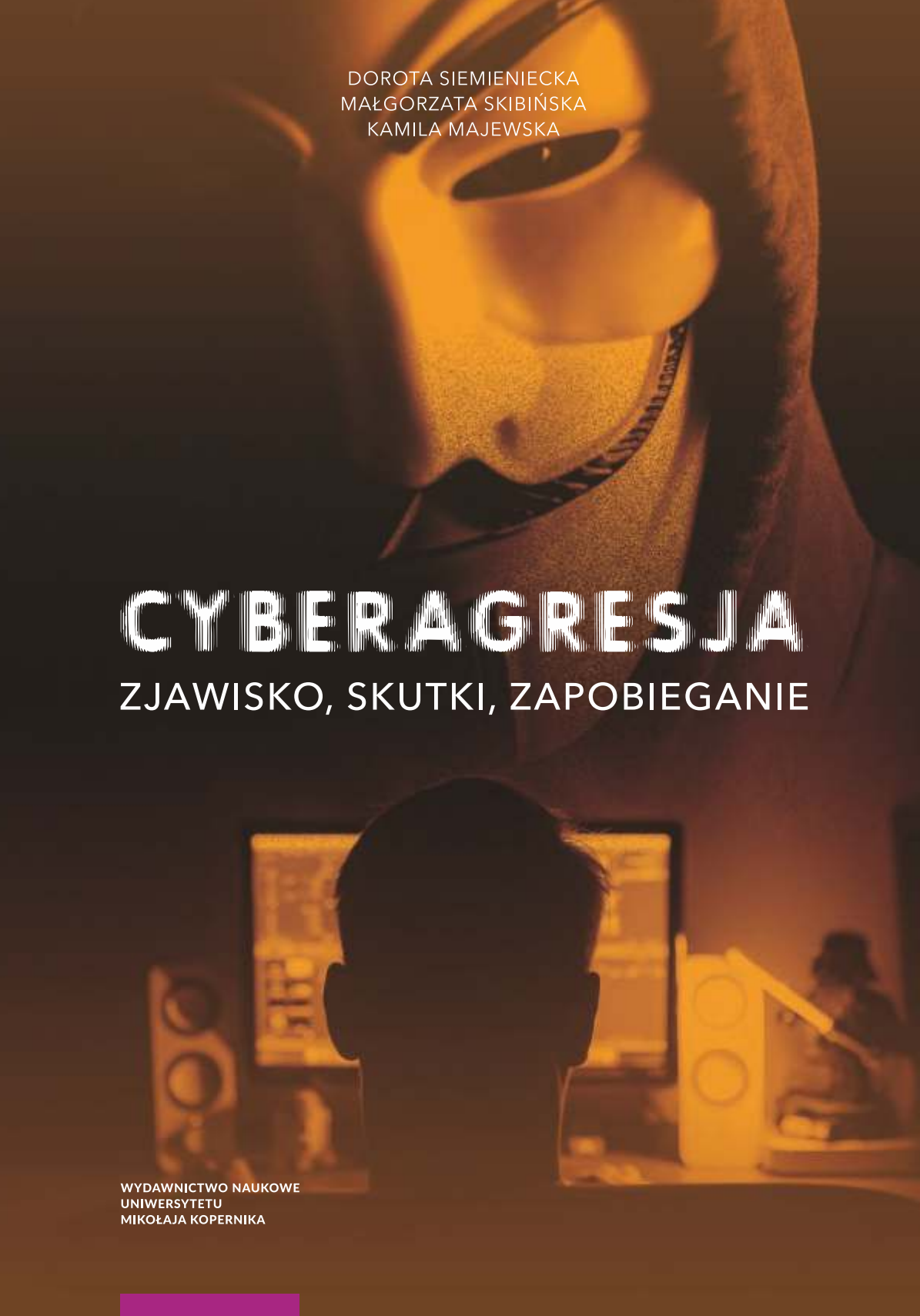
DOROTA SIEMIENIECKA
MAŁGORZATA SKIBIŃSKA
KAMILA MAJEWSKA

CYBERAGRESJA

ZJAWISKO, SKUTKI, ZAPOBIEGANIE



WYDAWNICTWO NAUKOWE
UNIWERSYTETU
MIKOŁAJA KOPERNIKA

Cyberagresja – zjawisko, skutki, zapobieganie

Dorota Siemieniecka
Małgorzata Skibińska
Kamila Majewska

Cyberagresja – zjawisko, skutki, zapobieganie

WYDAWNICTWO NAUKOWE
UNIWERSYTETU
MIKOŁAJA KOPERNIKA

Toruń 2020

Praca recenzowana

Projekt okładki
Łukasz Aleksandrowicz

Redakcja
Patrycja Maj-Palicka

Książka powstała w ramach projektu pt. „Agresja realna i wirtualna – zjawisko, skutki, zapobieganie – kurs e-learning" realizowanego przez Uniwersytet Mikołaja Kopernika w Toruniu w ramach konkursu nr POWR.03.01.00-IP.08-00-MOC/18 pt. „Kurs na MOOC" Działania 3.1 Kompetencje w szkolnictwie wyższym, Oś III Szkolnictwo wyższe dla gospodarki i rozwoju.
Program Operacyjny Wiedza Edukacja Rozwój 2014–2020

ISBN 978-83-231-4384-0
DOI: 10.12775/4384-0

WYDAWNICTWO NAUKOWE UMK
ul. Gagarina 5, 87-100 Toruń
Redakcja: tel. (56) 611 42 95; fax (56) 611 47 05
e-mail: wydawnictwo@umk.pl
Dystrybucja: tel./fax (56) 611 42 38
e-mail: books@umk.pl
www.wydawnictwo.umk.pl
Druk i oprawa: Drukarnia WN UMK

Spis treści

Rozdział 3

Wprowadzenie

Technologie sieciowe zmieniają obraz współczesnego społeczeństwa. Zmianie podlegają m.in. struktura rodziny, relacje międzyludzkie, hierarchia wartości. Nowe technologie stają się źródłem oferującym zróżnicowane style życia, oddziałując na decyzje i wybory. Przekłada się to bezpośrednio na rozwój gospodarki i dalsze przeobrażenia społeczeństw.

Postęp technologiczny wpływa na obniżenie cen sprzętu komputerowego, urządzeń mobilnych oraz usług internetowych. Ich łatwa osiągalność połączona z miniaturyzacją urządzeń sprawia, że każdy człowiek może korzystać w sposób swobodny z dostępu do światowej sieci internetowej. Jej zasoby wspomagane algorytmami proponującymi użytkownikom wybór treści mogą otwierać możliwości nieograniczonego uczenia się. Serwis YouTube zawiera niezliczone tutoriale, samouczki, przykłady zastosowań właściwie z wszystkich dziedzin nauki. Pod materiałami użytkownicy zamieszczają komentarze, inspirują się, dzielą się doświadczeniami. Informacje prezentowane w ten sposób pozwalają na budowanie wiedzy o otaczającym nas świecie. Doświadczenia te mają charakter pośredni, proces nauki odbywa się przez obserwację i uczestnictwo we wspólnotach wirtualnych.

