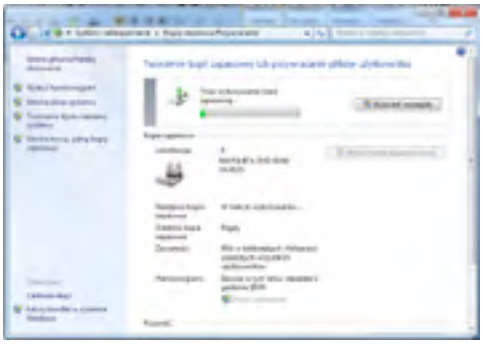
- skonfigurować tworzenie kopii zapasowej (backup może się dokonywać cyklicznie w ustalonym dniu tygodnia i godzinie),
- wskazać napęd, na który mają zostać przekopiowane nasze pliki,



dokonać wyboru, co chcemy, żeby było kopiowane (pliki danych, całe dyski komputera):

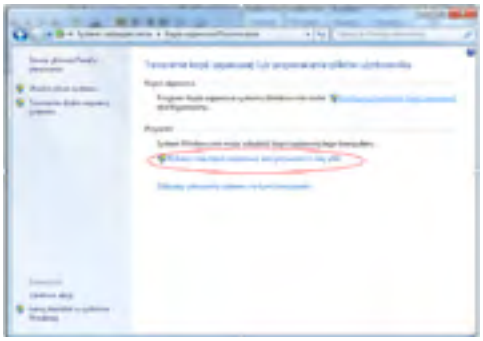


Nastepnie uruchamiamy wykonywanie kopii i obserwujemy postęp prac, aż do zakończenia:



Po wykonaniu kopii powinniśmy się upewnić, że została stworzona z sukcesem. W tym celu, za pomocą tych samych narzędzi („System i zabezpieczenia ->Kopia zapasowa/Przywracanie) dokonujemy odtworzenia z zewnętrznego nośnika zapisanej kopii bezpieczeństwa.

W ramach ćwiczenia spróbujmy zatem wykonać kolejną kopię bezpieczeństwa, aby zorientować się, jak przywraca się ostatnią wykonaną kopię, by mieć najaktualniejsze dane.



32 Silne hasło

Cel: tworzenie silnych haseł.

Przebieg:

- Poproś na początku zajęć (przed przedstawieniem wskazówek budowy silnych haseł) uczestników o napisanie na imiennych kartkach przykładowego hasła. (Czas: do 1 minuty)

- Udziel uczestnikom wskazówek budowy silnych haseł, które zostały przedstawione w artykule „Silne hasła". Następnie poproś uczestników o skonstruowanie silnego hasła, które napiszą na imiennych kartkach według ustalonych wspólnie wymaganych parametrów składających się na hasło jak np: (Czas: do 5 minut)

  1. Minimalna liczba znaków np. 8
  2. Wymagane małe i duże litery
  3. Wymagane znaki specjalne
  4. Wymagane cyfry
  5. Brak możliwości używania znaków, które znajdują się obok siebie na klawiaturze (np. qwerty, 123456, qweasd).

- Poproś każdego z uczestników o wypisanie na tablicy stworzonych haseł (pierwszego oraz drugiego). Przeprowadź dyskusje w grupie na temat technik budowania silnych a zarazem łatwych do zapamiętania haseł. (Czas do 15 minut)

33 Silne hasło na wesoło

Cel: trening kreatywności.

- Do przeprowadzenia ćwiczenia potrzebne są kartki papieru, nożyczki oraz dwa pojemniki.
- Poproś każdego uczestnika o napisanie na kartce drukowanymi literami słowa składającego się z 8 znaków oraz dwóch cyfr – przykład KOMPUTER03 lub KAROLINA90
- Ciągi znaków powinny zostać napisane na kartce przez uczestników tak, aby następnie mogli je pociąć na oddzielne litery i cyfry.
- Każdy z uczestników składa pocięty wyraz do dwóch przygotowanych pojemników
  - o Pierwszy z literami (8 kartek)
  - o Drugi z cyframi (2 kartki)
- Następnie poproś, aby każdy z uczestników wylosował z przygotowanych łącznie 10 kartek (8 z pierwszego i 2 z drugiego).
- Zadaniem każdego uczestnika jest zbudowanie zdania składającego się ze słów zaczynających się na litery oraz cyfry, które uczestnik wylosował, a następnie zapisanie go na kartce i przestawienie na forum. W celu skomplikowania zadania można wprowadzić utrudnienie dotyczące ułożenia zdania z liter w kolejności ich wylosowania.

34 Dbam o prywatność online

Cel: utrwalenie informacji o bezpiecznych zachowaniach podczas korzystania z portali społecznościowych oraz metodach przeciwdziałania cyberprzemocy**.**

Przebieg:

- Poproś grupę, aby zapoznała się z ustawieniami prywatności, które można zastosować na dwóch najbardziej popularnych serwisach społecznościowych w Polsce: Facebook i nk.pl.
  Podziel grupę na mniejsze 3–4 osobowe grupy robocze i poproś, aby w 15 minut przygotowali na piśmie przykładową sytuację związaną z cyberprzemocą. Potem niech grupy zamienią się kartkami z opisem danej sytuacji i zastanowią się, w jaki sposób można było danej ryzykownej sytuacji uniknąć.
- Podziel grupę na mniejsze, maksymalnie 10 osobowe grupy robocze. Jedna grupa niech przygotuje projekt plakatu z poradami, jak dbać o prywatność w sieci, druga grupa niech przygotuje projekt plakatu z procedurą reagowania w przypadku cyberprzemocy (jako źródło można zaproponować stronę saferinternet.pl lub helpline.org.pl).

35 Znajomy, nieznajomy…

Cel: utrwalenie wiedzy o sposobach ochrony danych osobowych oraz o zasadzie ograniczonego zaufania do osób poznanych w sieci.

Przebieg:

- Poproś grupę, aby każdy indywidualnie sprawdził, jak można zgłosić do GIODO próbę wyłudzenia danych osobowych? Zapytaj, gdzie jeszcze według grupy można zgłosić podobny przypadek (np. moderatorzy serwisów społecznościowych).
- Podziel grupę na pięcioosobowe zespoły robocze, niech na arkuszach papieru uzupełnią, jakie dane można lub jakich nie można publikować zgodnie z poniższą tabelą. Następnie przedyskutuj w większym gronie, dlaczego informacje zostały tak przez grupy podzielone.
- Przedyskutuj w grupie szkoleniowej, jakiego rodzaju informacje nie powinny znaleźć się na zdjęciach publikowanych w Internecie. Przed dyskusją przygotuj sytuację przykładową (np.: zdjęcie na tle domu z widocznym adresem).

Można publikować	Nie można publikować	Można publikować z zachowaniem szczególnej ostrożności

36 Filmy i muzyka

Cel: zdobycie praktycznej wiedzy o zasadach prawa autorskiego funkcjonujących w Internecie.

Przebieg:

- Rozdaj grupie kartki z opisem problemu lub zapisz na dużym arkuszu i zawieś w widocznym miejscu.

W kinach rozpoczęto emisję najnowszej produkcji z Jamesem Bondem. Pan Jan chce obejrzeć ten film, ale nie chce płacić za drogie, jego zdaniem, bilety. Rozważa trzy drogi postępowania.

- Podziel grupę na mniejsze zespoły i poproś o ocenę pod względem prawnym i możliwych konsekwencji dla funkcjonowania sieci każdą z proponowanych dróg.
- Przedyskutujcie zgodność konkretnych rozwiązań z prawem, a także konsekwencje płynące z wyboru konkretnego rozwiązania. Moderator w podsumowaniu wyjaśnia, czy oceny uczestników były prawidłowe[9].

Rozwiązanie 1:

Pan Jan ściąga nowy film na swój dysk z portalu, na który ktoś skopiował nielegalnie dzieło, ogląda go, a następnie umieszcza na swojej ogólnodostępnej stronie internetowej, tak aby był on dostępny dla wszystkich użytkowników.

Rozwiązanie 2:

Pan Jan ogląda film, korzystając z jednego z portali, na który ktoś skopiował nielegalnie dzieło.

Rozwiązanie 3:

Pan Jan decyduje się poczekać, aż film znajdzie się na jednym z legalnie działających portali internetowych oferujących filmy w zamian za oglądanie reklam.

Wyjaśnienie

Tylko stosując ostanie rozwiązanie Pan Jan postępuje prawidłowo. Z prawnego punktu widzenia oglądając nielegalnie skopiowany do Internetu film Pan Jan nie narusza prawa. Jednakże warto zauważyć, iż swym działaniem uszczupla dochody twórców i właścicieli praw autorskich tego dzieła. Masowa skala takich działań powoduje poważne perturbacje i mniejsze możliwości, jeśli chodzi o tworzenie nowych i wartościowych dzieł. Warto przy tym zauważyć, iż w przypadku bezdyskusyjnie nowego dzieła istnieje także ryzyko ponoszenia odpowiedzialności z tytułu korzystania z niego poza oficjalnymi kanałami dystrybucji. W przypadku pierwszego rozwiązania możemy mówić o ewidentnym naruszeniu prawa. Osoby postępujące w ten sposób narażają się na konkretne konsekwencje karne i finansowe.

[9] Więcej w rozdziale „**Cyberprzestępczość i nadużycia**" (artykuł *Treści szkodliwe i nielegalne*).

37 Zgłoś nielegalne treści

Cel: utrwalenie informacji o sposobach reakcji na nielegalne treści publikowane w Internecie

Przebieg:

- Poproś uczestników, aby wyszukali w Internecie strony internetowe, gdzie można:
  a/ zgłosić nielegalne i szkodliwe treści
  b/ znaleźć pomoc, jeśli dziecko natrafiło na nieodpowiednie strony
- Podziel grupę na mniejsze 3–4 osobowe grupy robocze i poproś, aby grupy dowiedziały się więcej o zespołach Dyżurnet.pl, Helpline.org.pl, Saferinternet.pl, Cert.pl. W jaki sposób można przekazać zgłoszenie do tych zespołów?
- Poproś uczestników, aby na swojej ulubionej witrynie informacyjnej odnaleźli sposób kontaktu z administratorami/moderatorami portalu. Możemy poprosić uczestników, aby zgłosili nieodpowiedni komentarz do moderacji.

38 3 kąty

Cel: omówienie wiarygodności informacji publikowanych w Internecie.

Przebieg:

Podziel grupę na trzy równoliczne zespoły robocze. Skład grup dobierany jest losowo. Podczas dyskusji uczestnicy reprezentują stanowisko grupy, którą wylosowali, starając się uargumentować dany pogląd.

- Poproś, aby grupy przygotowały stanowisko do opinii:

Grupa I – można powiedzieć, że praktycznie wszystkie, a na pewno większość materiałów zamieszczonych w sieci to dość wiarygodne źródła informacji, które mogą być wykorzystywane bez dodatkowej weryfikacji w innych źródłach informacji. W końcu umieszczane są tam często przez ekspertów, specjalistów w swoich dziedzinach, i poparte poważnymi instytucjami. Stronami godnymi zaufania są również niezależne źródła informacji zamieszczone przez internautów, np. w komentarzach, blogach, profilach.

Grupa II – tylko część materiałów zamieszczonych w sieci jest wiarygodną informacją. Stronami godnymi zaufania są strony prowadzone przez instytucje, duże portale informacyjne oraz ekspertów. Niestety sporo treści jest kompletnie bez sensu.

Grupa III – należy bardzo uważać na wiarygodność wszystkich informacji w sieci, ponieważ większość to informacje nieprawdziwe i nierzetelne. Na 100% można wierzyć tylko informacjom zamieszczonym w książkach i materiałach drukowanych. Posiadają recenzje merytoryczne.

Przedyskutujcie na forum grupy przygotowane stanowiska.

Dodatkowymi zagadnieniami, które można wziąć pod uwagę są: czym różni się czas publikacji od czasu edycji, kto może stworzyć definicję na Wikipedii, w jaki sposób rozpoznać wiarygodną stronę.

39 O czym mowa?

Cel: opisywanie, definiowanie zjawisk, rodzaju zagrożeń.

Przebieg:

- Podziel grupę na zespoły 5–6 osobowe.
- Poproś, by każdy zespół wybrał dowolne zjawisko dotyczące cyberzagrożeń zdrowia psychicznego i fizycznego, społeczno-wychowawczego, zagrożeń związanych z uzależnieniami lub cyberprzestępczością, a następnie opisał je bez używania słów kluczowych tj. nazwy danego zjawiska/zagrożenia i wyrazów od nich pochodzących. Zadaniem zespołów jest przekazanie opisów innym zespołom z prośbą o odgadnięcie, czego opis dotyczy.
- Omów ćwiczenia na forum grupy.

Uwaga: Zadanie można przedstawić w dowolny sposób, np. opisu tekstowego oraz w dowolnej formie graficznej.

40 Ukryte płatności i wykorzystanie danych osobowych

Cel: zaznajomienie uczestników z procedurą postępowania w przypadku ukrytych płatności oraz bezpodstawnego wykorzystania danych osobowych.

Przebieg:

- Podziel grupę na mniejsze 3–4 osobowe grupy robocze. Poproś uczestników, aby w mniejszych zespołach zastanowili się nad przypadkami witryn, które wykorzystywały ukryte płatności i jakie były konsekwencje prawne wobec takich administratorów. Poproś uczestników, aby obejrzeli w grupach witrynę http://uokik.gov.pl i zastanowili się, w jaki sposób można zgłosić tego typu nadużycia? Czy są potrzebne do tego jakieś dokumenty?
- Podziel grupę na mniejsze 3–4 osobowe grupy robocze. Poproś uczestników, aby w zespołach przedyskutowali, gdzie można zwrócić się o pomoc w przypadku, gdy portal bezpodstawnie przetwarza nasze dane osobowe? Poproś uczestników, aby obejrzeli w grupach witrynę http://giodo.gov.pl i zastanowili się, w jaki sposób można zgłosić tego typu nadużycia? Czy i ew. jakie dokumenty są potrzebne przy zgłoszeniu nadużyć?

41 Teleturniej czy talk-show

Cel: rozwijanie kreatywności, utrwalanie wiedzy dot. cyberzagrożeń.

Przebieg:

- Podziel grupę na mniejsze zespoły (5–6 osobowe).
- Zadaniem zespołów jest zaproponowanie gry podsumowującej zdobyte wiadomości/umiejętności z obszaru cyberzagrożeń. Gra powinna przypominać teleturniej, talk-show, program typu debata. Forma: zasady udziału, zakres tematyczny (pytania, zadania) powinny być ustalone i opisane przez zespół.
- Omów wszystkie propozycje na forum grupy.
- Przećwicz z grupą wybrane gry.

42 Gra planszowa

Cel: rozwijanie kreatywności, przygotowanie gry planszowej dla dzieci, młodzieży.