Podstawą funkcjonowania społecznego jest komunikacja. Tomasz Goban-Klas podaje dwa znaczenia pojęcia „komunikacja": jako procesu przekazywania informacji, idei, emocji, umiejętności oraz jako interakcji, społeczne oddziaływanie za pomocą symboli*. Komunikacja zapośredniczona jest nacechowana kulturowo i indywidualnie (płeć, wiek,

---

* T. Goban-Klas, *Komunikowanie i media*, s. 3, http://users.uj.edu.pl/~usgoban/files/socjologia_mediow_zarys.pdf (dostęp: 12.12.2019).

osobowość, poziom inteligencji). Mechanizmy psychologiczne oraz czynniki związane z zachowaniami ingracjacyjnymi wpływają na to, że osoby poznane w Internecie są postrzegane jako miłe i sympatyczne. Opisane czynniki oraz niemożność pełnej oceny charakteru i intencji partnerów sieciowej interakcji stanowią źródło deformacji w postrzeganiu tych osób, co może skutkować nadmiernym zaufaniem wobec nieznanych ludzi czy problemami w komunikacji. Wizerunek innego użytkownika Internetu jest budowany na podstawie własnych pozytywnych doświadczeń. Czynnikiem wzmacniającym ten efekt jest charakter komunikacji zapośredniczonej, ograniczającej możliwość obierania sygnałów kanałem niewerbalnym (mowa ciała). Bywa, że użytkownik mediów społecznościowych przyjmuje do grona znajomych osoby, których nie zna lub które nie istnieją (profile fikcyjne). Ogranicza to możliwość uzyskania dodatkowych informacji o tym użytkowniku od innych, znanych jej, osób.

Funkcjonowanie w przestrzeni internetowej wymaga szerokiej wiedzy na temat zagrożeń i zasad bezpiecznego korzystania z Internetu. Jest to wiedza o tym, jakie są narzędzia, metody i schematy działania przestępców lub osób, które mają złe intencje. Osoby lub grupy, sięgając po możliwości nowych technologii, wykorzystują naiwność, brak wiedzy swoich ofiar do uzyskania finansowych lub emocjonalnych korzyści. Zachowania te są ukierunkowane na zdobycie cudzych pieniędzy, sprawowanie kontroli nad inną osobą lub złośliwe działania zorientowane na zniszczenie mienia (warto wspomnieć, że w świecie cyfrowym mamy do czynienia z dobrami w formie niematerialnej – elektronicznej).

W tej książce opisano wybrane zagrożenia płynące z Internetu, są to: szeroko rozumiana cyberprzemoc oraz szczególne jej odmiany, takie jak: stalking, cyberstalking, hejt i hakerstwo.

Niestety ofiarami stalkingu i cyberstalkingu oraz hejtu są m.in. osoby wykonujące zawody tzw. zaufania publicznego. Do tej grupy zalicza się nauczycieli, dyrektorów szkół. Stalkerami i cyberstalkerami są zwykle byli partnerzy lub osoby znane z pracy. Złośliwe nękanie za pośrednictwem nowoczesnych środków komunikacji może również dotyczyć relacji między uczniami. Zjawisko hejtu dotyka zaś zarówno

nauczycieli, jak i uczniów. Dlatego tematyka ta znalazła swoje miejsce w prezentowanej czytelnikowi publikacji.

Rozdział pierwszy stanowi wprowadzenie w problematykę przemocy wirtualnej. Przedstawiono w nim wieloznaczność definicji oraz złożoność tego zjawiska. Szczególną grupą zagrożoną cyberprzemocą jest młode pokolenie użytkowników Internetu – dzieci i młodzież. Przeniesienie zachowań agresywnych z przestrzeni realnej do środowiska cyfrowego przynosi nie tylko wiele szkód wszystkim jego uczestnikom, tj. cyberofiarom, cyberświadkom i cybersprawcom, ale stawia także wyzwania dla pokolenia dorosłych, tj. rodziców, wychowawców, nauczycieli i terapeutów w zakresie zapobiegania i rozpoznawania zjawiska cyberprzemocy oraz pomocy w niwelowaniu jej negatywnych skutków. Nękanie innej osoby przez Internet jest niezwykle proste i przysparza ofierze ogromnych szkód w wymiarze psychologicznym i społecznym.

Każde z zagrożeń, mimo że dotyczy innego aspektu przemocy internetowej, odnosi się do działalności człowieka, który wykorzystuje to medium jako narzędzie agresji skierowane przeciwko osobom i grupom. Osoby stosujące agresję w sieci z jednej strony postrzegają to medium jako wolne od kontroli społecznej (która w tradycyjnym społeczeństwie przez normy reguluje funkcjonowanie jednostek), z drugiej zaś mają przekonanie o anonimowości swoich działań.

Rozdział drugi poświęcono specyficznej formie przemocy, jaką jest cyberstalking. Zachowania stalkerów i cyberstalkerów cechuje brak empatii, ukierunkowanie na własne cele i emocje. Wykorzystują oni narzędzia technologii komunikacyjnych do zastraszania i szantażowania swoich ofiar. Możliwość docierania do dużych grup odbiorców przez sieć oraz replikację treści powoduje, że ofiary czują się zagrożone upublicznieniem ich intymnej sfery życia oraz danych osobowych. Działania agresywne cyberstalkera mogą być połączone z hejtem. Zjawisko to jest obecne na wszystkich portalach i czatach umożliwiających swobodne wypowiadanie się ich użytkowników. Analizy rozmów internetowych ukazują, że komentarze hejterskie nie są częste, jednak są one mocno nasycone emocjami, dlatego są częściej dostrzegane przez uczestników rozmów internetowych. Na ten problem nakłada się po-

ważny kłopot związany z manipulacją informacją. Sieć jest przepełniona nieprawdziwymi informacjami i artykułami opracowywanymi przez inteligentne systemy. Odróżnienie tego, co realne i rzeczywiste, w przestrzeni Internetu staje się niemożliwe.

Grono specjalistów z zakresu bezpieczeństwa międzynarodowego i obronności państwa podkreśla, że obecnie cyberprzestrzeń jest przepełniona działaniami przestępczymi, wśród których wymienia się: szpiegostwo, cyberterroryzm, cyberagresję oraz hakerstwo. Z punktu widzenia statystycznego użytkownika sieci oraz obywatela naszego kraju szczególnie istotne z wyróżnionych obszarów są dwa ostatnie. W konsekwencji obok szeroko rozumianej cyberagresji w książce poruszone zostaną również zagrożenia związane z hakerstwem. Warto zaakcentować, że cyberprzestępczość z roku na rok staje się coraz bardziej wyrafinowana. Sprzyja temu rozwój nowych mechanizmów, np. sztucznej inteligencji, a także nieustanne dopracowywanie starych, dobrze sprawdzonych metod, takich jak phishing. Straty z tytułu nielegalnych działań hakerów sięgają poziomu bilionów dolarów rocznie. Szacuje się, że ponoszone koszty indywidualne i społeczne w dalszych latach będą nieustanie rosły.

Z myślą o studentach pedagogiki, przyszłych nauczycielach oraz pracownikach poradni, placówek oświatowych, szkolno-wychowawczych oraz resocjalizacyjnych w rozdziale trzecim wyjaśnione zostały podstawowe zagadnienia związane z hakerstwem, jego narodzinami oraz ewolucją. W pracy przedstawiony został również podział hakerstwa pod kątem form działania oraz efektów będących ich następstwem. Ukazano możliwe skutki działania hakerów w wybranych, a związanych z życiem pedagogów przestrzeniach. Szczególną uwagą otoczono środowisko szkolne, domowe oraz przestrzeń publiczną będącą udziałem każdego z uczniów.

Książka ta jest przeznaczona dla wszystkich użytkowników Internetu, którzy są zainteresowani tematyką zagrożeń płynących z sieci i sposobami radzenia sobie z nimi. Autorki mają świadomość, że oprogramowanie wykorzystywane przez przestępców komputerowych zmienia się i staje bardziej doskonałe, jednak zalecenia postępowania w sytuacji określonego agresywnego zjawiska oraz sprawców mają cha-

rakter uniwersalny. Książka zawiera przegląd aktualnej literatury poświęconej omawianej problematyce.