Przebieg:

- Podziel grupę na mniejsze zespoły (5–6 osobowe). Zadaniem zespołów jest przedstawienie gry planszowej skierowanej do wybranej przez zespół grupy wiekowej. Zakres tematyczny powinien być związany z obszarem zagrożeń cyberprzestrzeni, natomiast założenia – cel, zasady, zadania, grafika są dowolne i zależą od pomysłów zespołu.
- Zaprezentuj pomysły na forum grupy.

43 Bezpieczny smartfon

Cel: praktyczne ćwiczenia procedury bezpiecznego udostępniania sygnału

Przebieg:

Rozpocznij od historyjki:

> Pan Marek jak co miesiąc otrzymał rachunek od swojego operatora telefonii komórkowej. Bardzo zdziwiła go kwota tego rachunku, która zdecydowanie przewyższała jego dotychczasowe rachunki. Pan Marek zadzwonił do Biura Obsługi Klienta operatora komórkowego z pytaniem skąd taki wysoki rachunek. Uzyskał informację, że wysłał kilkanaście esemesów wysokopłatnych. Jego zdziwienie było jeszcze większe, kiedy zobaczył duży ubytek w stanie swojego konta bankowego, do którego dostęp miał również poprzez Internet. Pan Marek padł ofiarą ataku cyberprzestepców.

Co powinien zrobić pan Marek, aby w przyszłości uniknąć takich nieprzyjemnych sytuacji ?

A. Pobierać aplikacje tylko z zaufanych, pewnych i autoryzowanych źródeł.
B. Jeżeli będzie potrzebował pobrać aplikację z niepewnego źródła, to powinien sprawdzić przynajmniej jej uprawnienia.
C. Zainstalować na urządzeniu mobilnym program antywirusowy.
D. Nie korzystać z mobilnego dostępu do banku poprzez smartfon lub tablet.
E. Nie korzystać z aplikacji ściąganych na smartfona lub tablet.

Prawidłowe odpowiedzi A,B,C

Jak to zrobić?

Jedną z bardzo przydatnych funkcji nowoczesnych smartfonów jest możliwość uczynienia z nich przenośnych routerów WiFi. Jest to funkcja umożliwiająca udostępnienie sygnału internetowego dla innego urządzenia.

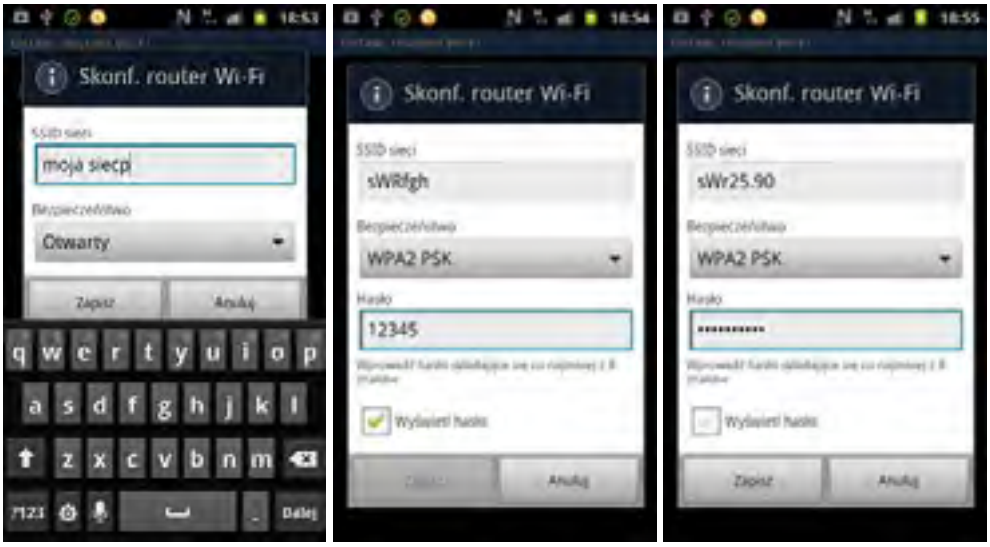
Prześledźmy to na przykładzie systemu Android.

W menu „Ustawienia" i dalej „Komunikacja" należy wybrać „Udostępnianie Internetu".

Następnie należy wybrać sposób udostepnienia transmisji internetowej innemu urządzeniu.
Możliwe są dwa takie sposoby: poprzez kabel USB i poprzez sieć WiFi.

Po wybraniu routera WiFi należy skonfigurować sposób dostępu do sieci.

A B C



Która z powyższych konfiguracji jest najbardziej bezpieczna?

Prawidłowa odpowiedź: C
Wyjaśnienia:
A: nieprawidłowe – zbyt prosta nazwa sieci (SSID sieci) i bezpieczeństwo jako otwarta, czyli całkowicie niezabezpieczona

B: nazwa sieci prawidłowa – trudniejsza, bezpieczeństwo sieci szyfrowane za pomocą protokołu WPA2 PSK, ale zbyt proste hasło

C: dobra nazwa sieci – skomplikowana, bezpieczeństwo sieci szyfrowane za pomocą protokołu WPA2 PSK, dobre hasło o wystarczającej długości oraz zablokowane jego wyświetlanie.

44 Mobile, mobile

Autorem ćwiczenia jest Wojciech Wrzesień

Cel: utrwalenie nazw programów/aplikacji antywirusowych, ćwiczenie rozluźniające.

Przebieg

- Wszyscy uczestnicy siedzą w kręgu. Prowadzący stoi lub siedzi wewnątrz kręgu na krześle. Prowadzący dzieli uczestników na równe grupy, które od tej chwili wchodzą w rolę programu/aplikacji antywirusowej. Prowadzący wymienia wybraną przez siebie nazwę. Wymienione osoby muszą szybko zamienić się miejscami. Na hasło: „Mobile, mobile" (lub inne wcześniej ustalone) wszyscy zamieniają się miejscami, a prowadzący zajmuje dowolne miejsce w kręgu. Ten z uczestników, dla którego zabrakło miejsca w kręgu, zajmuje miejsce w środku i prowadzi zabawę dalej.
- W drugiej części ćwiczenia uczestnicy w grupach (zgodnie z wcześniej przydzieloną nazwą) opracowują i prezentują innym funkcjonalności danej aplikacji, korzystając z zasobów Internetu lub/i materiałów dostarczonych przez prowadzącego.

Przykładowe aplikacje antywirusowe, których nazwy można wykorzystać w ćwiczeniu[10] :
avast! Mobile Security (http://www.avast.com/pl-pl/free-mobile-security)
Norton Mobile Security (http://pl.norton.com/norton-mobile-security/)
AVG Anti-Virus Free (http://www.avg.com/pl-pl/for-mobile)
Zoner AntiVirus (http://www.zonerantivirus.com/)
Lookout Security & Antivirus (https://www.lookout.com/pl)
G Data Internet Security for Android (https://www.gdata.pl/darmowy-download,pobierz-antywirusa,3)
Eset mobile security (http://www.eset.pl/Dla_domu_i_firmy/Produkty/ESET_Mobile_Security_for_Android)

[10] Więcej w rozdziale „Ochrona urządzeń mobilnych"

45 Konflikty

Cel: utrwalenie informacji o rodzajach konfliktów, kształtowanie umiejętności praktycznego zastosowania wiedzy (stosowanie analogii).

Przebieg:

- Zaprezentuj grupie podstawowe rodzaje konfliktów.
- Podziel grupę na mniejsze 3–4 osobowe grupy robocze i poproś, aby w 15 minut przygotowali na piśmie przykładowe konflikty, z jakimi zetknęli się/byli uczestnikami w ostatnim czasie.
- Poproś grupę, aby zastanowiła się, jaki to był typ konfliktu, a swoją odpowiedź uzasadnili.

46 Trudne sytuacje[11]

Cel: utrwalenie wiedzy o sytuacjach konfliktu oraz umiejętności zastosowania teorii w odniesieniu do codziennych sytuacji.

Przebieg:

- Poproś grupę, aby w zespołach 3–4 osobowych zastanowili się, z jakiego rodzaju konfliktem mają do czynienia w przypadku wskazanych poniżej sytuacji (ok. 10 minut):
  - negocjacje między szefem a pracownikiem dotyczące podwyżki w pracy,
  - konflikt pomiędzy rządem a związkami zawodowymi,
  - konflikt pomiędzy sąsiadami – o to, czy psy muszą być wyprowadzane na smyczy,
  - konflikt pomiędzy kierownikami działów – o to, który z działów najpierw powinien dostać wsparcie z działu IT.
- Poproś grupę, aby postarała się znaleźć uzasadnienie dla swoich odpowiedzi.

[11] A. Cybulko, *Konflikt*, w: E. Gmurzyńska, R. Morka (red.), *Mediacje, Teoria i praktyka*, Oficyna Wolters Kluwer Business, Warszawa 2009 , s. 67.

47 Plakat dla rodziców

Cel: utrwalenie wiedzy o stylach rozwiązywania konfliktów**.**

Przebieg:

- Poproś członków grupy, aby w zespołach 3–4 osobowych zastanowili się, jakie są wady i zalety poszczególnych strategii rozwiązywania konfliktów, uzupełniając tabelę (poniżej 15–20 minut).
- Wspólnie omówcie zapisy tabeli, odwołując się także do przykładów z własnego życia.

Plusy +	Minusy -
wycofanie	
uleganie	
rywalizacja	
współpraca	

48 Tematy do dyskusji

Poproś członków grupy, aby

- Wymienili i krótko scharakteryzowali mechanizmy odpowiedzialne za eskalację konfliktu.
- Wyjaśnili, na czym polega cykl konfliktu.
- Podali przykłady zachowań z własnego życia, które mogą prowadzić do eskalacji konfliktu.

BIBILOGRAFIA:

Baer U., *Gry dyskusyjne: materiały pomocnicze do pracy z grupą Lublin* : „Klanza”, Lublin 1997.

Gmurzyńska E., Morka R. (red.), *Mediacje, Teoria i praktyka*, Oficyna Wolters Kluwer Business, Warszawa 2009

Kirby A., *Gry szkoleniowe: materiały dla trenerów*, Wolters Kluwer, Warszawa2011.

Thanhoffer M., *Nauczanie kreatywne*, „Klanza”, Lublin 1997

Vopel Klaus W., *Poradnik dla prowadzących grupy*, Wydawnictwo Jedność, Kielce 1999.

NARZĘDZIA (TESTY I ANKIETY)

NARZĘDZIA
TESTY I ANKIETY

Prosimy o wypełnienie poniższej metryczki oraz testu kompetencyjnego.
Testy mają na celu sprawdzenie kompetencji uczestników programu w momencie ich przystąpienia do programu jak i po jego realizacji. Dane zebrane dzięki ankiecie pozwolą na analizę skutków działania produktu w fazie testowania. Dane te będą prezentowane jako dane zbiorcze (tzn. nigdzie nie będą prezentowane imienne wyniki poszczególnych osób).

PRE-TEST

Imię i Nazwisko .....

Płeć
- ☐ kobieta
- ☐ mężczyzna

Wiek
a) od 25 do 30 lat
b) od 31 do 40 lat
c) od 41 do 50 lat
d) powyżej 50 lat

Staż pracy w służbach społecznych:
a) poniżej 5 lat
b) od 5 do 10 lat
c) od 11 do 20 lat
d) powyżej 20 lat

Wielkość miejsca zamieszkania:
- ☐ wieś
- ☐ miasto do 10 tys. mieszkańców
- ☐ miasto od 10 do 100 tys. mieszkańców
- ☐ miasto od 100 do 500 tys. mieszkańców
- ☐ miasto powyżej 500 tys. mieszkańców

Wykształcenie:
- ☐ średnie
- ☐ wyższe
- ☐ podyplomowe

Który stopień specjalizacji Pan/Pani posiada? (pytanie dotyczy tylko pracowników socjalnych)
- ☐ I stopień specjalizacji
- ☐ II stopień specjalizacji

Jak ocenia Pan/Pani swoją sprawność w posługiwaniu się Internetem?
- ☐ raczej słabo posługuję się Internetem
- ☐ w miarę dobrze posługuję się Internetem
- ☐ bardzo dobrze posługuję się Internetem

Proszę o uzupełnienie lub wybranie w każdym z pytań JEDNEJ, najlepszej odpowiedzi.

1. Twój współpracownik pracujący na komputerze narzeka na „suchość w oku". Co mu radzisz:
.....
.....
.....
.....

2. W Twoim dziale ma być przemeblowanie. Jakie ustawienie biurek/komputerów rekomendujesz?
- ☐ ekrany monitorów komputerowych powinny stać przodem do okna
- ☐ ekrany monitorów komputerowych nie powinny stać przodem do okna
- ☐ dla komfortu pracy przy komputerze nie ma znaczenia, czy stoi on ekranem monitora do okna czy nie

3. Twoi współpracownicy skarżą się na bóle kręgosłupa od pracy przy komputerze. Jakie najważniejsze rzeczy zalecisz im do sprawdzenia, aby upewnili się, że ich krzesło biurowe jest ergonomiczne:
- ☐ czy krzesło jest miękkie, ma regulowaną wysokość siedziska i podłokietniki
- ☐ czy krzesło ma regulowaną wysokość siedziska, podłokietniki i regulację pochylenia oparcia
- ☐ czy krzesło ma zagłówek, możliwość obrotu o 360 stopni i regulowaną wysokość siedziska

4. Zgłasza się do Ciebie osoba, która mówi, że nie jest w stanie kontrolować ilości czasu spędzanego przy komputerze i coraz gorzej to wpływa na jej życie osobiste i zawodowe. U jakiego specjalisty doradzisz jej wizytę?

- ☐ u psychiatry, gdyż uzależnienie od Internetu jest uznane za jednostkę chorobową
- ☐ u psychologa, gdyż uzależnienie od Internetu nie jest uznane za jednostkę chorobową
- ☐ u socjologa, gdyż uzależnienie od Internetu wynika z czynników społecznych

5. Zgłaszają się do Ciebie rodzice dziewczynki nękanej przez koleżanki z klasy, które zamieszczają w Internecie na jej profilu wulgarne wpisy. Jak wyjaśniasz sytuację prawną ich córki i jakie dasz rady jej rodzicom?

- ☐ zwrócenie się z prośbą do rodziców nękających ją koleżanek, aby przestały ją nękać (ponieważ rodzice nie mogą zagrozić im pozwem, gdyż nie istnieją przepisy prawne dotyczące cyberprzemocy)
- ☐ zwrócenie się z żądaniem do rodziców nękających ją koleżanek, dotyczącym natychmiastowego zaprzestania nękania ich córki, gdyż w przeciwnym razie złożą przeciwko nim pozew na podstawie przepisów Kodeksu cywilnego
- ☐ zagrożenie rodzicom, że jak tylko ich córka skończy 18 lat, to wytoczy im proces na podstawie Kodeksu cywilnego za obecne nękanie (ponieważ w takiej sytuacji podlega się ochronie prawnej dopiero po osiągnięciu pełnoletności, ale mobbing nie podlega przedawnieniu)

6. Zgłasza się do Ciebie z prośbą o poradę dziewczyna (18 lat), której były chłopak (również 18 lat) umieścił na swojej stronie internetowej filmik przedstawiający, jak uprawiali seks. Jak wyjaśniasz sytuację prawną takiej osoby i jakie dasz jej rady?