Mamy nadzieję, że lektura tej książki przyczyni się do pewnej refleksji i skłoni czytelnika do dalszych dociekań literaturowych oraz podjęcia działań na rzecz zwalczania negatywnych zjawisk w przestrzeni wirtualnej.

Autorki

Rozdział 1

Cyberprzemoc – zjawisko, skutki, zapobieganie

Margaret Mead w 1978 r. oceniła ówczesne zmiany społeczno-kulturowe, pisząc: „Teraz wchodzimy w okres nieznany dotąd historii, w którym młodzi zyskują sobie unikalny autorytet w swym prefiguratywnym rozumieniu nieznanej jeszcze nikomu przyszłości”[1]. Po pół wieku jej ocena nabiera nowego znaczenia w kontekście współczesnej rzeczywistości, w której zagadkowe dzieci[2] tłumaczą wirtualny świat swoim rodzicom i dziadkom. Jednak autorytet młodych nie opiera się na ich kompetencjach i mądrości. W obliczu zagrożeń związanych z funkcjonowaniem w wirtualnej rzeczywistości ukazuje się niewystarczające przygotowanie młodych pokoleń, by rzeczywiście zrozumieć otaczający świat i wypełnić go wartościami umożliwiającymi prawidłowe funkcjonowanie społeczne.

Kontekst technologiczny

Według raportu badawczego „EU Kids Online 2020” większość dzieci w 19 krajach europejskich korzysta ze swoich smartfonów codziennie lub „prawie cały czas”. Oznacza to znaczny wzrost zarówno odsetka

---

[1] M. Mead, *Kultura i tożsamość. Studium dystansu międzypokoleniowego*, tłum. J. Hołówka, PWN, Warszawa 1978, s. 25.

[2] Termin użyty przez Mead jako synonim kultury prefiguratywnej, tzw. kultura zagadkowych dzieci.

dzieci używających smartfonów, jak i liczby dzieci korzystających z Internetu w porównaniu z poprzednim raportem z 2010 r.[3]

Obecnie posługiwanie się Internetem jest nieodłączną częścią codziennego życia dzieci. Według najnowszego raportu badawczego NASK z ogólnopolskiego badania uczniów pn. „Nastolatki 3.0" blisko 96% młodych ludzi korzysta z sieci każdego dnia. Sporadyczne użytkowanie Internetu („kilka razy w tygodniu" czy „kilka razy w miesiącu") zadeklarowało niespełna 4% badanych. Online jest codziennie prawie każdy nastolatek w Polsce, niezależnie od wieku, typu szkoły i płci. Nastolatki używają sieci samodzielnie już od siódmego roku życia, a im młodsze pokolenie, tym ten kontakt następuje wcześniej[4].

Do takiej popularności Internetu wśród młodych przyczyniło się wiele czynników, m.in. upowszechnienie dostępu przez obniżenie cen sprzętu komputerowego i opłat telekomunikacyjnych, ale także rozwój technologii Internetu, określanych jako Web 2.0. Pojęciem tym nazywa się serwisy internetowe powstałe po 2001 r. Podstawą ich działania jest treść generowana przez użytkowników danego serwisu. Wśród technologii Web 2.0 można wyróżnić kanały RSS, blogi, podcasty, wiki, systemy tagowania, newslettery, fora internetowe i media społecznościowe. Głównym założeniem mediów społecznościowych jest funkcjonowanie w taki sposób, by umożliwiać wszystkim uczestnikom dialog oraz interakcję. Zaliczają się do nich nie tylko popularne portale społecznościowe, ale również blogi, fora dyskusyjne, platformy do udostępniania zdjęć czy strony, na których można umieścić opinie[5] i komentarze.

Web 2.0 i media społecznościowe pozwalają użytkownikom Internetu tworzyć treści i upubliczniać je w sieci. Każdy może być odbiorcą tych treści, oceniać je, komentować czy wyrażać swoją opinię. Web 2.0 umożliwia również interakcję z innymi użytkownikami stron interneto-

---

[3] D. Smahel i in., *EU Kids Online 2020: Survey results from 19 countries*, EU Kids Online 2020, https://doi.org/10.21953/lse.47fdeqj01ofo (dostęp: 10.04.2020).

[4] M. Bochenek, R. Lange (red.), *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów*, Państwowy Instytut Badawczy NASK, Warszawa 2019, s. 6, 9, https://www.nask.pl/download/30/2601/RAPORTNASTOLATKI2019.pdf (dostęp: 10.04.2019).

[5] *Social media (media społecznościowe)*, blog marketingwsieci.pl, https://marketingwsieci.pl/slownik-e-marketingu/social-media/ (dostęp: 22.07.2019).

wych czy serwisów społecznościowych przez nawiązywanie kontaktów, możliwość prowadzenia rozmów w czasie rzeczywistym (np. w formie rozmów tekstowych, głosowych, wysyłania obrazów, używania komunikatorów itp.) czy współdzielenie i współtworzenie treści. Wszystko to bez konieczności posiadania zaawansowanej wiedzy i umiejętności technologicznych. Właśnie te cechy przyczyniły się do wzrostu popularności Web 2.0 i mediów społecznościowych wśród młodych użytkowników Internetu.

Jak wynika z badań, swój profil w przynajmniej jednym serwisie społecznościowym utworzyło od 72,6%[6] do 94,6%[7] badanych nastolatków. Jednocześnie warto zwrócić uwagę, że takie profile ma prawie połowa najmłodszych badanych w wieku 9–10 lat[8]. Należy zatem zaznaczyć, że spory odsetek młodych ludzi zakłada konta w różnych portalach, wbrew ograniczeniom wiekowym określonym w regulaminach portali.

Współczesna młodzież jest stale „podłączona", korzystając z Internetu codziennie, średnio przez ok. cztery godziny. Młodzież używa do tego celu głównie smartfona[9]. Bycie online jest dziś możliwe wszędzie i w każdym momencie, a najwygodniejszym narzędziem łączenia się jest będący zawsze pod ręką telefon komórkowy.

Oprócz komunikacji i rozrywki nastolatki używają Internetu również do kreowania własnego wizerunku czy poszukiwania tożsamości. Według wspomnianego raportu badawczego „Nastolatki 3.0" uczniowie chętnie wykorzystują do tego celu media społecznościowe, udostępniając na swoich profilach treści związane z prezentacją własnego wizerunku oraz informacje o życiu towarzyskim i społecznym. W szczególności chodzi o zdjęcia: zarówno przedstawiające własny wizerunek (prezentuje

---

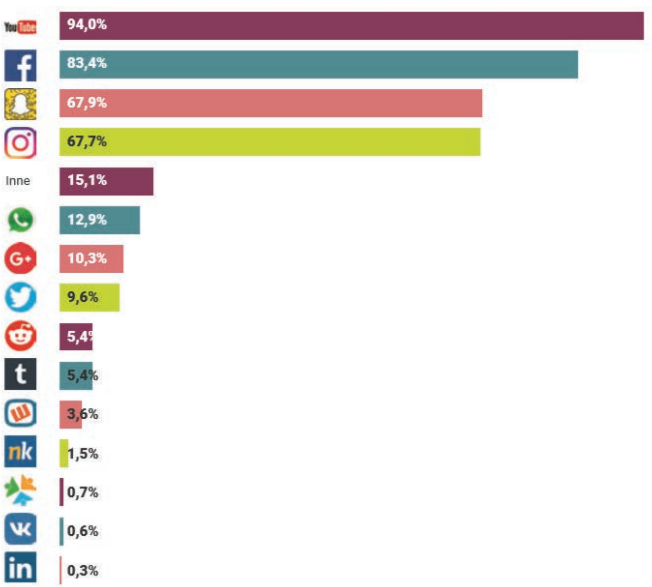
[6] J. Pyżalski i in., *Polskie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski*, Wydawnictwo Naukowe UAM, Poznań 2019, s. 21, https://fundacja.orange.pl/files/user_files/EU_Kids_Online_2019_v2.pdf (dostęp: 22.07.2019).

[7] *Nastolatki 3.0. Wybrane wyniki ogólnopolskiego badania uczniów w szkołach*, Państwowy Instytut Badawczy NASK, 2016, s. 11, https://akademia.nask.pl/badania/RAPORT%20-%20Nastolatki%203.0%20-%20wybrane%20wyniki%20bada-%C5%84%20og%C3%B3lnopolskich.pdf (dostęp: 10.04.2019).

[8] J. Pyżalski i in., dz. cyt., s. 28.

[9] Por. M. Bochenek, R. Lange (red.), dz. cyt., s. 9, 11.

je blisko 58% badanych), jak i ukazujące znajomych (umieszcza je blisko 30% młodzieży) oraz inne samodzielnie wykonane zdjęcia (publikuje je 44,5% badanych). Istnieje wiele rodzajów aplikacji i witryn dostępnych za darmo, które dają użytkownikom możliwość wyszukiwania osób oraz anonimowego udostępniania lub publikowania informacji na ich temat. Na rysunku 1 przestawiono na podstawie opinii młodzieży w badaniu „Nastolatki 3.0" najbardziej popularne wśród dzieci i młodzieży media społecznościowe.



Rysunek 1. Najbardziej popularne media społecznościowe wśród młodych użytkowników Internetu (źródło: M. Bochenek, R. Lange (red.), *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów*, Państwowy Instytut Badawczy NASK, Warszawa 2019, s. 19)

Młodzież jako najczęściej używane media społecznościowe wskazała:

- YouTube: platformę udostępniania wideo, która umożliwia użytkownikom bezpłatne publikowanie, ocenianie i komentowanie filmów (http://youtube.com);

-  **Facebook i Facebook Live:** serwis społecznościowy dostępny na wielu różnych platformach medialnych; zarejestrowani użytkownicy mogą tworzyć własne profile, sieci i grupy, dzielić się wiadomościami, zdjęciami i filmami oraz korzystać z aplikacji, a także komentować i oceniać treści innych użytkowników Facebooka (https://www.facebook.com);
-  **Snapchat:** aplikację na urządzenia mobilne umożliwiającą wysyłanie błyskawicznych wiadomości, przesyłanie i udostępnianie zdjęć i krótkich filmów, które mają zostać usunięte wkrótce po dostarczeniu (10 sekund) lub po 24 godzinach, jeśli zostały dodane do „My Story" (https://www.snapchat.com);
-  **Instagram:** fotograficzny serwis społecznościowy, który umożliwia użytkownikom edycję zdjęć i filmów, stosowanie do nich filtrów cyfrowych oraz udostępnianie ich w innych serwisach społecznościowych (https://www.instagram.com);
-  **WhatsApp:** aplikację do przesyłania wiadomości, która umożliwia użytkownikom wysyłanie wiadomości tekstowych, zdjęć i filmów (https://www.whatsapp.com);
-  **Google Plus:** serwis społecznościowy firmy Google, w którym użytkownicy, posiadając swoje profile, mogli publikować wiadomości, zdjęcia, filmy i łączyć się ze znajomymi; ze względu na małą popularność został zamknięty wśród zwykłych użytkowników w 2019 r.
-  **Twitter:** platformę mikroblogową, która umożliwia użytkownikom wysyłanie, czytanie i odpowiadanie na „tweety", czyli krótkie (do 140 znaków) wiadomości tekstowe (https://twitter.com);
-  **Reddit:** witrynę, która przechowuje wiadomości społecznościowe i ocenia treści internetowe oraz wątki dyskusyjne; każdy użytkownik może zgłosić link do treści w sieci, który później jest poddawany głosowaniu przez innych użytkowników (https://www.reddit.com/r/Polska);

- **Tumblr:** platformę mikroblogową pozwalającą użytkownikom publikować „tumblelog", czyli krótkie wpisy na blogu w kategoriach: tekst, obrazek, klip wideo, plik dźwiękowy, link, cytat, dialog (https://www.tumblr.com/);
- **Wykop:** polski serwis internetowy będący ideową kopią amerykańskiego digg.com; pozwalający polecać swoim znajomym ciekawe informacje znalezione w Internecie, które mogą być następnie oceniane i komentowane (https://www.wykop.pl).

Wobec wcześniej przedstawionych informacji dotyczących użytkowania Internetu przez młodzież zaskakujące może być to, że nastolatki – choć zanurzone w cyfrowym świecie – mają dość niewielkie kompetencje informacyjne[10]. Młode osoby najgorzej radzą sobie z poszukiwaniem i selekcją czy weryfikacją informacji zamieszczonych online. Choć w literaturze nazywa się ich „cyfrowymi tubylcami" czy *tech savvy* (z ang. „znający się na technologii"), to jednak przeważnie nie są oni – poza biegłym obsługiwaniem narzędzi telekomunikacyjnych – kompetentnymi użytkownikami Internetu.

Młodzi ludzie bardzo często deklarują, że Internet poznają w drodze samoedukacji, gdyż w sieci brakuje kompetentnych dorosłych przewodników będących wyznacznikiem wartości i wzorów godnych naśladowania[11].

Nieustanny rozwój oraz wszechobecność technologii sieciowych wpływa na codzienny sposób funkcjonowania współczesnych dzieci i nastolatków, których świat społeczny powiększył się o wymiar „online", nie mniejszy – a być może nawet rozleglejszy – niż ten „offline". Nie dziwi więc, że młode osoby przejawiają w Internecie zachowania ze świata realnego, bo ten wirtualny jest dla nich tylko jego przedłu-

---

[10] Kompetencje informacyjne, czyli umiejętność określania własnych potrzeb informacyjnych, lokalizowania potrzebnej informacji, jej krytycznej oceny i efektywnego wykorzystania.

[11] Zob. *Raport z badania Nastolatki 3.0*, NASK – Instytut Badawczy, Warszawa 2017, s. 15–18, https://akademia.nask.pl/publikacje/Raport_z_badania_Nastolatki_30.pdf (dostęp: 10.04.2019).

żeniem. Cyfrowe media i aplikacje pozwalają dzieciom komunikować się, relaksować, przezwyciężać nudę, prezentować swoją kreatywność, kontaktować się z rówieśnikami i dzielić się swoimi uczuciami. Mogą jednak stać się także miejscem i narzędziem cyberprzemocy.

Przemoc czy agresja elektroniczna? Próba definicji

Zachowania agresywne dorastającej młodzieży to znany i wszechobecny problem społeczny, jednak zjawisko określane w Polsce terminami, takimi jak „agresja elektroniczna", „cyberprzemoc", „cyberagresja", „cyberprześladowanie", „cyberdręczenie" czy „cybernękanie", pojawiło się w powszechnym użyciu zaledwie kilkanaście lat temu. Zagadnienie cyberprzemocy wśród dzieci i młodzieży staje się problemem międzynarodowym, uwarunkowanym cechami tożsamości tzw. globalnego nastolatka, którego osobowość kształtuje kultura popularna, szczególnie aczasowy i aprzestrzenny Internet. Z tego powodu nastolatki całego globu i ich styl życia są znacząco bardziej podobne do siebie niż do pokolenia ich rodziców[12].