- ☐ mówisz jej, że skoro jest osobą pełnoletnią i wówczas wyraziła zgodę na nagranie tego filmu, prawo już jej nie chroni
- ☐ sugerujesz jej, aby wezwała swojego byłego chłopaka (najlepiej na piśmie) do natychmiastowego usunięcia filmu z jego strony internetowej oraz zaprzestania rozpowszechniania go, gdyż w przeciwnym wypadku złoży przeciwko niemu pozew sądowy
- ☐ sugerujesz jej zwrócenie się do dyrektora szkoły, w której jej były chłopak uczy się, aby dyrektor wymusił na nim usunięcie filmu pod groźbą wyrzucenia go ze szkoły

7. Zauważyłaś/łeś, że na swoim profilu społecznościowym jedna ze znajomych matek umieszcza zdjęcia swojego małego dziecka. Na niektórych zdjęciach dziecko jest nagie. Co robisz?

- ☐ uznajesz, że nie wolno ci ingerować, gdyż każdy rodzic sam decyduje o tym, jakie zdjęcia swojego dziecka prezentuje
- ☐ zgłaszasz od razu sprawę na policję, aby drogą formalną wezwała ją do usunięcia tych zdjęć
- ☐ spotykasz się z tą matką i tłumaczysz jej, że takie zdjęcia są pożywką dla pedofilów oraz naruszeniem prawa i namawiasz do natychmiastowego usunięcia tych zdjęć

8. Widzisz, jak 10–letnie dzieci podczas zabawy naśladują zachowania seksualne. Co robisz?

- ☐ mówisz dzieciom, że takie zachowanie jest bardzo złe i nie wolno im tak więcej robić
- ☐ rozmawiasz o tym z rodzicami dzieci
- ☐ pytasz nauczycieli, czy dzieci miały już jakieś zajęcia w szkole na temat prokreacji

9. Zgłasza się do Ciebie z prośbą o radę kobieta, która odkryła, że jej 13-letnia córka zamieściła na swoim profilu na portalu społecznościowym zdjęcia w kostiumie kąpielowym. Co jej radzisz?

- ☐ aby zmusiła córkę do usunięcia swojego profilu
- ☐ aby wyjaśniła córce, że jeśli coś raz wrzuci do Internetu, to straci nad tym kontrolę i powinna natychmiast usunąć te zdjęcia oraz nie umieszczać podobnych zdjęć w przyszłości
- ☐ mówisz, że nie ma powodów do obaw, gdyż dużo dzieci w jej wieku zamieszcza takie swoje zdjęcia

10. Nauczyciel zauważył, że jedna z dziewcząt zaczęła ubierać się w stroje ze sklepu z hinduską odzieżą i przestała jeść mięso. Prosi Cię o radę. Co mu powiesz?

- ☐ aby prosił katechetę, by podczas lekcji religii powiedział o sektach
- ☐ aby powiedział jej, że padła ofiarą sekty, która „zrobi jej pranie mózgu" i musi natychmiast z tym skończyć
- ☐ że nie może wnioskować o przynależności do sekty tylko z powodu czyjegoś stylu odżywania ani ze stroju

11. Zgłasza się do Ciebie rodzic, który postanawia zakazać swojemu 7-letniemu dziecku gry na komputerze, gdyż boi się, że trafi ono na przemoc, wulgarny język itp. Co robisz?

- ☐ mówisz rodzicowi, iż całkowity zakaz gier na komputerze nie jest dobrym pomysłem i sugerujesz, aby kupując gry zwracał uwagę na oznaczenia, jakie znajdują się na pudełkach gier
- ☐ mówisz rodzicowi, że to bardzo dobry pomysł, gdyż w ten sposób najlepiej uchroni swoje dziecko przed niechcianymi treściami
- ☐ mówisz rodzicowi, że nie powinien ograniczać dziecku gier komputerowych, gdyż będzie ono czuło się wyalienowane – inne dzieci przecież w nie grają

12. W okolicznej szkole wybuchł skandal związany z tym, że podczas zajęć z informatyki uczniowie grali w brutalne gry (które sami zainstalowali na szkolnych komputerach). Dyrekcja szkoły zamierza ukarać grających zawieszeniem w prawach ucznia oraz poinformowaniem o tej karze wszystkich uczniów, ale chcą jeszcze usłyszeć Twoją opinię w tej sprawie.

- ☐ popierasz to rozwiązanie, gdyż dzięki surowej i publicznie nagłośnionej karze takie przypadki nie będą się już zdarzać, a równocześnie sprawcy tego czynu zostaną ukarani
- ☐ zachęcasz dyrekcję szkoły, aby wyciszyła tę sprawę, gdyż negatywny rozgłos zaszkodzi wizerunkowi szkoły, a rodzice uczniów mogą stracić zaufanie do nauczycieli
- ☐ zachęcasz dyrekcję szkoły, aby wspólnie z pedagogiem szkolnym (lub inną osobą posiadającą odpowiednią wiedzę) przygotowali scenariusz lekcji związanej z niebezpieczeństwami związanymi z brutalnymi grami komputerowymi i przeprowadzili je we wszystkich klasach

13. Jesteś świadkiem, jak dziecko wpada w histerię, gdy jego rodzic zabiera mu smartfona, gdyż dziecko było całkowicie pochłonięte grą i nie zwracało uwagi, co rodzic do niego mówił. Co robisz?

- ☐ mówisz rodzicowi, że takie zachowanie to przemoc wobec dziecka i może być za takie zachowanie ukarany, gdyż smartfon należy do dziecka i rodzic powinien ten fakt uszanować
- ☐ mówisz rodzicowi, że powinien udać się z dzieckiem do lekarza, gdyż może ono cierpieć na ADHD – stąd histeryczna reakcja dziecka
- ☐ mówisz rodzicowi, że tak histeryczne zachowanie może być objawem uzależnienia od gier komputerowych i warto, aby porozmawiał o tym z psychoterapeutą

14. Zauważasz, że w świetlicy jeden z nastolatków codziennie spędza całe wieczory przy komputerze – nie robiąc nawet krótkich przerw. Co robisz:

- ☐ sprawdzasz po jego wyjściu, czy nie wchodził na treści zakazane (np. pornograficzne). Jeśli nie – to wszystko w porządku
- ☐ mówisz temu nastolatkowi, że nie może tyle czasu spędzać przy komputerze, gdyż powinien on być dostępny dla innych
- ☐ kontaktujesz się z rodzicami tego nastolatka, mówisz o jego zachowaniu i pytasz, czy ich zdaniem może on być uzależniony od Internetu. Jeśli tak, sugerujesz rodzicom rozmowę z nastolatkiem – w razie potrzeby w obecności psychoterapeuty

15. Które z poniższych zachowań w największym stopniu wskaże Ci, że dana osoba może być uzależniona od komputera?

- ☐ wydaje dużo pieniędzy na sprzęt komputerowy i gadżety IT
- ☐ okłamuje innych co do czasu, jaki spędza przy komputerze (tzn. deklaruje, że spędza mniej czasu przy komputerze niż w rzeczywistości)
- ☐ spędza dużo czasu przy komputerze, jest na bieżąco ze wszystkimi nowinkami technicznymi

16. Osoba próbująca zalogować się na bankowym koncie internetowym otrzymuje komunikat, żeby podała swój PIN. Osoba ta prosi Cię o radę, czy ma to zrobić. Co jej radzisz?

- ☐ mówisz, że skoro na tej stronie jest logo banku i strona wygląda tak samo jak zawsze, to powinna podać PIN – bo transakcje na stronach banku mają dobre zabezpieczenia
- ☐ mówisz, że banki nie proszą przy logowaniu o podanie PIN–u, więc jest to podejrzana operacja i nie powinna podać tego numeru
- ☐ radzisz, aby jeszcze raz spróbowała się zalogować na tej stronie

17. Ktoś prosi Cię o pomoc przy wypełnieniu internetowego formularza, w którym trzeba podać dane osobowe. Problem polega na tym, że przy pasku adresowym w przeglądarce pojawiła się zielona kłódeczka i osoba ta nie wie, co to znaczy. Jakiego wyjaśnienia jej udzielisz?

- ☐ zielona kłódeczka oznacza, że połączenie z tą witryną jest bezpieczne i może ona kontynuować wypełnianie formularza
- ☐ zielona kłódeczka oznacza, że ktoś się w tym momencie próbuje włamać do komputera i trzeba szybko wyjść z Internetu
- ☐ zielona kłódeczka oznacza, że za chwilę osoba ta otrzyma swoje indywidualne hasło, które będzie jej potrzebne przy kolejnym logowaniu się do tego formularza

18. Twój znajomy dostał e-mail od swojego banku, w którym proszą go o podanie danych do konta internetowego w celu weryfikacji jego tożsamości, gdyż inaczej zostanie mu zablokowany dostęp do tego konta. Co mu radzisz?

- ☐ powinien podać te dane, gdyż skoro jego bank wysłał ten e–mail właśnie do niego, to dane te będą chronione
- ☐ nie podawać żadnych danych i skontaktować się z bankiem
- ☐ powinien najpierw poprosić, aby podano mu numer infolinii, pod którą będzie mógł upewnić się o celu tej procedury

19. Zgłasza się do Ciebie osoba, która zorientowała się, że dziś z jej karty kredytowej została wykonana transakcja zakupu na 150 zł, której ona nie zleciła. Co jej radzisz?

- ☐ mówisz, że przy kradzieży pieniędzy na tak małą kwotę nic już nie może zrobić (tzw. niska szkodliwość społeczna)
- ☐ mówisz, żeby szybko skontaktowała się z bankiem i zgłosiła, że to nie ona wykonała transakcję
- ☐ mówisz, żeby szybko skontaktowała się z firmą, w której dokonano zakupu z jej konta i poprosiła ich o zwrot tych pieniędzy, gdyż ona tego zakupu nie zlecała

20. Współpracownik prosi Cię o doradzenie, jakiego typu hasło do służbowego komputera powinien wymyślić. Co mu radzisz?

- ☐ aby jego hasło było łatwe dla niego do zapamiętania (np. imię psa, miejsce urodzin czy ulubiona potrawa), aby nie musiał go nigdzie zapisywać
- ☐ aby jego hasło zawierało duże i małe litery oraz cyfry i znaki specjalne
- ☐ aby jego hasło do komputera służbowego było takie samo, jak do maila prywatnego, gdyż wtedy nie będzie mylił się przy logowaniu

Dziękujemy za wypełnienie testu.

Opracowała: Anna Daria Nowicka

Prosimy o wypełnienie poniższej metryczki oraz testu kompetencyjnego.
Testy mają na celu sprawdzenie kompetencji uczestników programu w momencie ich przystąpienia do programu, jak i po jego realizacji. Dane zebrane dzięki ankiecie pozwolą na analizę skutków działania produktu w fazie testowania. Dane te będą prezentowane jako dane zbiorcze (tzn. nigdzie nie będą prezentowane imienne wyniki poszczególnych osób).

POST-TEST

Imię i Nazwisko ……

Proszę o uzupełnienie lub wybranie w każdym z pytań JEDNEJ, najlepszej odpowiedzi.

1. Twój współpracownik pracujący na komputerze narzeka na „suchość w oku". Co mu radzisz:
……
……
……
……

2. W Twoim dziale ma być przemeblowanie. Jakie ustawienie biurek/komputerów rekomendujesz?
- ☐ ekrany monitorów komputerowych powinny stać przodem do okna
- ☐ ekrany monitorów komputerowych nie powinny stać przodem do okna
- ☐ dla komfortu pracy przy komputerze nie ma znaczenia, czy stoi on ekranem monitora do okna, czy nie

3. Twoi współpracownicy skarżą się na bóle kręgosłupa od pracy przy komputerze. Jakie najważniejsze rzeczy zalecisz im do sprawdzenia, aby upewnili się, że ich krzesło biurowe jest ergonomiczne:
- ☐ czy krzesło jest miękkie, ma regulowaną wysokość siedziska i podłokietniki
- ☐ czy krzesło ma regulowaną wysokość siedziska, podłokietniki i regulację pochylenia oparcia
- ☐ czy krzesło ma zagłówek, możliwość obrotu o 360 stopni i regulowaną wysokość siedziska

4. Zgłasza się do Ciebie osoba, która mówi, że nie jest w stanie kontrolować ilości czasu spędzanego przy komputerze i coraz gorzej to wpływa na jej życie osobiste i zawodowe. U jakiego specjalisty doradzisz jej wizytę?
- ☐ u psychiatry, gdyż uzależnienie od Internetu jest uznane za jednostkę chorobową
- ☐ u psychologa, gdyż uzależnienie od Internetu nie jest uznane za jednostkę chorobową
- ☐ u socjologa, gdyż uzależnienie od Internetu wynika z czynników społecznych

5. Zgłaszają się do Ciebie rodzice dziewczynki nękanej przez koleżanki z klasy, które zamieszczają w Internecie na jej profilu wulgarne wpisy. Jak wyjaśniasz sytuację prawną ich córki i jakie dasz rady jej rodzicom?
- ☐ zwrócenie się z prośbą do rodziców nękających ją koleżanek, aby przestały ją nękać (ponieważ rodzice nie mogą zagrozić im pozwem, gdyż nie istnieją przepisy prawne dotyczące cyberprzemocy)
- ☐ zwrócenie się z żądaniem do rodziców nękających ją koleżanek, dotyczącym natychmiastowego zaprzestania nękania ich córki, gdyż w przeciwnym razie złożą przeciwko nim pozew na podstawie przepisów Kodeksu cywilnego
- ☐ zagrożenie rodzicom, że jak tylko ich córka skończy 18 lat, to wytoczy im proces na podstawie Kodeksu Cywilnego za obecne nękanie (ponieważ w takiej sytuacji podlega się ochronie prawnej dopiero po osiągnięciu pełnoletności, ale mobbing nie podlega przedawnieniu)

6. Zgłasza się do Ciebie z prośbą o poradę dziewczyna (18 lat), której były chłopak (również 18 lat) umieścił na swojej stronie internetowej filmik przedstawiający, jak uprawiali seks. Jak wyjaśniasz sytuację prawną takiej osoby i jakie dasz jej rady?

- ☐ mówisz jej, że skoro jest osobą pełnoletnią i wówczas wyraziła zgodę na nagranie tego filmu, prawo już jej nie chroni
- ☐ sugerujesz jej, aby wezwała swojego byłego chłopaka (najlepiej na piśmie) do natychmiastowego usunięcia filmu z jego strony internetowej oraz zaprzestania rozpowszechniania go, gdyż w przeciwnym wypadku złoży przeciwko niemu pozew sądowy
- ☐ sugerujesz jej zwrócenie się do dyrektora szkoły, w której jej były chłopak uczy się, aby dyrektor wymusił na nim usunięcie filmu pod groźbą wyrzucenia go ze szkoły

7. Zauważyłaś/łeś, że na swoim profilu społecznościowym jedna ze znajomych matek umieszcza zdjęcia swojego małego dziecka. Na niektórych zdjęciach dziecko jest nagie. Co robisz?

- ☐ uznajesz, że nie wolno ci ingerować, gdyż każdy rodzic sam decyduje o tym, jakie zdjęcia swojego dziecka prezentuje
- ☐ zgłaszasz od razu sprawę na policję, aby drogą formalną wezwała ją do usunięcia tych zdjęć
- ☐ spotykasz się z tą matką i tłumaczysz jej, że takie zdjęcia są pożywką dla pedofilów oraz naruszeniem prawa i namawiasz do natychmiastowego usunięcia tych zdjęć

8. Widzisz, jak 10-letnie dzieci podczas zabawy naśladują zachowania seksualne. Co robisz?

- ☐ mówisz dzieciom, że takie zachowanie jest bardzo złe i nie wolno im tak więcej robić
- ☐ rozmawiasz o tym z rodzicami dzieci pytasz nauczycieli, czy dzieci miały już jakieś zajęcia w szkole na temat prokreacji

9. Zgłasza się do Ciebie z prośbą o radę kobieta, która odkryła, że jej 13-letnia córka zamieściła na swoim profilu na portalu społecznościowym zdjęcia w kostiumie kąpielowym. Co jej radzisz?

- ☐ aby zmusiła córkę do usunięcia swojego profilu
- ☐ aby wyjaśniła córce, że jeśli coś raz wrzuci do Internetu, to straci nad tym kontrolę i powinna natychmiast usunąć te zdjęcia oraz nie umieszczać podobnych zdjęć w przyszłości
- ☐ mówisz, że nie ma powodów do obaw, gdyż dużo dzieci w jej wieku zamieszcza takie swoje zdjęcia

10. Nauczyciel zauważył, że jedna z dziewcząt zaczęła ubierać się w stroje ze sklepu z hinduską odzieżą i przestała jeść mięso. Prosi Cię o radę. Co mu powiesz?

- ☐ aby prosił katechetę, by podczas lekcji religii powiedział o sektach
- ☐ aby powiedział jej, że padła ofiarą sekty, która „zrobi jej pranie mózgu" i musi natychmiast z tym skończyć
- ☐ że nie może wnioskować o przynależności do sekty tylko z powodu czyjegoś stylu odżywiania ani stroju

11. Zgłasza się do Ciebie rodzic, który postanawia zakazać swojemu 7-letniemu dziecku gry na komputerze, gdyż boi się, że trafi ono na przemoc, wulgarny język itp. Co robisz?

- ☐ mówisz rodzicowi, iż całkowity zakaz gier na komputerze nie jest dobrym pomysłem i sugerujesz, aby kupując gry zwracał uwagę na oznaczenia, jakie znajdują się na pudełkach gier
- ☐ mówisz rodzicowi, że to bardzo dobry pomysł, gdyż w ten sposób najlepiej uchroni swoje dziecko przed niechcianymi treściami
- ☐ mówisz rodzicowi, że nie powinien ograniczać dziecku gier komputerowych, gdyż będzie ono czuło się wyalienowane – inne dzieci przecież w nie grają

12. W okolicznej szkole wybuchł skandal związany z tym, że podczas zajęć z informatyki uczniowie grali w brutalne gry (które sami zainstalowali na szkolnych komputerach). Dyrekcja szkoły zamierza ukarać grających zawieszeniem w prawach ucznia oraz poinformowaniem o tej karze wszystkich uczniów, ale chcą jeszcze usłyszeć Twoją opinię w tej sprawie.

- ☐ popierasz to rozwiązanie, gdyż dzięki surowej i publicznie nagłośnionej karze takie przypadki nie będą się już zdarzać, a równocześnie sprawcy tego czynu zostaną ukarani
- ☐ zachęcasz dyrekcję szkoły, aby wyciszyła tę sprawę, gdyż negatywny rozgłos zaszkodzi wizerunkowi szkoły, a rodzice uczniów mogą stracić zaufanie do nauczycieli
- ☐ zachęcasz dyrekcję szkoły, aby wspólnie z pedagogiem szkolnym (lub inną osobą posiadającą odpowiednią wiedzę) przygotowali scenariusz lekcji związanej z niebezpieczeństwami związanymi z brutalnymi grami komputerowymi i przeprowadzili je we wszystkich klasach

13. Jesteś świadkiem, jak dziecko wpada w histerię, gdy jego rodzic zabiera mu smartfona, gdyż dziecko było całkowicie pochłonięte grą i nie zwracało uwagi, co rodzic do niego mówił. Co robisz?

- ☐ mówisz rodzicowi, że takie zachowanie to przemoc wobec dziecka i może być za takie zachowanie ukarany, gdyż smartfon należy do dziecka i rodzic powinien ten fakt uszanować
- ☐ mówisz rodzicowi, że powinien udać się z dzieckiem do lekarza, gdyż może ono cierpieć na ADHD – stąd histeryczna reakcja dziecka
- ☐ mówisz rodzicowi, że tak histeryczne zachowanie może być objawem uzależnienia od gier komputerowych i warto, aby porozmawiał o tym z psychoterapeutą

14. Zauważasz, że w świetlicy jeden z nastolatków codziennie spędza całe wieczory przy komputerze – nie robiąc nawet krótkich przerw. Co robisz:

- ☐ sprawdzasz po jego wyjściu, czy nie wchodził na treści zakazane (np. pornograficzne). Jeśli nie – to wszystko w porządku
- ☐ mówisz temu nastolatkowi, że nie może tyle czasu spędzać przy komputerze, gdyż powinien on być dostępny dla innych
- ☐ kontaktujesz się z rodzicami tego nastolatka, mówisz o jego zachowaniu i pytasz, czy ich zdaniem może on być uzależniony od Internetu. Jeśli tak, sugerujesz rodzicom rozmowę z nastolatkiem – w razie potrzeby w obecności psychoterapeuty

15. Które z poniższych zachowań w największym stopniu wskaże Ci, że dana osoba może być uzależniona od komputera?

- ☐ wydaje dużo pieniędzy na sprzęt komputerowy i gadżety IT
- ☐ okłamuje innych co do czasu, jaki spędza przy komputerze (tzn. deklaruje, że spędza mniej czasu przy komputerze niż w rzeczywistości)
- ☐ spędza dużo czasu przy komputerze, jest na bieżąco ze wszystkimi nowinkami technicznymi

16. Osoba próbująca zalogować się na bankowym koncie internetowym otrzymuje komunikat, żeby podała swój PIN. Osoba ta prosi Cię o radę, czy ma to zrobić. Co jej radzisz?

- ☐ mówisz, że skoro na tej stronie jest logo banku i strona wygląda tak samo jak zawsze, to powinna podać PIN – bo transakcje na stronach banku mają dobre zabezpieczenia
- ☐ mówisz, że banki nie proszą przy logowaniu o podanie PIN–u, więc jest to podejrzana operacja i nie powinna podać tego numeru
- ☐ radzisz, aby jeszcze raz spróbowała się zalogować na tej stronie

17. Ktoś prosi Cię o pomoc przy wypełnieniu internetowego formularza, w którym trzeba podać dane osobowe. Problem polega na tym, że przy pasku adresowym w przeglądarce pojawiła się zielona kłódeczka i osoba ta nie wie, co to znaczy. Jakiego wyjaśnienia jej udzielisz?
- ☐ zielona kłódeczka oznacza, że połączenie z tą witryną jest bezpieczne i może ona kontynuować wypełnianie formularza
- ☐ zielona kłódeczka oznacza, że ktoś się w tym momencie próbuje włamać do komputera i trzeba szybko wyjść z Internetu
- ☐ zielona kłódeczka oznacza, że za chwilę osoba ta otrzyma swoje indywidualne hasło, które będzie jej potrzebne przy kolejnym logowaniu się do tego formularza

18. Twój znajomy dostał e-mail od swojego banku, w którym proszą go o podanie danych do konta internetowego w celu weryfikacji jego tożsamości, gdyż inaczej zostanie mu zablokowany dostęp do tego konta. Co mu radzisz?
- ☐ powinien podać te dane, gdyż skoro jego bank wysłał ten e-mail właśnie do niego, to dane te będą chronione
- ☐ nie podawać żadnych danych i skontaktować się z bankiem
- ☐ powinien najpierw poprosić, aby podano mu numer infolinii, pod którą będzie mógł upewnić się o celu tej procedury

19. Zgłasza się do Ciebie osoba, która zorientowała się, że dziś z jej karty kredytowej została wykonana transakcja zakupu na 150 zł, której ona nie zleciła. Co jej radzisz?
- ☐ mówisz, że przy kradzieży pieniędzy na tak małą kwotę nic już nie może zrobić (tzw. niska szkodliwość społeczna)
- ☐ mówisz, żeby szybko skontaktowała się z bankiem i zgłosiła, że to nie ona wykonała transakcję
- ☐ mówisz, żeby szybko skontaktowała się z firmą, w której dokonano zakupu z jej konta i poprosiła ich o zwrot tych pieniędzy, gdyż ona tego zakupu nie zlecała

20. Współpracownik prosi Cię o doradzenie, jakiego typu hasło do służbowego komputera powinien wymyślić. Co mu radzisz?
- ☐ aby jego hasło było łatwe dla niego do zapamiętania (np. imię psa, miejsce urodzin czy ulubiona potrawa), aby nie musiał go nigdzie zapisywać
- ☐ aby jego hasło zawierało duże i małe litery oraz cyfry i znaki specjalne
- ☐ aby jego hasło do komputera służbowego było takie samo, jak do e-maila prywatnego, gdyż wtedy nie będzie mylił się przy logowaniu

Dziękujemy za wypełnienie testu.

Opracowała: Anna Daria Nowicka

ANKIETA EWALUACYJNA SZKOLENIA

1. Płeć

- mężczyzna
- kobieta

2. Jaką instytucję Pan(i) reprezentuje?

- Ośrodek pomocy społecznej
- Dom pomocy społecznej
- Świetlica środowiskowa
- Placówka opiekuńczo-wychowawcza
- Dom dziecka
- Organizacja pozarządowa
- Firma prywatna
- Inna instytucja: **jaka?** _____

3. Proszę powiedzieć, od ilu lat pracuje Pan(i) jako pracownik służb społecznych?

- od 5 lat lub krócej
- od 6 do 10 lat
- od 11 do 20 lat
- od 21 lat lub dłużej

Otrzymał/a Pan(i) produkt, który powstał w ramach Projektu pt.: „PI-PWP Zagrożenia cyberprzestrzeni – nowe kompetencje pracownika socjalnego", bardzo prosimy o wyrażenie opinii na jego temat w następujących obszarach:

4. Jak ocenia Pan(i) poniższe aspekty dotyczące programu szkolenia?

	1 - Bardzo słabo	2	3	4	5 - Bardzo dobrze
Kompletność (tematyka)					
Komplementarność (zakres materiału)					
Użyteczność (zdobycie nowej wiedzy)					
Uzyskanie nowych umiejętności					
Przydatność w dalszej karierze zawodowej					
Poziom merytoryczny materiałów szkoleniowych otrzymanych w czasie szkolenia					

5. Jak ocenia Pan(i) prowadzącego szkolenie?

	1 - Bardzo słabo	2	3	4	5 - Bardzo dobrze
Znajomość tematu, przygotowanie merytoryczne	■	■	■	■	■
Sposób przekazywania informacji (przystępny, klarowny?)	■	■	■	■	■
Tempo szkolenia	■	■	■	■	■
Dbanie o dobrą atmosferę podczas szkolenia	■	■	■	■	■
Proporcja między częścią wykładową a ćwiczeniową	■	■	■	■	■
Jakość prezentacji	■	■	■	■	■
Współpraca z prowadzącym	■	■	■	■	■
Ogólna ocena prowadzącego szkolenie	■	■	■	■	■

6. Jak ocenia Pan(i) kryteria innowacyjności produktu?

	1 - Bardzo słabo	2	3	4	5 - Bardzo dobrze
Przedstawia nowy obszar zagrożeń	■	■	■	■	■
Kompleksowo traktuje problematykę	■	■	■	■	■
Proponuje krótko i długofalowe działania społeczne i edukacyjne	■	■	■	■	■
Wielowątkowo odpowiada na potrzeby pracowników socjalnych	■	■	■	■	■
Ma charakter interdyscyplinarny – łączy zagadnienia polityki społecznej, pracy socjalnej i pedagogiki z innymi obszarami, takimi jak informatyka oraz prawo	■	■	■	■	■

7. Czy Pan(i) zdaniem zostały zrealizowane następujące cele:

	tak	nie
Poznawczy: zapoznaje z wiedzą dot. zagrożeń cyberprzestrzeni	■	■
Kształcący: pozwala przygotować pracowników kadr służb społecznych do rozpoznawania nowych zagrożeń spowodowanych przez cyberprzestrzeń i przeciwdziałania ich skutkom społecznym	■	■
Wychowawczy: kształtuje świadomość społeczną wśród pracowników służb społecznych na temat miejsca i znaczenia zagrożeń powodowanych przez cyberprzestrzeń	■	■

8. Program był:

■ zbyt przeładowany

■ odpowiedni

■ za mało nasycony

9. Szkolenie trwało:

- ☐ zbyt długo
- ☐ w sam raz
- ☐ zbyt krótko

10. Dzięki szkoleniu:

	tak	nie	nie mam zdania
Rozumiem istniejące zagrożenia	☐	☐	☐
Wiem, jak rozpoznawać zagrożenia	☐	☐	☐
Wiem, jakie są metody diagnozowania zagrożeń	☐	☐	☐
Posiadam wiedzę na temat dobrych praktyk unikania zagrożeń	☐	☐	☐
Wymieniłem/am się doświadczeniami z innymi uczestnikami szkolenia	☐	☐	☐
Nawiązałem/am ciekawe kontakty	☐	☐	☐