Pojęcie elektronicznej agresji rówieśniczej jest określane w języku angielskim terminem „cyberbullying". Po raz pierwszy zostało ono użyte przez Billa Belseya w 2004 r.[13], który definiował je jako „wykorzystanie technologii informacyjnych i komunikacyjnych do wspierania zamierzonego, powtarzającego się i wrogiego zachowania jednostki lub grupy, mającego na celu wyrządzenie krzywdy innym"[14].

Do dzisiaj nie przyjęto uniwersalnej definicji. Punktem wyjścia w interpretacji znaczenia tego terminu jest rozważanie osobnych znaczeń słów „cyber" i „bullying", a następnie łączenie ich w celu uzyskania spójnego opisu tego zjawiska. Przedrostek „cyber" można po prostu

---

[12] Koncepcja „globalnego nastolatka" została szerzej opisana przez Zbyszka Melosika, *Edukacja, młodzież i kultura współczesna: kilka uwag o teorii i praktyce pedagogicznej*, „Chowanna" 2003, 1, s. 26–28.

[13] J. Barlińska, A. Szuster, *Cyberprzemoc. O zagrożeniach i szansach na ograniczenie zjawiska wśród adolescentów*, Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 2014, s. 13.

[14] B. Belsey, *Always on? Always aware!*, strona internetowa poświęcona problemowi cyberprzemocy, http://www.cyberbullying.ca/ (dostęp: 22.08.2019).

opisać jako formę komunikacji i aktywności wykonywanych przy użyciu urządzeń cyfrowych, przy czym współcześnie najczęściej określenie to odnosi się do przestrzeni Internetu. Zdefiniowanie słowa „bullying" (z ang. „nękanie, dręczenie"), szczególnie w języku polskim, stanowi trudniejsze zadanie, przypisuje się mu bowiem wiele znaczeń, dotyczących różnych typów działań o charakterze agresywnym i przemocowym, tj. zastraszanie, znęcanie, nękanie, prześladowanie, grożenie, upokarzanie. W literaturze przyjęto definicję tradycyjnego dręczenia, czyli **intencjonalnego, krzywdzącego, powtarzającego się działania w relacji, w której agresor lub agresorzy mają nad ofiarą przewagę**. Dan Olweus będący pionierem badań nad przemocą szkolną uznał bullying za specyficzny rodzaj agresji (przemocy) stosowanej przez jedną lub kilka osób wobec ofiary. Według badacza o dręczeniu można mówić, gdy „ofiara musi znosić negatywne, skierowane przeciwko sobie, powtarzające się i długotrwałe działania jednej lub kilku osób, przy czym osoba poszkodowana nie jest w stanie przed nimi samodzielnie się obronić"[15]. Tym samym wyróżnił trzy konieczne cechy negatywnych zachowań wskazujących na przemoc szkolną:

- intencjonalność;
- powtarzalność;
- nierównowagę sił między sprawcą (sprawcami) a ofiarą.

Intencją agresywnego działania może być chęć skrzywdzenia, przestraszenia, zawstydzenia czy poniżenia innej osoby. **Brak równowagi sił** wynika z przewagi liczebnej, fizycznej (wzrost, waga, siła, umiejętność użycia siły itp.), intelektualnej (wiek, upośledzenie umysłowe itp.), psychicznej (poziom lęku, samoakceptacja wraz z pozytywną, ale i adekwatną samooceną, poczucie tożsamości, poczucie sprawstwa, poczucie kontroli i samokontroli itp.) i społecznej (pozycja w grupie). **Powtarzalność,** czyli wielokrotne i trwające określony czas działania agresywne, przez co wywołują u ofiary lęk i degradację jej dobrostanu psychicznego.

---

[15] Por. D. Olweus, *A profile of bullying at school*, „Educational Leadership" 2003, 60(6), s. 12.

Definicję tradycyjnego dręczenia (bullyingu) Olweusa rozwinął Robert S. Tokunaga w odniesieniu do pojęcia cyberbullyingu, które określił jako „każde zachowanie dokonywane za pośrednictwem mediów elektronicznych lub cyfrowych przez osoby lub grupy, które wielokrotnie komunikują wrogie lub agresywne wiadomości z zamiarem wyrządzenia krzywdy lub dyskomfortu innym”[16]. Definicja ta akcentuje kilka ważnych cech cyberprzemocy, tj. komponent technologiczny oraz cechy tradycyjnego aktu dręczenia: wrogi charakter czynu, intencję dręczenia, a także powtarzalność. Jednak propozycja Tokunagi nie akcentuje wyraźnie ostatniej cechy z trzech identyfikujących przemoc, tj. przewagi sił sprawcy.

Definicję uwzgledniającą wszystkie kryteria identyfikujące cyberprzemoc zaproponowali Peter K. Smith i współpracownicy, opisując „cyberbullying” jako „agresywne umyślne działanie prowadzone przez grupę lub osobę, przy użyciu elektronicznych form kontaktu, wielokrotnie i przez dłuższy czas przeciw ofierze, która nie może się łatwo obronić”[17].

Powszechne korzystanie z urządzeń elektronicznych i mediów przez młodzież i wykorzystywanie ich także do atakowania kogoś właściwie w dowolnym miejscu i w dowolnym momencie jest, obok znamion tradycyjnej przemocy, charakterystyczną cechą cyberprzemocy.

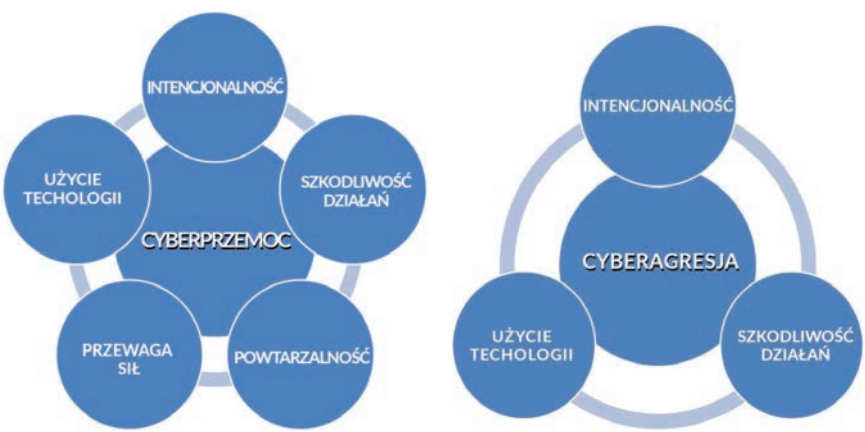
Z przywołanych definicji wynika, że najczęściej cyberprzemoc (cyberbullying) traktuje się jako rodzaj przemocy tradycyjnej (bullying), której celem jest intencjonalne krzywdzenie słabszej osoby, jednak przemoc ta jest stosowana za pomocą narzędzi technologii informacyjno-komunikacyjnych. Należy przy tym zaznaczyć, że nie każde działanie przemocowe z użyciem narzędzi cyfrowych pozwala uznać je za cyberprzemoc. Mimo że wiele negatywnych cyberzachowań jest ze sobą skorelowanych i wywołuje negatywne skutki, zjawiska te różnią się od siebie, szczególnie w odniesieniu do nierównowagi mocy i chęci wy-

---

[16] R.S. Tokunaga, *Following you home from school: A critical review and synthesis of research on cyberbullying victimization*, „Computers in Human Behavior” 2010, 26(3), s. 278.