11. Jakie zagadnienia chciałbyś/łabyś rozwinąć/poruszyć na następnym szkoleniu?

……

……

12. Podczas szkolenia najbardziej podobało mi się:

……

……

13. Podczas szkolenia przede wszystkim zabrakło mi:

……

……

14. Czy ogólnie rzecz biorąc jesteś zadowolony/a ze szkolenia?

- ☐ Zdecydowanie tak
- ☐ Raczej tak
- ☐ Raczej nie
- ☐ Zdecydowanie nie

Opracowała: Karolina Geletta

ZAŁĄCZNIKI

ZAŁĄCZNIK 1

WYBRANE FORMALNO-PRAWNE PODSTAWY POLITYKI SPOŁECZNEJ

Józef Bednarek

1 WPROWADZENIE

W poniższych dokumentach podkreślono rolę i miejsce najnowszych mediów cyfrowych, technologii interaktywnych w badaniach i kształcenia w zakresie polityki społecznej, edukacji cyfrowej, życia społecznego, gospodarki oraz znaczenie nowych kompetencji społeczno-komunikacyjnych, medialnych i informacyjno-komunikacyjnych we współczesnym świecie. Należą do nich:

2 STRATEGIE ROZWOJOWE UE

1. *Komunikat Komisji Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów,* nt. *Europejskiego podejścia do umiejętności korzystania z mediów w środowisku cyfrowym* z 20.12.2007 r.
2. *Zalecenie Komisji Parlamentu Europejskiego w sprawie umiejętności korzystania z mediów w środowisku cyfrowym* w celu stworzenia bardziej konkurencyjnego sektora audiowizualnego i treści cyfrowych oraz stworzenia integracyjnego społeczeństwa opartego na wiedzy z dnia 20.08.2009 r.
3. *Strategia „Europa 2020"* zmierzająca do wyjścia z kryzysu i mająca przygotować unijną gospodarkę na wyzwania następnego dziesięciolecia. Nakreślono w niej wizję wysokiego poziomu zatrudnienia, gospodarki niskoemisyjnej, wydajności i spójności społecznej, które mają zostać osiągnięte na szczeblu unijnym i krajowym[1].
4. *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejskiej Agendy Cyfrowej*, na podstawie którego przygotowano *Program rozwoju społeczeństwa informacyjnego w Unii Europejskiej w latach 2010–2015*. Przedstawiona w nim strategia „… zmierza do wyjścia z kilkuletniego kryzysu i jest podstawą przygotowania unijnej gospodarki na wyzwania następnego dziesięciolecia. Nakreślono w niej wizję wysokiego poziomu zatrudnienia, gospodarki niskoemisyjnej, wydajności i spójności społecznej, który ma zostać osiągnięty poprzez konkretne działania na szczeblach unijnych i krajowym"[2].
5. *Komunikat Komisji Parlamentu Europejskiego, Rady Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, Europejskie podejście do umiejętności korzystania z mediów w środowisku cyfrowym,* Komisja Wspólnot Europejskich, Bruksela, 20.12.2007 r.
6. *Dyrektywa 2011/92/UE Parlamentu Europejskiego i Rady* z dnia 13 grudnia 2013 r. w sprawie zwalczania nielegalnego traktowania w celach seksualnych i wykorzystania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz. Urz. L. 335 z dnia 17 grudnia 2011).
7. W 2009 r. UE znowelizowała ramy regulacyjne łączności elektronicznej, a w 2010 r. ogłosiła Europejską Agencję Cyfrową, która stanowi jedną z 7 inicjatyw flagowych „Europy 2020" – dziesięcioletniej unijnej strategii na rzecz wzrostu[3]. W strategii tej zwrócono uwagę na rozwój w UE, który ma być nie tylko zrównoważony i sprzyjający włączeniu społecznemu, a może przede wszystkim, rozwój ten może

[1] *Strategia Europa 2020* została przedstawiona przez Komisję Europejską w marcu 2010 r.

[2] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-społecznego i Komitetu Regionów,* Europejska Agenda Cyfrowa, Bruksela, 19.05.2010, Ministerstwo Spraw Wewnętrznych, czerwiec 2010, s. 3.

[3] K. Ławniczak, *Jednolity rynek łączności elektronicznej UE, jako fundament EAC. Reforma regulacji z 2009,* „Przegląd Europejski", 2 (25), s. 65–84.

też być inteligentny”[4]. Eksponuje się zatem badania naukowe i innowacje technologiczne oraz inne działania przygotowujące grunt pod przekształcanie gospodarki przemysłowej w gospodarkę opartą na wiedzy, a więc taką, w której wiedza, obok kapitału i pracy, posiada wartość jako środek produkcji i źródło dobrobytu. Powstają nowe wcześniej nieznane cyfrowe usługi i urządzenia, np. literatura i muzyka w postaci cyfrowej dostępna będzie za pośrednictwem Internetu.

3 W dokumencie tym Komisja Europejska określa siedem najważniejszych obszarów problemowych:

1. Dynamiczny jednolity rynek cyfrowy.
2. Interoperacyjność i normy, chodzi o zapewnienie interoperacyjności urządzeń, usług, aplikacji i baz danych.
3. Zaufanie i bezpieczeństwo, w elektronicznej UE, jako fundament Europejskiej Agendy, której celem jest unowocześnienie Europejskiej Agencji Bezpieczeństwa Sieci i Informacji, utworzonej w 2004 r.
4. Szybki i bardzo szybki dostęp do Internetu w przystępnej cenie.
5. Badania i innowacje, mające na celu minimalizowanie zbyt dużego dysonansu między UE a USA. W tym celu niezbędna jest nowa, tym razem cyfrowa alfabetyzacja. Chodzi także o opracowanie mechanizmów uznawania kwalifikacji w dziedzinie TIK i wskaźników kompetencji informatycznych.
6. Zwiększenie umiejętności wykorzystania technologii cyfrowych włączenia społecznego.
7. Korzyści z TIK dla społeczeństwa UE [5].

[4] J. M. Durao Barroso, Słowo wstępne, w: *Komunikat Komisji „Europa 2020”. Strategie na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu,* Komisja Europejska, KOM (2010) 2020 wersja ostateczna.

[5] Tamże, s. 8–39.

Potrzebę realizacji polityki społecznej i działalności w zakresie pracy socjalnej sankcjonują także następujące dokumenty, raporty, strategie itp., które pogrupowano w pięciu zasadniczych obszarach:

4 DOKUMENTY I RAPORTY EDUKACYJNE UE

1. Raport Jacgues`a Delorsa.
2. Raport Martina Bangenmanna.
3. Biała Księga Komisji Europejskiej.
4. Raport „Przyszłość świata”.
5. Edukacja dla Europy. Raport Komisji Europejskiej.
6. Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013.
7. E-Europa 2020. Społeczeństwo Informacyjne dla Wszystkich.
8. Europejska Agencja Cyfrowa (program wskazujący szereg konkretnych zadań zarówno dla Komisji Europejskiej, jak i państw członkowskich).
9. Europejski Raport Konkurencyjności Cyfrowej.
10. Nowe Kompetencje Medialne UE.

5 AKTY NORMATYWNE POLITYKI SPOŁECZNEJ:

1. Ustawa o pomocy społecznej z dnia 12 marca 2004 r., Dz.U. 2004 r., nr 64, poz. 593, z późn. zm.
2. Ustawa z dnia 22 marca 1990 r. o pracownikach samorządowych, Dz.U z 2001 r., nr 142 poz. 1593, z późn. zm.
3. Ustawa z dnia 5 lipca o zawodach pielęgniarek i położnych, Dz.U. z 2001 r., nr 57, poz. 602, z późn. zm.
4. Ustawa z dnia 8 czerwca 2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów, Dz.U., nr 73, poz. 763 z późn. zm.
5. Ustawa z dnia 26 stycznia 1982r. Karta Nauczyciela, Dz.U. z 2006 r., nr 97, poz. 674, z późn. zm.
6. Ustawa z dnia 30 czerwca 2005 r. O finansach publicznych, Dz.U., nr 249, poz. 2104, z późn. zm.

7. Rozporządzenie Rady Ministrów z dnia 2 sierpnia 2005 r. w sprawie zasad wynagradzania pracowników samorządowych zatrudnionych w jednostkach organizacyjnych jednostek samorządu terytorialnego, Dz.U., nr 146, poz. 1222, z późn. zm.
8. Rozporządzenie Ministra Polityki Społecznej z dnia 19.10.2005 r. w sprawie domów pomocy społecznej, Dz.U., nr 217, poz. 1837
9. Rozporządzenie Ministra Edukacji Narodowej z dnia 29 marca 2001 r. zmieniające rozporządzenie w sprawie klasyfikacji zawodów szkolnictwa zawodowego, Dz.U., nr 34, poz. 405.

6 POLSKIE DOKUMENTY NORMATYWNE SANKCJONUJĄCE ZADANIA I PLANY W ZAKRESIE CYBERPRZESTRZENI

1. Strategia Rozwoju Polski do roku 2020 Komitetu Prognoz „Polska 2000 Plus" przy Prezydium PAN.
2. Strategia e-Polska – Plan działań na rzecz rozwoju elektronicznej administracji (eGovernment) na lata 2005–2006, MNiSzW, Warszawa 2004.
3. Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013.
4. Strategia państwa polskiego w dziedzinie mediów elektronicznych na lata 2005–2020, KRRiT, 26 sierpnia 2005.
5. Wyzwania dla Polski – kluczowe szanse i zagrożenia – perspektywa 2030, a na jej podstawie Polska 2030. Wyzwania rozwojowe.
6. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne.
7. Rządowy Program Ochrony Cyberprzestrzeni PR na lata 2011–2016, MSWiA, Warszawa 2011.
8. Raport o Stanie Edukacji 2010, IBE, Warszawa 2011.
9. Raport Społeczeństwo informacyjne 2012, MAiC Warszawa 2013.

7 DOKUMENTY DOTYCZĄCE E-ZDROWIA W POLSCE

1. Program Informatyzacji Ochrony Zdrowia (PIOZ).
2. Plan informatyzacji e-Zdrowie Polska na lata 2010–2015.
3. Do 2015 r. podjęcie działań pilotażowych w celu umożliwienia Europejczykom bezpiecznego dostępu przez Internet do swoich danych medycznych oraz osiągnięcie do 2020 r. powszechnego dostępu do usług telemedycznych.
4. Zalecenia określające minimalny wspólny zestaw danych pacjenta w celu zapewnienia interoperacyjności rejestrów danych.

8 DOKUMENTY DOTYCZĄCE OSÓB NIEPEŁNOSPRAWNYCH

1. Narodowe Plany Działań Przeciw Ubóstwu i Społecznemu Wykluczeniu.
2. Europejska Strategia Wobec Osób Niepełnosprawnych.
3. Konwencja Narodów Zjednoczonych o Prawach Osób Niepełnosprawnych.
4. Strategia UE w sprawie niepełnosprawności na lata 2010–2020.
5. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne.
6. Ponadto mają nastąpić zmiany w Ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne (chodzi o zapewnienie dostępu do zasobów informacji osobom niepełnosprawnym).

9 7. Dokumenty o przemocy w rodzinie

1. Kodeks cywilny, Dz. U. z 1964 r., nr 16 poz. 93.
2. Kodeks karny, Dz. U. z 1997 r., nr 88, poz. 553.
3. Kodeks postępowania karnego, Dz. U. z 1997 r. nr 89, poz. 553.
4. Kodeks rodzinny i opiekuńczy Dz. U. z 1997 r. nr 89, poz. 555.
5. Kodeks wykroczeń Dz. U. z 1997 r., nr

ZAŁĄCZNIKI

12, oz. 114.
6. Ustawa o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod karą Dz. U. z 2002, nr 197, poz. 1661.
7. Ustawa o postępowaniu nieletnich Dz. U. z 1982 r., nr 35, poz. 228.
8. Ustawa z dnia 6.04.1990 r. o Policji, nieletnich oraz działaniach podejmowanych na rzecz małoletnich, Dz. U. KGP 2010.11.64. 2011.287.1687.
9. Ustawa z dnia 29.07.2005 r. o przeciwdziałaniu przemocy w rodzinie Dz.U. 2010.33.178 j.t. z późn. zm.
10. Ustawa z dnia 6.04. Dz U. 05.180.1493 z 1. Ustawa z dnia 6.04. z późn. zm.
11. Ustawa z dnia 26.10 1982 r. o postępowaniu w sprawach nieletnich Dz. U 2010.33.178 jt z późn. zm.
12. Ustawa z dnia 6.06.1997 r. Kodeks karny, Dz. U. 1997.88 553, z późn. zm.
13. Zarządzenie 1619 KGP z dnia 03.11.2010 r. w sprawie metod i form wykonywania zadań przez policjantów w zakresie przeciwdziałania demoralizacji i przestępczości nieletnich oraz działań podejmowanych na rzecz małoletnich, Dz. U. KGP.2010.11.64.

10 DODATKOWO WARTO ZOBACZYĆ

1. B. Sochal, *Obowiązujące przepisy oświatowe a Konwencja o Prawach Dziecka*, w: Bińczycka J. (red.), *Humaniści o prawach dziecka*, Oficyna Wydawnicza „Impuls" Kraków 2000.
2. Powszechna Deklaracja Praw Człowieka.
3. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności.
4. Konwencja o Prawach Dziecka.
5. Karta Praw Podstawowych.

ZAŁĄCZNIKI

ZAŁĄCZNIK 2

LISTA INSTYTUCJI POMOCOWYCH MOGĄCYCH UDZIELIĆ WSPARCIA

Wojciech Duranowski
Arkadiusz Durasiewicz

1 **WPROWADZENIE**

Ochrona cyberprzestrzeni stała się jednym z najczęściej podejmowanych tematów dotyczących bezpieczeństwa. Państwa, organizacje międzynarodowe i inni aktorzy niepaństwowi zrozumieli, że stabilność funkcjonowania i rozwój globalnego społeczeństwa informacyjnego jest uzależniony od otwartej, niezawodnej i – przede wszystkim – bezpiecznej cyberprzestrzeni. Podnoszenie świadomości w tym zakresie idzie w parze z gwałtownym wzrostem liczby incydentów komputerowych i nowych rodzajów zagrożeń.

2 Polska również jest obiektem ataków cybernetycznych. Podobnie jak inne państwa stoi przed wyzwaniem, jakim jest wypracowanie zmian prawnych i organizacyjnych, pozwalających na zapewnienie właściwego poziomu bezpieczeństwa cyberprzestrzeni i funkcjonujących w niej obywateli.

INSTYTUCJE MOGĄCE UDZIELIĆ WSPARCIA W KWESTIACH ZWIĄZANYCH Z CYBERPRZESTRZENIĄ:

3 **RZĄDOWE CENTRUM BEZPIECZEŃSTWA**

Rządowe Centrum Bezpieczeństwa jest państwową jednostką budżetową powołaną na podstawie art.10 ust.1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

Zadania:

Do podstawowych zadań RCB należy dokonywanie pełnej analizy zagrożeń, na podstawie danych uzyskiwanych ze wszystkich możliwych „ośrodków kryzysowych" funkcjonujących w ramach administracji publicznej oraz danych od partnerów międzynarodowych. Ponadto do zadań RCB należy opracowywanie optymalnych rozwiązań pojawiających się sytuacji kryzysowych, a także koordynowanie przepływu informacji o zagrożeniach.

Pozostałe zadania Rządowego Centrum Bezpieczeństwa to:

1. stworzenie katalogu zagrożeń,
2. monitorowanie zagrożeń w kraju i poza jego granicami,
3. uruchamianie procedur zarządzania kryzysowego na poziomie krajowym,
4. realizacja zadań planistycznych i programowych z zakresu zarządzania kryzysowego i ochrony infrastruktury krytycznej,
5. nadzór nad spójnością procedur reagowania kryzysowego,
6. organizowanie i prowadzenie szkoleń i ćwiczeń z zakresu zarządzania kryzysowego,
7. realizacja zadań z zakresu przeciwdziałania, zapobiegania i likwidacji skutków zdarzeń o charakterze terrorystycznym,
8. współpraca międzynarodowa, szczególnie z NATO i UE w ramach zarządzania kryzysowego.

RCB zapewnia również prezesowi Rady Ministrów, Radzie Ministrów oraz Rządowemu Zespołowi Zarządzania Kryzysowego niezbędne wsparcie w procesie podejmowania decyzji szeroko rozumianego bezpieczeństwa, poprzez dostarczanie merytorycznych opracowań i analiz.

Adres: Rządowe Centrum Bezpieczeństwa, Al. Ujazdowskie 5, 00-583 Warszawa, e-mail: poczta@rcb.gov.pl, strona internetowa: www.rcb.gov.pl

4 **MINISTERSTWO SPRAW WEWNĘTRZNYCH – DEPARTAMENT TELEINFORMATYKI**

Do zakresu działania Departamentu Teleinformatyki należy:

1. nadzór nad utrzymaniem systemów i sieci teleinformatycznych: Sieci Łączności Rządowej, TESTA, s-TESTA do przesyłania informacji niejawnych o klauzuli zastrzeżone, GovNET, PESEL-NET, WAN-CEPiK, System Infor-

macyjny Schengen (SiS) i Wizowy System Informacyjny (VIS);
2. zarządzanie architekturą systemów teleinformatycznych prowadzonych na potrzeby ewidencji pozostających we właściwości Ministra;
3. prowadzenie spraw związanych z:
   a. nadzorem nad utrzymaniem trwałości infrastruktury teleinformatycznej systemów informatycznych i ewidencji eksploatowanych w Departamencie, ze szczególnym uwzględnieniem bezpieczeństwa i efektywności przetwarzania i udostępniania danych,
   b. koordynowaniem działań w zakresie budowy i utrzymania sieci oraz urządzeń podstawowego i zapasowego centrum komputerowego dla ewidencji, rejestrów publicznych i systemów teleinformatycznych Ministerstwa obsługiwanych przez Departament,
   c. nadzorem i utrzymaniem sieci teleinformatycznych Ministerstwa obsługiwanych przez Departament,
   d. planowaniem, rozwojem, koordynacją oraz wykorzystaniem sieci i systemów radiokomunikacyjnych i telekomunikacyjnych dla potrzeb Ministra oraz organów i jednostek organizacyjnych podległych Ministrowi lub przez niego nadzorowanych, a także innych organów administracji rządowej,
   e. wykonywaniem zadań operatora i administratora Sieci Łączności Rządowej;
4. prowadzenie spraw pozostających w kompetencji Ministra związanych z organizacją i koordynacją zadań w zakresie bezpieczeństwa teleinformatycznego i ochrony danych przekazywanych i przetwarzanych w sieciach i systemach teleinformatycznych Ministerstwa, w tym:
   a. pełnienie funkcji Administratora Bezpieczeństwa Informacji,
   b. opracowywanie i nadzorowanie planów ciągłości działania dla krytycznej infrastruktury teleinformatycznej;
5. prowadzenie prac związanych z:
   a. nadzorem nad budową oraz wdrożeniem infrastruktury systemu łączności specjalnej dla potrzeb służb bezpieczeństwa i porządku publicznego oraz służb ratownictwa,
   b. koordynacją w zakresie zapewnienia łączności dla całodobowej obsługi Centrum Zarządzania Kryzysowego Ministra, Służby Dyżurnej Ministra oraz wymiany informacji z naczelnymi i centralnymi organami administracji rządowej oraz organami i jednostkami podległymi Ministrowi lub przez niego nadzorowanymi, w tym ustaleniem standardów technicznych,
   c. organizacją i koordynacją w zakresie bezpieczeństwa państwa, w tym obronności, w odniesieniu do sieci i systemów teleinformatycznych budowanych i eksploatowanych dla potrzeb Ministra oraz nadzór nad realizacją zadań związanych z organizacją łączności na potrzeby stanowisk kierowania dla kierowniczych organów państwa,
   d. koordynacją zadań związanych z implementacją Dyrektywy 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników w zakresie europejskiego numeru alarmowego 112 w zakresie dotyczącym służb bezpieczeństwa publicznego i ratownictwa podległych Ministrowi,
   e. nadzorem Ministra nad utrzymaniem, rozwojem i finansowaniem Ogólnopolskiej Sieci Teleinformatycznej na potrzeby obsługi numeru alarmowego 112 (OST 112),

ZAŁĄCZNIKI

f. planowaniem wykorzystania systemów nawigacji satelitarnej dla potrzeb Ministra oraz organów i jednostek organizacyjnych podległych Ministrowi lub przez niego nadzorowanych, a także innych organów administracji rządowej;

6. określanie warunków i zasad organizacji łączności radiokomunikacyjnej dla potrzeb współdziałania Ministerstwa oraz organów i jednostek organizacyjnych podległych Ministrowi lub przez niego nadzorowanych oraz innych organów administracji rządowej;
7. gospodarowanie zasobami numeracji telekomunikacyjnej i częstotliwości radiowych przydzielonymi dla potrzeb Ministerstwa oraz organów i jednostek organizacyjnych podległych Ministrowi lub przez niego nadzorowanych oraz innych organów administracji rządowej, z uwzględnieniem zakresu zarządzania kryzysowego i koordynacji zadań ratowniczych;
8. prowadzenie uzgodnień i określanie potrzeb niezbędnych dla sporządzania planów działań, o których mowa w art. 176a ust. 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
9. współpraca z jednostkami administracji rządowej i samorządowej w zakresie opracowywania rozwiązań integracyjnych z systemami teleinformatycznymi prowadzonymi przez te jednostki;
10. prowadzenie spraw w zakresie współpracy z organami innych państw, w tym z instytucjami Unii Europejskiej w szczególności w obszarze spraw związanych z integracją polskich systemów teleinformatycznych z systemami Unii Europejskiej, w tym sieci TESTA oraz ochrony teleinformatycznej infrastruktury krytycznej i cyberprzestrzeni, w uzgodnieniu z Departamentem Współpracy Międzynarodowej i Funduszy Europejskich;
11. współpraca z Ministerstwem Administracji i Cyfryzacji w zakresie wykorzystania systemu Portal Informacji Administracji (PIA) dla potrzeb ewidencji prowadzonych przez Ministra i systemu ePUAP.

Adres: Ministerstwo Spraw Wewnętrznych ul. Stefana Batorego 5, 02-591 Warszawa, e-mail: sekretariat.dt@msw.gov.pl, strona internetowa: www.msw.gov.pl

5 MINISTERSTWO ADMINISTRACJI I CYFRYZACJI

Zadania:

1. Zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej państwa.
2. Zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni.
3. Zmniejszenie skutków incydentów godzących w bezpieczeństwo teleinformatyczne.
4. Określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni.
5. Stworzenie i realizacja spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych.
6. Stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz użytkownikami cyberprzestrzeni.

Adres: Ministerstwo Administracji i Cyfryzacji, ul. Królewska 27, 00-060 Warszawa, e-mail: mac@mac.gov.pl, strona internetowa: www.mac.gov.pl

6 IMINISTERSTWO OBRONY NARODOWEJ – INSPEKTORAT SYSTEMÓW INFORMACYJNYCH

Zadania:

Inspektorat Systemów Informacyjnych jest właściwy w zakresie informatyzacji resortu obrony narodowej, organizując i kierując procesami planowania, dostarczania, wsparcia eksploatacji oraz użytkowania systemów teleinformatycznych stosownie do

wypracowanych kierunków rozwoju przez organizatorów systemów funkcjonalnych, w szczególności wsparcia dowodzenia oraz potrzeb zgłoszonych przez inne komórki i jednostki organizacyjne. Odpowiada za system zarządzania bezpieczeństwem teleinformatycznym w cyberprzestrzeni pozostającej w kompetencji Ministra Obrony Narodowej. Uczestniczy oraz wykonuje zadania planowania i organizacji systemu dowodzenia w czasie pokoju, kryzysu i wojny.

Adres: Inspektorat Systemów Informacyjnych, Al. Niepodległości 218, 00-911 Warszawa, e-mail: isi@mon.gov.pl, strona internetowa: www.isi.wp.mil.pl

7 RZĄDOWY ZESPÓŁ REAGOWANIA NA INCYDENTY KOMPUTEROWE NALEŻĄCY DO STRUKTUR AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO.

Zadania:
Zgodnie z przyjętą Polityką Ochrony Cyberprzestrzeni RP, w zakresie realizacji zadań związanych z bezpieczeństwem cyberprzestrzeni RP, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełni rolę głównego zespołu CERT w obszarze administracji rządowej i obszarze cywilnym.

Podstawowym jego zadaniem jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami. Realizuje on jednocześnie zadania głównego narodowego zespołu odpowiadającego za koordynację procesu obsługi incydentów komputerowych w obszarze CRP. Stanowi poziom drugi Krajowego Systemu Reagowania na Incydenty Komputerowe w CRP.

Adres: Rządowy Zespół Reagowania na Incydenty Komputerowe, ul. Rakowiecka 2A, 00-993 Warszawa, e-mail: cert@cert.gov.pl, strona internetowa: www.cert.gov.pl

8 CERT Polska

CERT (Computer Emergency Response Team) Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet. CERT Polska działa od 1996 roku (do końca roku 2000 pod nazwą CERT NASK), a od roku 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams). W ramach tej organizacji współpracuje z podobnymi zespołami na całym świecie. Zespół CERT Polska działa w strukturach Naukowej i Akademickiej Sieci Komputerowej. Działalność zespołu jest finansowana przez NASK.

Do głównych zadań zespołu należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci
- alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń
- współpraca z innymi zespołami IRT (Incidents Response Team) w ramach FIRST
- prowadzenie działań zmierzających do wzrostu świadomości dotyczącej bezpieczeństwa teleinformatycznego
- prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu
- niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego
- prace w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów, a także klasyfikacji i tworzenia statystyk.

W 2012 r. zespół CERT Polska obsłużył 605 incydentów naruszających bezpieczeństwo teleinformatyczne, zgłoszonych przez różne podmioty. Najczęściej zgłaszanym typem incydentu były oszustwa komputerowe (o 1/3 więcej niż w 2011 r.). Na kolejnych pozycjach znalazły się incydenty dotyczące obraźliwych i nielegalnych treści, a także gromadzenia informacji oraz złośliwego oprogramowania. Zespół CERT

Polska zwraca uwagę, że już po raz kolejny zanotowano mniejszą liczbę incydentów. Są one przy tym bardziej skomplikowane, a proces ich obsługi znacznie się wydłużył.

Adres: ul. Wąwozowa 18, 02-796 Warszawa, e-mail: info@cert.pl, strona internetowa: www.cert.pl

9 Fundacja Dzieci Niczyje

Fundacja Dzieci Niczyje istnieje po to, aby zapewnić każdemu dziecku bezpieczne dzieciństwo. Chronim dzieci przed krzywdzeniem i pomaga tym, które doświadczyły przemocy.

Cele:

- Uczy dorosłych, jak traktować dzieci, żeby ich nie krzywdzić
- Pokazuje im, jak reagować, gdy podejrzewają, że dziecku dzieje się krzywda
- Uczy dzieci, jak mogą uniknąć przemocy i wykorzystywania
- Oferuje krzywdzonym dzieciom i ich opiekunom pomoc psychologiczną i prawną
- Wpływa na polskie prawo, by jak najlepiej chroniło interes dziecka

Zadania:

Od 2004 roku działalność Fundacji Dzieci Niczyje obejmuje problem bezpieczeństwa dzieci i młodzieży w Internecie. Wtedy to zainicjowano program Dziecko w Sieci, w ramach którego przygotowano kampanię „Nigdy nie wiadomo, kto jest po drugiej stronie". Była to pierwsza w Polsce kampania społeczna poruszająca problem uwodzenia dzieci w Internecie.

Od stycznia 2005 roku projekt Dziecko w Sieci, już jako kompleksowe działania na rzecz bezpieczeństwa dzieci i młodzieży w Internecie jest realizowany w ramach programu Komisji Europejskiej Safer Internet. Głównym partnerem programu jest Fundacja Orange.

W ramach programu prowadzone są badania poświęcone zagrożeniom dzieci i młodzieży w Internecie. Na ich podstawie, jak również na podstawie dostępnej wiedzy oraz doświadczenia pracowników fundacji wypracowywane są przekazy medialne oraz projekty edukacyjne poświęcone bezpieczeństwu młodych internautów. Bogata oferta scenariuszy zajęć, filmów, ale i kursów e-learningowych powinna zainteresować przede wszystkim profesjonalistów (nauczycieli, pedagogów szkolnych, psychologów), których praca jest związana z bezpieczeństwem dzieci i młodzieży. Materiały te (obecnie obejmujące już wszystkie grupy wiekowe) mogą być doskonałą podstawą do poprowadzenia lub uatrakcyjnienia zajęć dotyczących bezpieczeństwa przede wszystkim w Internecie, ale i w życiu realnym, na które globalna sieć ma coraz większy wpływ.

W ramach programu Dziecko w Sieci Fundacja Dzieci Niczyje we współpracy z Fundacją Orange prowadzi projekt Helpline.org.pl. Jego założeniem jest oferowanie pomocy dzieciom i młodzieży w sytuacjach zagrożenia w sieci, obejmujących m.in. cyberprzemoc, uwodzenie w Internecie, jak i problem uzależnienia od komputera i/lub Internetu. Codziennie za pośrednictwem bezpłatnego telefonu (800 100 100), e-maila (helpline@helpline.org.pl) lub strony internetowej (www.helpline.org.pl) do konsultantów trafiają sprawy związane z problemami młodych internautów. W wypadku, kiedy zachodzi podejrzenie popełnienia przestępstwa, którego ofiarą padło dziecko lub młody człowiek, sprawa jest przekazywana policji lub prokuraturze.