[17] P.K. Smith i in., *Cyberbullying: Its nature and impact in secondary school pupils*, „The Journal of Child Psychology and Psychiatry” 2008, 49(4), s. 376.

rządzenia krzywdy. Podobnie jak w przypadku różnic w definiowaniu przemocy i agresji tradycyjnej, tak i w środowisku cyfrowym odróżnia się cyberprzemoc i **cyberagresję** (ang. *cyberaggression*). Cyberagresja odnosi się bowiem do umyślnych szkodliwych działań, które są podejmowane za pomocą technologii, ale które nie obejmują nierównowagi mocy lub powtarzalności, charakterystycznej dla cyberprzemocy. Niektórzy badacze rozróżniają także „niegrzeczne/nieuprzejme zachowania występujące za pośrednictwem technologii informacyjnych i komunikacyjnych (ICT), takich jak e-mail lub SMS-y", określając je jako **cyberniegrzeczność** czy też **cybergrubiaństwo** (ang. *cyber incivility*)[18]. Mimo że są to zachowania dewiacyjne, agresywne, krzywdzące i naruszające normy w zakresie wzajemnego szacunku, to jednak cechują się niską intensywnością i niejednoznacznym zamiarem zaszkodzenia celowi.



Rysunek 2. Cyberprzemoc a cyberagresja (opracowanie własne)

Aby zatem móc stwierdzić, że dane działanie nosi oznaki cyberprzemocy, musi odznaczać się ono wszystkimi cechami typowymi dla tego rodzaju przemocy: intencjonalnością, powtarzalnością, przewagą

[18] R.M. Kowalski, S.P. Limber, A. McCord, *A developmental approach to cyberbullying: Prevalence and protective factors*, „Aggression and Violent Behavior" 2019, 45, s. 21.

sił, a także wykorzystaniem narzędzi TI. Trzeba mieć jednak świadomość, że właściwości typowe dla przemocy tradycyjnej mogą uwidaczniać się w odmienny sposób.

Najbardziej problematycznym elementem opisu cyberprzemocy jest intencjonalność. Trudność wynika z właściwości komunikacji zapośredniczonej, tj. brak kontaktu bezpośredniego uczestników komunikacji i zredukowane możliwości obserwowania reakcji osób przekazywanych kanałem pozawerbalnym (mimika, gest, ton głosu itp.). Ten fakt może w niektórych przypadkach wpływać na podejmowanie pewnych aktywności w sieci, które w sposób nieświadomy wywołują poczucie krzywdy u innych osób. Jednak w przeważającej liczbie przypadków sprawca ma intencję skrzywdzenia ofiary i osiąga swój cel.

Cyberprzemoc staje się bardziej uporczywą wersją tradycyjnych form nękania, wykraczającą poza granice fizyczne (np. szkoły, boiska sportowego, świetlicy itp.), przez co ofiara często nie znajduje od niej chwili wytchnienia. Nawet mury domu nie stanowią bariery ochronnej dla ofiary wrogich działań. Cyberprzemoc daje zastraszającemu moc zawstydzenia lub skrzywdzenia ofiary przed całą społecznością online, zwłaszcza w ramach portali społecznościowych. Dzięki popularności mediów społecznościowych komentarze, zdjęcia, posty i treści udostępniane przez osoby prywatne mogą być często przeglądane przez znajomych i nieznajomych. Treści, które dana osoba udostępnia online – zarówno osobiste, jak i wszelkie treści szkodliwe – tworzą rodzaj stałego, publicznego zapisu jej poglądów, działań i zachowań. Ten publiczny zapis może być uważany za sieciową reputację, widoczną i dostępną przez długi czas dla wszystkich użytkowników Internetu, w tym dla nauczycieli, pracodawców, szkół wyższych i innych osób, które mogą daną osobę poznawać i „sprawdzać" w przyszłości. Cybernękanie może zaszkodzić reputacji online wszystkich zaangażowanych osób – nie tylko ofiary, ale także sprawcy i wspierających go świadków. Cyberbullying jest zatem wyjątkowo dolegliwy, ponieważ może być [19]:

---

[19] Por. stopbullying.gov, oficjalna strona internetowa rządu Stanów Zjednoczonych, https://www.stopbullying.gov/cyberbullying/what-is-it/index.html (dostęp: 11.11.2019).

- **Uporczywy** – urządzenia cyfrowe umożliwiają natychmiastową i ciągłą (całodobową) komunikację, więc osobom doświadczającym cyberprzemocy może być trudno znaleźć wytchnienie. Na uporczywość wpływają cechy cyberprzemocy warunkowane właściwościami technologicznymi urządzeń cyfrowych, tj.[20]:
  - **duży zasięg** – o ile „tradycyjna" przemoc odbywa się w stosunkowo niedużej grupie, np. w klasie, szkole lub na podwórku, przez co naocznych świadków jest zazwyczaj niewielu, a informacje o akcie agresji docierają do niewielkiej liczby osób i trwają krótko (gdyż opierają się na ustnym przekazie), o tyle akty cyberprzemocy mogą być unaocznione (przez rejestrację) i udostępnione szerokiej publiczności w Internecie;
  - **szybkie rozpowszechnianie i kopiowalność materiałów** – rejestracja aktów przemocy i szybkość rozpowszechniania materiałów w Internecie (np. przez udostępnianie) sprawia, że dużo trudniej jest powstrzymać rozprzestrzenianie się krzywdzących materiałów, bezpośrednimi świadkami przemocy może stać się zatem duża grupa osób. Czasem świadkowie zdarzeń mogą udostępniać szkodliwe treści, a nawet je modyfikować, będąc nieświadomymi zamierzonego przez sprawcę celu skrzywdzenia ofiary;
  - **anonimowość sprawcy i świadków** – poczucie anonimowości w Internecie znacznie ośmiela sprawców, którzy spodziewając się, że nie poniosą odpowiedzialności za swoje czyny, podejmują działania, na jakie być może nie odważyliby się w sytuacji „twarzą w twarz". Ofiary mogą z kolei nawet nie wiedzieć, kto wyrządza im krzywdę, a tym samym mają mniejszą możliwość obrony i nękanie staje się bardziej uciążliwe. Obciążający dla ofiary może być także brak możliwości identyfikacji tożsamości widzów – ile osób i kto mógł zobaczyć krzywdzący ją materiał;

---

[20] Por. A. Borkowska, *Cyberprzemoc – włącz blokadę na nękanie*, Państwowy Instytut Badawczy NASK, Warszawa 2019, s. 13–14, https://www.gov.pl/attachment/6d56e2fc-abfb-4983-b5ac-578064342c6a (dostęp: 17.08.2019).

  - **brak kontroli dorosłych** – działania przemocowe odbywają się w przestrzeni Internetu, w której rodzice i wychowawcy są najczęściej nieobecni. Brak kontroli dorosłych jest z jednej strony czynnikiem ułatwiającym nastolatkom decyzję o podjęciu aktu przemocy, z drugiej strony trudniej jest rodzicom i nauczycielom zauważyć taki problem i odpowiednio zareagować. W rezultacie młode ofiary cyberprzemocy często samotnie borykają się ze skutkami działań agresywnych;
  - **nieograniczona możliwość nękania** – ofiary cyberprzemocy są stale narażone na atak, niezależnie od miejsca czy pory dnia. Dom rodzinny nie jest już bezpiecznym miejscem odcinającym zasięg i pole działania sprawcy. Przebywając w domu, ofiara nadal może być nękana za pośrednictwem różnych urządzeń cyfrowych oraz różnych technik dręczenia.
- **Trwały** – większość informacji przekazywanych drogą elektroniczną jest stale dostępna dla szerokiej publiczności, dopóki nie zostanie zgłoszona odpowiednim służbom i usunięta. Negatywna reputacja online, w tym sprawców i wspierających go świadków, może mieć w przyszłości wpływ na przyjęcie na studia, zatrudnienie i inne dziedziny życia.
- **Trudny do zauważenia** – ponieważ nauczyciele i rodzice często są nieobecni w sieci albo też nie współużytkują wybranych przez dzieci usług telekomunikacyjnych; bliscy nie kontrolują wzajemnie urządzeń cyfrowych, przez co trudniej zaobserwować, kiedy i jak dochodzi do cybeprzemocy.

Tradycyjni prześladowcy zazwyczaj osiągają przewagę na podstawie wyglądu i siły fizycznej, cyberprześladowcy nie muszą natomiast martwić się swoim wyglądem. Zamiast tego mogą bardziej skoncentrować się na sile emocjonalnej, łatwości manipulacji i dominacji. W cyberprzestrzeni przewaga fizyczna przestaje mieć zatem znaczenie, o nierównowadze sił zaczyna zaś decydować lepsza umiejętność wykorzystywania mediów oraz zdolność do zachowania anonimowości w cyberprzestrzeni czy też możliwość natychmiastowego rozpowszechniania treści.

Nie da się jednak wykluczyć tego, że również w przestrzeni wirtualnej cechy przemocy mogą być realizowane w tradycyjny sposób, przez co repertuar możliwych kontekstów cyberprzemocy jest znacznie szerszy i trudniejszy do właściwego rozpoznania. Dla porównania w tabeli 1 dokonano zestawienia cech przemocy i cyberprzemocy.

Tabela 1. Porównanie cech konstytutywnych przemocy tradycyjnej i cyberprzemocy

	Przemoc (bullying)	Cyberprzemoc (cyberbullying)
Intencjonalność	• wynika najczęściej ze świadomej chęci skrzywdzenia ofiary	• wynika najczęściej ze świadomej chęci skrzywdzenia ofiary; • część badań wskazuje, że ze względu na charakter komunikacji zapośredniczonej (m.in. redukcję sygnałów niewerbalnych) niektórzy sprawcy nieświadomie krzywdzą inne osoby
Powtarzalność	• wynika z wielokrotnego działania sprawców	• wynika z wielokrotnego działania sprawców; • może wynikać z cech samego materiału zamieszczonego w Internecie, w wyniku których ofiara doświadcza powtarzanej wiktymizacji tj.: – duży zasięg, – szybkie rozpowszechnianie i kopiowalność, – anonimowość, – brak kontroli dorosłych, – nieograniczona możliwość nękania
Nierównowaga sił	• wynika z przewagi liczebnej, fizycznej, intelektualnej, psychicznej lub społecznej	• wynika z przewagi liczebnej, intelektualnej, psychicznej lub społecznej; • może wynikać z większej kompetencji w zakresie wykorzystywania narzędzi TIK, zdolności do zachowania anonimowości w cyberprzestrzeni czy też cech samego materiału zamieszczonego w Internecie, potęgujących skalę krzywdy ofiary

Źródło: opracowanie własne na podstawie: J. Pyżalski, *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Oficyna Wydawnicza IMPULS, Kraków 2012, s. 124.

W Polsce zjawisko cyberprzemocy definiuje się jako „przemoc z użyciem technologii informacyjnych i komunikacyjnych”[21], przy czym najczęściej wykorzystywanymi narzędziami są Internet i telefony komórkowe. Jej celem i nieuniknionym skutkiem jest wyrządzenie krzywdy innej osobie.

Podobne rozumienie tego pojęcia prezentuje Jacek Pyżalski, nazywając „agresją elektroniczną” „wszystkie akty agresji, w których narzędziem realizacji są telefony komórkowe i internet”[22], jednak autor ten odróżnia „agresję elektroniczną” (pojedyncze akty przemocy w sieci) od „cyberbullyingu”, będącego działaniem intencjonalnym, trwającym dłuższy czas, przed którym ofiara nie może się obronić.

Według Fundacji Dajemy Dzieciom Siłę „cyberbullying” to „wysyłanie i publikowanie szkodliwych treści lub obrazów przy użyciu Internetu lub innych cyfrowych narzędzi komunikacyjnych”[23].

Mimo że najbardziej licznymi użytkownikami technologii są młodzi ludzie, to jednak zacytowane powyżej definicje zamieszczone w polskim piśmiennictwie naukowym nie dotyczą wyłącznie rówieśniczej agresji elektronicznej. Warto zaznaczyć wyraźne odniesienie do przemocy rówieśniczej z użyciem technologii informacyjnych i komunikacyjnych, jakie prezentuje Pyżalski. Autor proponuje stosowanie w Polsce jako synonimu cyberbullyingu pojęcia „mobbing elektroniczny”, rozumianego jako „forma elektronicznej agresji rówieśniczej, w której zarówno sprawca, jak i ofiara są młodymi osobami, będącymi często uczestnikami tej samej grupy społecznej”[24]. Mobbing elektroniczny można odnosić zatem do elektronicznej agresji rówieśniczej, polegającej na realizacji zachowań przemocowych w obrębie funkcjonującej grupy rówieśniczej zarówno w przestrzeni realnej, jak i wirtu-

---

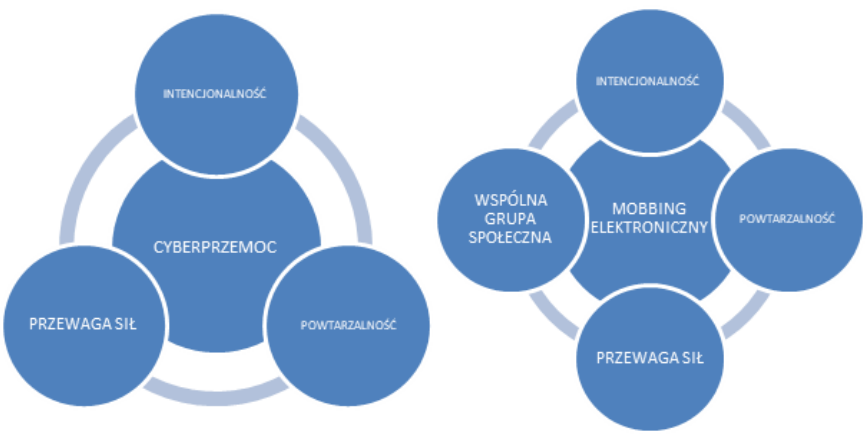
[21] Ł. Wojtasik, *Cyberprzemoc – charakterystyka zjawiska*, w: Ł. Wojtasik (red.), *Jak reagować na cyberprzemoc? Poradnik dla szkół*, wydanie II poprawione, Fundacja Dajemy Dzieciom Siłę, s. 6, https://www.ore.edu.pl/wp-content/plugins/download-attachments/includes/download.php?id=3167 (dostęp: 11.11.2019).

[22] J. Pyżalski, *Agresja elektroniczna wśród dzieci i młodzieży*, GWP, Sopot 2011, s. 41.

[23] *Cyberbullying*, definicja pojęcia, oficjalna strona internetowa Fundacji Dajemy Dzieciom Siłę, https://fdds.pl/baza_wiedzy/cyberbullying/ (dostęp: 5.10.2019).

[24] Por. J. Pyżalski, *Agresja elektroniczna wśród…*, s. 54.

alnej. Jednak nie każdy akt elektronicznej agresji rówieśniczej można nazwać mobbingiem elektronicznym. O kwalifikacji określonych cyfrowych form rówieśniczych zachowań agresywnych jako mobbingu elektronicznego będą decydować trzy specyficzne cechy charakteryzujące tradycyjną przemoc i cyberprzemoc oraz dodatkowa cecha wyróżniająca przemoc rówieśniczą (najczęściej przemoc szkolną) i mobbing elektroniczny (elektroniczną agresję rówieśniczą).