Adres: Fundacja Dzieci Niczyje, ul. Katowicka 31, 03-932 Warszawa, e-mail: fdn@fdn.pl, strona internetowa: www.fdn.pl

10 **Safer Internet**

Program Komisji Europejskiej Safer Internet uruchomiony został w 1999 r. i ma na celu promocję bezpiecznego korzystania z nowych technologii i Internetu wśród dzieci i młodzieży. W ramach programu prowadzone są również działania na rzecz zwalczania nielegalnych treści i spamu w Internecie. Od 2005 r. do programu włączona została problematyka związana z zagrożeniami wynikającymi z użytkowania telefonów komórkowych, gier online, wymianą plików P2P i innymi formami komunikacji online w czasie rzeczywistym (czaty i komunikatory). Priorytetem programu na lata 2009–2013 jest zwalczanie cyberprzemocy i uwodzenia dzieci w Internecie.

W ramach programu Safer Internet w całej Europie działają narodowe punkty, których działalność koncentruje się na budowaniu świadomości o zagrożeniach, z jakimi w Sieci mogą zetknąć się jej najmłodsi użytkownicy. Aktualnie sieć obejmuje 30 krajów. Ich współpracę na poziomie europejskim koordynuje stowarzyszenie Insafe.

Polskie Centrum Programu Safer Internet (PCPSI) powołane zostało w 2005 r. w ramach programu Komisji Europejskiej Safer Internet. Tworzą je Fundacja Dzieci Niczyje oraz Naukowa i Akademicka Sieć Komputerowa (koordynator PCPSI). Centrum podejmuje szereg kompleksowych działań na rzecz bezpieczeństwa dzieci i młodzieży korzystających z Internetu i nowych technologii. Partnerem większości realizowanych przez Centrum projektów jest Fundacja Orange.

W ramach Polskiego Centrum Programu „Safer Internet" realizowane są trzy projekty:

Saferinternet.pl – projekt, którego celem jest zwiększanie społecznej świadomości na temat zagrożeń, jakie niosą ze sobą najnowsze techniki komunikacji. Wśród podejmowanych działań priorytetem jest edukacja, zarówno dzieci, jak i rodziców, a także podnoszenie kompetencji profesjonalistów w zakresie bezpiecznego korzystania z Internetu.
Projekt realizowany przez FDN i NASK we współpracy z Fundacją Orange.

Helpline.org.pl
Projekt realizowany przez FDN oraz Fundację Orange.

Dyżurnet.pl – punkt kontaktowy, tzw. hot-line, do którego można anonimowo zgłaszać przypadki występowania w Internecie treści zabronionych prawem, takich jak pornografia dziecięca, pedofilia, treści o charakterze rasistowskim i ksenofobicznym.
Projekt realizowany przez NASK.

Adres: ul. Wąwozowa 18, 02-796 Warszawa, strona internetowa: www.saferinternet.pl

11 **Fundacja Bezpieczna Cyberprzestrzeń**

Fundacja Bezpieczna Cyberprzestrzeń powstała w czerwcu 2010 roku. Celem Fundacji jest działanie na rzecz bezpieczeństwa cyberprzestrzeni, w tym na rzecz poprawy bezpieczeństwa w sieci Internet.

Zadania:

- uświadamianie o zagrożeniach teleinformatycznych,
- reagowanie na przypadki naruszania bezpieczeństwa w cyberprzestrzeni,
- prowadzenie działalności badawczo-rozwojowej w dziedzinie bezpieczeństwa teleinformatycznego.

Fundacja Bezpieczna Cyberprzestrzeń zaangażowana jest w wiele inicjatyw, konferencji, szkoleń i projektów dotyczących tematyki bezpieczeństwa teleinforma-

tycznego. Tworzy i współtworzy raporty i opracowania z tematyki bezpieczeństwa teleinformatycznego i ochrony infrastruktury krytycznej, jak również wiele materiałów szkoleniowych z zakresu bezpieczeństwa IT wykorzystywanych w kraju i za granicą.

Fundacja ma swój udział w tworzeniu periodyku „CIIP Focus" wydawanego przez Rządowe Centrum Bezpieczeństwa. W 2012 roku zainicjowała, współorganizowała i koordynowała pierwsze w Polsce ćwiczenia z ochrony w cyberprzestrzeni – Cyber-EXE Polska 2012, które będą kontynuowane w następnych latach.

Ponadto Fundacja jest członkiem konsorcjum organizującego współpracę CERT-ów europejskich w ramach inicjatywy Trusted Introducer, będącej częścią projektu TERENA TF-CSIRT. Blisko współpracuje również z Europejską Agencją Bezpieczeństwa Sieci i Informacji (ENISA), Stowarzyszeniem CEENet (Central Eastern European Network Association) oraz jest członkiem polskiego forum zespołów reagujących i zespołów bezpieczeństwa – Abuse-Forum.

Adres: Fundacja Bezpieczna Cyberprzestrzeń, ul. Tytoniowa 20, 04—228 Warszawa, e-mail: kontakt@cybsecurity.org, strona internetowa: www.cybsecurity.org

12 PODSUMOWANIE

Cyberprzestrzeń stała się nowym środowiskiem bezpieczeństwa, co pociąga za sobą konieczność dokonania licznych zmian, zarówno w pragmatyce, jak i w prawno-organizacyjnym wymiarze funkcjonowania systemów bezpieczeństwa na świecie. W tym kontekście szczególnie istotne jest zrozumienie dynamiki zmian tego środowiska.

Budowa systemu prawnego, stanowiącego odpowiedź państwa na szanse i wyzwania związane z jego obecnością w cyberprzestrzeni, jest zadaniem niezwykle złożonym. Wynika to nie tylko z tempa zmian technologicznych, ale także ze szczególnego charakteru środowiska Web 2.0 i jego „interaktywnej" natury. Trendy w prawie międzynarodowym, występujące od zakończenia zimnej wojny, zmierzające do traktowania jednostki jako jednego z równoprawnych aktorów w stosunkach międzynarodowych, zyskują szczególne znaczenie w warunkach społeczeństwa sieci. Małe, często trudne do zdefiniowania grupy – zarówno pod kątem tożsamości indywidualnych uczestników, jak i ich „zbiorowej" tożsamości – mogą stanowić zagrożenie dla funkcjonowania nie tylko podmiotów pozapaństwowych, ale także samych państw.

Kształtując normy prawne na poziomie krajowym, przepisy regulujące współpracę międzynarodową oraz strategie i polityki bezpieczeństwa należy zatem uwzględniać te dwa podstawowe wyzwania. Konieczność z jednej strony szybkiego reagowania, a z drugiej – reagowania na zagrożenia ze strony małych, mobilnych grup stanowią nową jakość w obszarze formułowania przepisów regulujących funkcjonowanie państwa w sferze bezpieczeństwa.

Nie można zapominać, że choć zagrożenia w cyberprzestrzeni stanowią odmienną kategorię wyzwań legislacyjno-organizacyjnych, to problemy, które stwarzają, w znacznej mierze przypominają te generowane przez inne zagrożenia asymetryczne, jak np. terroryzm. Ich wspólną cechą jest zmuszanie struktur państwowych do ewolucji w stronę rozwiązań mniej hierarchicznych, a bardziej elastycznych. Sieciowość, zarówno w wymiarze społecznym, jak i technologicznym, wraz z jej wszystkimi konsekwencjami, zdaje się

ZAŁĄCZNIKI

stanowić jedno z najważniejszych pojęć nowego paradygmatu bezpieczeństwa na poziomie krajowym i międzynarodowym.

BIBLIOGRAFIA:

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, Warszawa 2012.

Raport o stanie bezpieczeństwa cyberprzestrzeni, www.cert.gov.pl, data dostępu: 10.01.2014.

Raport – Polityka Ochrony Cyberprzestrzeni, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013.

Rządowy Program Ochrony Cyberprzestrzeni na lata 2011-2016.

EKSPERCI

Eksperci w projekcie PI-PWP Zagrożenia cyberprzestrzeni – nowe kompetencje pracownika socjalnego

Prof. dr hab. Józef Bednarek
Pedagog, dydaktyk, medioznawca.

Zainteresowania badawcze: świat wirtualny – jego możliwości i zagrożenia.

Doświadczenie: prof. dr hab. Józef Bednarek jest pracownikiem naukowo-dydaktycznym Akademii Pedagogiki Specjalnej im. Marii Grzegorzewskiej w Warszawie. Autor i redaktor wielu publikacji. Organizator i współorganizator wielu konferencji i seminariów naukowych, na których wygłaszał referaty oraz komunikaty z własnych badań. Kierownik projektów badawczych. Promotor prac doktorskich i magisterskich. Twórca licznych innowacyjnych rozwiązań edukacyjnych. Prof. Józef Bednarek pełni wiele funkcji w organizacjach i stowarzyszeniach. **Jest m.in. wiceprzewodniczącym w Zespole ds. Bezpieczeństwa Dziecka w Cyberprzestrzeni przy Rzeczniku Praw Dziecka RP**.

Wybrane publikacje:
- Osoby niepełnosprawne a media cyfrowe. Z pogranicza teorii i praktyki (2010),
- Multimedialne kształcenie ustawiczne nauczycieli. Teoria. Badania. Praktyka (2010),
- Przemoc i agresja w sieci – cyberbullying (2009),
- Cyberświat – możliwości i ograniczenia (2009),
- Multimedia w kształceniu (2006),
- Społeczeństwo informacyjne i mediów w opinii osób niepełnosprawnych (2005),
- Media w nauczaniu (2002).

Prof. Velta Lubkina
Pedagog i dydaktyk

Zainteresowania badawcze: socjalizacja osobowości, procesy resocjalizacyjne, profesjonalna edukacja w kontekście zrównoważonego rozwoju i współpracy z partnerami społecznymi.

Doświadczenie: prof. dr Velta Lubkina jest wykładowcą w Rezekne Higher Education Institution na Łotwie, dyrektorem Personality Socialization Research Institute (PSRI) w tejże Uczelni. W PSRI koordynuje program studiów doktoranckich na kierunku Pedagogika. **Od wielu lat uczestniczy w grupach roboczych UE opracowujących rozwój europejskich programów studiów**. Kierownik wielu projektów badawczych. Prelegent licznych międzynarodowych i krajowych konferencji. Ekspert i doradca projektów, programów i seminariów dotyczących socjalizacji oraz edukacji.

Wybrane publikacje (tłumaczenie tytułów na potrzeby dokumentu):
- Komputer jako medium przydatne dla rozwoju języka i umiejętności społecznych uczniów specjalnych potrzeb (2010),
- Korzystanie z technologii informacyjnych na rzecz problemów z integracją osób niepełnosprawnych (2010),
- Oglądać. Myśleć. Robić. Narzędzia metodologiczne (2008),
- Pedagogiczne i społeczno-ekonomiczne aspekty zachowań konsumentów (2008),
- Rozwój zaufania i procesu komunikacji dzieci przedszkolnych i nauczycieli (2007).

Prof. Gilberto Marzano
Pedagog w zakresie edukacji informatycznej i medialnej, ekspert w dziedzinie informatyki (systemy multimedialne, zarządzania dokumentami, ochrony zasobów cyfrowych) i antropologii społecznej.

Zainteresowania badawcze: informatyka, zarządzanie dokumentacją, ochrona zasobów cyfrowych i antropologia społeczna.

Doświadczenie: Profesor na Uniwersytecie w Trieście. Prezes prywatnego instytutu badawczego non profit (Ecoistituto del Friuli Venezia Giulia). Członek zarządu i wykładowca na studiach doktoranckich na Uniwersytecie w Udine we Włoszech. Kierownik Technological Laboratory of Personality and Socialization Research Institute w Rezekne Augstskola (Łotwa). Członek zarządu Uniwersytetu Liberta (Włochy). Pracuje nad rozwojem innowacyjnych rozwiązań komputerowych. Prowadził badania w dziedzinie wyszukiwania informacji i antropologii. Prof. Gilberto Marzano jest odpowiedzialny za rozwój wielu systemów informatycznych. Uczestnik krajowych i międzynarodowych projektów. Koordynator projektów badawczych. Autor licznych publikacji naukowych i technicznych.

Wybrane publikacje (tłumaczenie tytułów na potrzeby dokumentu):
- Udział obywateli w dziedzinie ochrony zdrowia: owocna szansa czy idea etyczna populistów (2012),
- Przechowywanie danych cyfrowych, metody standaryzacji technologii (2011),
- Korzystanie z gramatyki funkcjonalnej w automatycznym przetwarzaniu dokumentów administracyjnych w rejestrze gruntów. Dziennik dokumentacji (1993),
- Środowisko, technologia informacyjna i inteligentne systemy wsparcia V.I.A (1992),
- Technologia i społeczeństwo w ocenie oddziaływania na środowisko (1991),
- Dokumenty, praktyki zawodowe i nowe scenariusze, biblioteki dziś (1991).

Dr Anna Andrzejewska
Pedagog w zakresie edukacji informatycznej i medialnej, specjalista w zakresie zagrożeń generowanych przez cyberprzestrzeń.

Zainteresowania badawcze: pedagogika, psychologia, edukacja medialna, cyberprzestrzeń, patologie społeczne w cyberprzestrzeni.

Doświadczenie: pracownik naukowo-dydaktyczny Akademii Pedagogiki Specjalnej im. Marii Grzegorzewskiej w Warszawie. Zajmuje się edukacją medialną, patologiami w cyberprzestrzeni oraz uzależnieniami od mediów cyfrowych. **Od lat prowadzi badania związane z wpływem najnowszych mediów na życie dzieci i młodzieży**. Uczestniczka międzynarodowych i krajowych konferencji naukowych i sympozjów. Prowadzi szkolenia i warsztaty z zakresu zagrożeń generowanych przez cyberprzestrzeń. Współautorka projektów badawczych. Kierownik i realizator wielu edukacyjnych etiud filmowych i aplikacji multimedialnych z powyższych obszarów wiedzy. Pełni liczne funkcje w organizacjach i stowarzyszeniach społecznych. **Dr Andrzejewska jest m.in. członkiem Zespołu ds. Bezpieczeństwa Dziecka w Cyberprzestrzeni przy Rzeczniku Praw Dziecka RP**.

Wybrane publikacje:
- Osoby niepełnosprawne a media cyfrowe. Z pogranicza teorii i praktyki (2010),
- Patologie moralne w sieci (2009),
- Gry komputerowe i sieciowe. Nasze dziecko w wielkiej sieci (2009),
- Cyberświat – możliwości i ograniczenia (2009),
- (Nie)Bezpieczny komputer. Od euforii do uzależnień (2008),
- Magia szklanego ekranu – zagrożenia płynące z telewizji (2007).

Dr Ewa Karolina Flaszyńska
polityk społeczny, dyrektorka Ośrodka Pomocy Społecznej Dzielnicy Bielany m. st. Warszawy.

Zainteresowania badawcze: polityka społeczna, przedsiębiorczość, ekonomia społeczna, dialog społeczny.