Rysunek 3. Cechy cyberprzemocy i mobbingu elektronicznego (opracowanie własne)

W tym przypadku obok opisanych wyżej cech przemocy i cyberprzemocy (tj. intencjonalność, powtarzalność, nierównowaga sił) powinien zaistnieć dodatkowy warunek, jakim jest akt agresji w obszarze znanej grupy społecznej. Ofiarą agresji elektronicznej mogą być rówieśnicy sprawców, znani ze świata realnego lub wirtualnego, a działania sprawców najczęściej opierają się na udostępnianiu agresywnych treści w obrębie określonych grup internetowych, do których należy ofiara. Autorki proponują zatem opisywanie cyberprzemocy rówieśniczej jako: **wykorzystywanie technik informacyjnych i komunikacyjnych przez rówieśników do świadomego, wielokrotnego i wrogiego zachowania się osoby lub grupy osób, mających na celu krzywdzenie innego uczestnika (lub uczestników) funkcjonujących w obrębie tej samej grupy,** natomiast pojęcie „cyberprzemoc" w tym opracowaniu

będzie rozumiane jako **wykorzystywanie technik informacyjnych i komunikacyjnych do świadomego, wielokrotnego i wrogiego zachowania się osoby lub grupy osób, mających na celu krzywdzenie innej osoby lub innych osób.**

Typy cyberagresji

Psychologowie, opisując zachowania agresywne ludzi, wymieniają różne typy agresji. Ze względu na źródło pobudzenia wyróżnia się **agresję wrogą (reaktywną) i instrumentalną (proaktywną)**. Agresja wroga jest motywowana gniewem, złością, odczuwaniem wobec ofiary niechęci czy nienawiści, a wyrządzenie krzywdy ofierze jest bezpośrednim celem działania. W agresji instrumentalnej krzywdzenie innych jest jedynie środkiem w osiągnieciu zamierzonego celu[25]. Jeśli pobudzenie i działanie agresywne wynika z emocji gniewu, to mówi się o **agresji gniewnej**. Jeśli agresja występuje w odpowiedzi na konkretną sytuację, to określa się ją jako **agresję reaktywną** lub impulsywną, w tym przypadku sprawca na ogół nie planuje swojego działania[26].

Ze względu na różne poziomy przejawiania się agresji (i formę jej realizacji) rozróżnia się trzy typy zachowań agresywnych: **agresję fizyczną, werbalną i „nie wprost"**, zwaną także społeczną, psychiczną[27] czy relacyjną. Agresja fizyczna jest rozumiana jako naruszanie granic ciała przez np. uderzenie, popychanie, ciągnięcie za włosy lub ucho, ale także ograniczanie możliwości zaspokajania podstawowych potrzeb fizjologicznych. Za przejaw agresji werbalnej uznaje się np. krzyk, podniesiony ton głosu, ale także ośmieszanie czy poniżające inną osobę żarty. Zachowania agresywne w wymiarze psychicznym i społecznym obejmują m.in. rozsiewanie plotek, pomijanie, wykluczanie, ale także osłabianie pozycji wśród bliskich i ważnych dla ofiary osób[28]. Agresja

---

[25] Por. D.G. Myers, *Psychologia społeczna*, tłum. A. Bezwińska-Walerjan, Zysk i S-ka, Poznań 2003, s. 486.

[26] Por. M. Farnicka, H. Liberska, D. Niewiedział, *Psychologia agresji: wybrane problemy*, Wydawnictwo Naukowe PWN, Warszawa 2016, s. 31.

[27] Za: tamże, s. 142.

[28] Tamże, s. 142–143.

wroga wiąże się najczęściej z pobudzeniem emocjonalnym, w wyniku którego głównym motorem działania są negatywne emocje, w przypadku agresji instrumentalnej podstawowe znaczenie mają natomiast procesy poznawcze, m.in. planowanie i podejmowanie decyzji.

Agresja elektroniczna może także przejawiać się w opisanych wyżej typach zachowań. Agresja fizyczna może zostać zarejestrowana i udostępniona szerokiej publiczności za pomocą urządzeń cyfrowych. Agresja werbalna może być stosowana w formie tekstowej w różnych kanałach komunikacji internetowej, przemoc relacyjna opiera się zaś na wykluczaniu z grup i społeczności internetowych czy ignorowaniu aktywności sieciowej ofiary. Elektroniczna agresja może zatem wyrażać się w przeróżny sposób: od wysłania obraźliwego SMS-a czy e-maila do koleżanki, aż po założenie komuś fałszywego konta na portalu społecznościowym.

Niektórzy autorzy wyróżniają dwie kategorie cyberagresji: **bezpośrednią** i **pośrednią**. Bezpośrednie cybernękanie dotyczy agresywnych działań ograniczonych tylko do sprawcy i ofiary. Susan W. Brenner i Megan Rehberg wskazują, że bezpośrednie cybernękanie zachodzi wtedy, gdy sprawca „kieruje komunikację elektroniczną bezpośrednio do ofiary, wykorzystując w sposób przestępczy wiadomości tekstowe lub multimedialne (SMS, MMS, komunikatory internetowe) lub wiadomości e-mail w celu wywierania bezpośredniego i natychmiastowego wpływu na ofiarę”[29]. Taki sposób postępowania sprawcy nadaje tym działaniom prywatny charakter, ograniczający liczbę możliwych świadków. W pośredniej formie cyberagresji sprawca nie kieruje komunikacji elektronicznej bezpośrednio do swojej ofiary, lecz wykorzystuje do tego celu media społecznościowe (np. Facebook), specjalnie utworzoną stronę internetową, blog lub inne elementy publicznej strefy Internetu[30]. Pośrednie cybernękanie występuje zatem na wielu platformach medialnych i może potencjalnie zaangażować znacznie większą grupę odbiorców.

---

[29] S.W. Brenner, M. Rehberg, *“Kiddie Crime?” The utility of criminal law in controlling cyberbullying*, „First Amendment Law Review” 2010, 8, s. 16.

[30] Por. tamże, s. 17.

Przedstawiona klasyfikacja dokonuje podziału agresji elektronicznej ze względu na charakter publiczności. Możliwość zaobserwowania przez innych użytkowników agresywnych działań sprawcy decyduje więc, czy ofiara doświadcza cyberprzemocy bezpośredniej, czy pośredniej. Pośredni charakter przemocy elektronicznej niejednokrotnie rozmywa odpowiedzialność agresora i potęguje jego przewagę sił, gdy świadkowie swoimi reakcjami zaczynają, świadomie lub nieświadomie, wspierać sprawcę.

Jacek Pyżalski przywołuje natomiast klasyfikację typów agresji elektronicznej ze względu na „tożsamość ofiary", wyróżniając w ten sposób:

- agresję wobec pokrzywdzonych;
- agresję wobec celebrytów;
- agresję wobec grup/idei (uprzedzeniową);
- agresję przypadkową (impulsywną);
- mobbing elektroniczny[31].

W przypadku **agresji wobec pokrzywdzonych** ofiarami są osoby słabsze w wyniku sytuacji życiowej, które nie mogą się bronić, czasami nie są nawet świadome wyrządzanej im krzywdy. Takimi osobami mogą być upośledzeni umysłowo, chorzy psychicznie, bezdomni, alkoholicy itp. Elektroniczne zachowania agresywne wobec tych osób są realizowane najczęściej przez nagrywanie filmów ukazujących