Doświadczenie: Dyrektor Ośrodka Pomocy Społecznej Dzielnicy Bielany w Warszawie. Wcześniej pełniła funkcję m.in. Kierownika w Wojewódzkim Urzędzie Pracy w Warszawie oraz Naczelnika Wydziału Instytucjonalnej Obsługi i Programów Rynku Pracy w Departamencie Rynku Pracy Ministerstwa Pracy i Polityki Społecznej. Jest pracownikiem naukowo-dydaktycznym w Wyższej Szkole Ekonomiczno-Społecznej w Ostrołęce oraz Akademii Pedagogiki Specjalnej im. Marii Grzegorzewskiej w Warszawie. Od lat prowadzi badania w obszarze szeroko rozumianej polityki społecznej, przedsiębiorczości i dialogu społecznego. Uczestniczka wielu międzynarodowych i krajowych konferencji naukowych, kursów, szkoleń z zakresu polityki rynku pracy i polityki społecznej oraz funduszy Unii Europejskiej, m.in. w Niemczech, Francji, Wielkiej Brytanii, Szwajcarii, Hiszpanii. Prowadziła również gościnne wykłady na Uniwersytecie Narodów Zjednoczonych w Tokio.

Wybrane publikacje:
- Praca w Polsce (2013),
- Ekonomia z elementami polityki społecznej a zadania dla regionalnego dialogu społecznego (2011),
- Europejski dialog społeczny i instytucje UE a dialog regionalny (2011),
- Znaczenie pracy w życiu człowieka (2011),
- Kobiety na rynku pracy (2008),
- Pomoc społeczna w Polsce – poradnik dla pracowników GCI (2008),
- Aktywizacja zawodowa osób zagrożonych długotrwałym bezrobociem. Kobiety i osoby po 50. roku życia na rynku pracy (2008).

Wojciech Duranowski
Pracownik Działu Rozwoju i Współpracy Międzynarodowej w Wyższej Szkole Pedagogicznej im. Janusza Korczaka w Warszawie. Przygotowuje doktorat w Szkole Głównej Handlowej w Warszawie. Zajmuje się działalnością rozwojową uczelni, pozyskiwaniem środków unijnych, rozszerzaniem współpracy międzynarodowej oraz badaniami naukowymi prowadzonymi na uczelni.

Zainteresowania badawcze: zarządzanie międzykulturowe, przedsiębiorczość, ekonomia społeczna, społeczeństwa Azji, Afryki i Ameryki Południowej.

Doświadczenie: Wojciech Duranowski jest doradcą i ekspertem wielu projektów realizowanych na uczelni WSP im. Janusza Korczaka w Warszawie. Prelegent oraz wykładowca na zagranicznych uczelniach. Wielokrotny organizator i uczestnik delegacji zagranicznych oraz konferencji. Inicjator współpracy z czołowymi uczelniami w Europie i Azji. Posiada bogatą wiedzę oraz znajomość Programów Unii Europejskiej dla szkół wyższych i umiejętność kierowania wielokulturowym zespołem ludzkim.

Wybrane publikacje:
- Standardy superwizji pracy socjalnej w USA, w publikacji (2013),
- Przeciwdziałanie wykluczeniu społecznemu w Bangladeszu za pomocą modelu mikrokredytu opartego na kapitale społecznym (2012),
- Czy mikrokredyty mogą być panaceum na biedę (2010),
- Overview of Microfinance Sector in Bangladesh (2011),
- Podejście oparte na empowermencie w pracy socjalnej, w publikacji (2013).

Łukasz Tomczyk
Pedagog i informatyk, specjalista w dziedzinie nowych mediów.

Zainteresowania badawcze: zagadnienia z zakresu społeczeństwa informacyjnego, edukacji permanentnej (szczególnie oświaty dorosłych) oraz interakcji człowieka z komputerem.

Doświadczenie: Łukasz Tomczyk współpracuje z kilkoma uczelniami wyższymi. Egzaminator Europejskiego Certyfikatu Umiejętności Komputerowych (ECDL). Członek licznych stowarzyszeń naukowych i edukacyjnych m.in. Polskiego Towarzystwa Informatycznego, Akademickiego Towarzystwa Andragogicznego oraz Stowarzyszenia Gerentologów Społecznych. Prelegent i uczestnik wielu konferencji naukowych poświęconych tematyce TI. Łukasz Tomczyk jako ekspert bierze aktywny udział w wielu projektach badawczych m.in. w WSP im. Janusza Korczaka w Warszawie.

Wybrane publikacje:
- Zostań E-Obywatelem (2011),
- (Nie)Bezpieczny Internet (2007),
- Jak przeciwdziałać wykluczeniu cyfrowemu? Przykład Nowego Horyzontu (2011),
- Współczesne dylematy pedagogiczne (2009),
- Seniorzy w świetle nowych technologii. Implikacje dla praktyki edukacyjnej oraz rozwoju społeczeństwa informacyjnego (2013). Publikacja w druku.

GRUPA EKSPERCKA NAUKOWEJ I AKADEMICKIEJ SIECI KOMPUTEROWEJ (NASK)

Marcin Bochenek
Dyrektor Projektów Strategicznych w NASK. Absolwent historii UJ, dziennikarz, manager, specjalista w dziedzinie nowych mediów i telewizji. W latach 20042010 pracował w Telewizji Polskiej, kierował komunikacją wewnętrzną i PR. W latach 2006-2009 członek Zarządu TVP odpowiedzialny za rozwój, inwestycje i nowe technologie. Prowadził między innymi projekty: budowy kanału TVP HD, TVP Historia, uczestniczył w projekcie tworzenia kanału TVP Sport. Odpowiadał za projekty iTVP, TVP.pl, nadzorował projekt budowy nowego portalu Telewizji Polskiej TVP.pl. Nadzorował również projekty informatyczne w TVP jako szef Komitetu Sterującego, tworzył i odpowiadał za realizację planów inwestycyjnych TVP w latach 2006-2008, tworzył i realizował koncepcję cyfryzacji TVP. Prowadził liczne projekty z dziedziny PR, promocji i konsultingu dla polskich przedsiębiorstw oraz międzynarodowych koncernów.

Dr Agnieszka Wrońska
Kierownik Działu Akademia NASK, który odpowiada za tworzenie oraz realizację działalności szkoleniowej, edukacyjnej oraz popularyzatorskiej. Posiada szerokie doświadczenie menedżerskie i szkoleniowe w różnych sektorach. Doktor nauk humanistycznych, wykładowca akademicki, trener trzeciego stopnia i superwizor, członek – założyciel, w latach 1996-2005 prezes Oddziału Warszawskiego Polskiego Stowarzyszenia Pedagogów i Animatorów KLANZA (obecnie członek honorowy), inicjator i koordynator wielu programów i projektów animacji kulturalnej i środowiskowej, również międzynarodowych. Posiada duże doświadczenie w realizacji zadań badawczych i dydaktycznych dla różnych grup wiekowych o zróżnicowanych i specjalnych potrzebach edukacyjnych. Nagrodzona Dyplomem Przyjaciela Dziecka przyznanym przez Towarzystwo Przyjaciół Dzieci. Autorka licznych publikacji oraz podręczników edukacyjnych dla uczniów szkoły podstawowej.

Krzysztof Silicki
Ukończył studia na Politechnice Warszawskiej. Pracuje w instytucie badawczym NASK (Naukowa i Akademicka Sieć Komputerowa) od 1992 roku. Obecnie na stanowisku Doradcy Dyrektora – Dyrektora

ds. Współpracy z Europejską Agencją Bezpieczeństwa Sieci i Informacji (ENISA). W latach 2000-2012 pełnił funkcję dyrektora technicznego w NASK. W latach 2000-2008 był także członkiem Rady Naukowej w instytucie oraz pełnił funkcję pełnomocnika ds. CERT Polska.

Od roku 2004 reprezentuje Polskę w Radzie Zarządzającej Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA). Współtworzył strategię i plan działania ENISA w dziedzinie bezpieczeństwa sieci i informacji. Od roku 2005 nadzorował rozwój badawczo- wdrożeniowego projektu ARAKIS, w wyniku którego powstał system wczesnego wykrywania i reagowania na zagrożenia bezpieczeństwa dla sieci internetowych. Uczestniczył i wspierał wiele projektów CERT Polska krajowych i międzynarodowych.

Jest autorem wielu publikacji i opracowań w kraju i za granicą z dziedziny sieci teleinformatycznych ze szczególnym uwzględnieniem tematyki bezpieczeństwa.
Nominowany do prestiżowej nagrody InfoStar w roku 2009 i 2011, laureat tej nagrody w roku 2011 w kategorii rozwiązania informatyczne.

Anna Rywczyńska
Koordynatorka Polskiego Centrum Programu Safer Internet oraz Kierownik Zespołu Szkoleń i Projektów Społecznych w Naukowej i Akademickiej Sieci Komputerowej. Ukończyła Uniwersytet Warszawski na Wydziale Dziennikarstwa i Nauk Politycznych ze specjalizacją Ekonomika Mediów oraz Archeologię w Instytucie Archeologii UW ze specjalizacją realizowaną w ramach Andyjskiej Misji Archeologicznej. Posiada szerokie doświadczenie we współpracy międzynarodowej, jest prelegentką oraz organizatorką szeregu konferencji o tematyce dotyczącej bezpieczeństwa telekomunikacyjnego, współtworzy również szereg medialnych oraz edukacyjnych kampanii społecznych dotyczących problematyki bezpieczeństwa w Internecie dla najmłodszych. W ostatnich latach zaangażowana w prace grup eksperckich agencji ENISA dotyczących tematyki WEB 2.0 („ENISA Virtual Group on Web 2.0 Security") oraz podniesienia świadomości o zagrożeniach on-line („Awareness Raising"). Od 2003 r. współorganizuje konferencję SECURE, najstarszą w Polsce cykliczną konferencję poświęconą bezpieczeństwu sieci i systemów ICT. Od 2007 r. jest wiceprzewodniczącą międzynarodowej konferencji „Bezpieczeństwo Dzieci i Młodzieży w Internecie".

Martyna Różycka
Absolwentka Informacji Naukowej i Bibliotekoznawstwa na Uniwersytecie Warszawskim. Od czasów studiów związana z tematyką bezpieczeństwa dzieci w Internecie. Autorka książki „Strony Internetowe dla dzieci i młodzieży" oraz innych publikacji poświęconych różnym aspektom bezpieczeństwa dziecka w Internecie. Wcześniej pracowała w agencji PR, gdzie zajmowała się głównie PR internetowym. Od sześciu lat związana z projektem „Safer Internet" – a szczególnie z polskim punktem kontaktowym, przyjmującym zgłoszenia o treściach nielegalnych i szkodliwych w Internecie. Jest prelegentem na konferencjach dla profesjonalistów oraz prowadzi warsztaty dla dzieci.

Piotr Bisialski
Absolwent Wojskowej Akademii Technicznej oraz Wyższej Szkoły Informatyki Stosowanej i Zarządzania. Pracuje w Dziale Menedżerów Produktu, odpowiedzialny za rozwiązania i usługi dotyczące bezpieczeństwa teleinformatycznego (od 5 lat w branży teleinformatycznej). W wolnych chwilach: narciarz, żeglarz i paralotniarz.

RADA PROGRAMOWO-KONSULTACYJNA W PROJEKCIE PI-PWP ZAGROŻENIA CYBERPRZESTRZENI – NOWE KOMPETENCJE PRACOWNIKA SOCJALNEGO

Dr Agnieszka Wrońska – Naukowa i Akademicka Sieć Komputerowa
Anna Brzezińska – Dyrektor Ośrodka Pomocy Społecznej w Legionowie
Maciej Sotomski – Dyrektor Wydziału Spraw Społecznych i Zdrowia w Urzędzie Dzielnicy Ochota w Warszawie
Marta Pletty-Sotomska – Asystent Rodziny w Ośrodku Pomocy Społecznej Włochy w Warszawie
Joanna Rosiek-Bryks – Kierownik Wydziału ds. Wdrażania programów społecznych – Mazowieckie Centrum Polityki Społecznej

KOMITET STERUJĄCY
Prof. dr hab. Julian Auleytner
Prof. dr hab. Mirosław Grewiński

ZESPÓŁ ZARZĄDZAJĄCY PROJEKTEM
Joanna Lizut – Kierownik Projektu
Anna Zielińska – Asystent Kierownika Projektu
Iwona Sowa – Specjalista ds. promocji i rekrutacji
Anna Cygan – Specjalista ds. rozliczeń

Wyższa Szkoła Pedagogiczna im. Janusza Korczaka w Warszawie została powołana w 1993 roku. W ponad 20-letniej historii, uczelnia utworzyła sześć placówek na terenie całego kraju. WSP edukuje w obszarze szeroko pojętych nauk społecznych. Ponadto uczelnia oferuje krótkie formy kształcenia kierowane do osób dorosłych, seniorów jak również młodzieży i dzieci w wieku szkolnym.

W swojej bogatej ofercie edukacyjnej WSP proponuje naukę na czterech kierunkach studiów: polityka społeczna, pedagogika, politologia i praca socjalna. Wszystkie kierunki studiów są dostępne również w formie Kształcenia na Odległość (KnO).

Misją uczelni jest kształcenie ustawiczne. Programy nauczania, jak również odpowiednio dobrane metody dydaktyczne, mają na celu wykształcenie otwartych i kreatywnych humanistów, którzy dostrzegają i rozumieją rzeczywistość publiczną, społeczną i gospodarczą. System dydaktyczny i naukowy opiera się na wspólnych wartościach, takich jak: równość w dostępie do wykształcenia, sprawiedliwe traktowanie, indywidualne podejście do studenta.

Partnerem Wyższej Szkoły Pedagogicznej im. Janusza Korczaka w Warszawie w projekcie innowacyjnym, w ramach którego powstała publikacja, jest Rezekne Higher Education Institution.

Rezekne Higher Education Institution (RHEI) jest wyższą instytucją naukową na Łotwie, która nie tylko kształci studentów, ale również angażuje się w badania i twórczość artystyczną. Uczelnia została utworzona w 1993 roku, na podstawie oddziałów Uniwersytetu Łotwy i Technicznego Uniwersytetu w Rydze. RHEI posiada duże doświadczenie w realizacji projektów dotyczących kształcenia zawodowego i ustawicznego. Najważniejszym celem RHEI jest zapewnienie profesjonalnej edukacji wyższej zgodnie z poziomem rozwoju nauki i tradycjami kulturalnymi Łotwy.

Publikacja powstała w ramach projektu **„PI-PWP Zagrożenia cyberprzestrzeni – nowe kompetencje pracownika socjalnego”**, którego celem jest wdrożenie innowacyjnego programu rozwoju przygotowującego pracowników służb społecznych do pracy z rodzinami oraz osobami potrzebującymi pomocy w związku z zagrożeniami generowanymi przez cyberprzestrzeń. Wdrożenie innowacyjnego programu ujętego w tej publikacji ma na celu wyposażenie pracowników służb społecznych w szerszy zakres kompetencji i instrumentów wykonawczych.

Projekt objęty honorowym patronatem Ministra Pracy i Polityki Społecznej.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Zagrożenia cyberprzestrzeni

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego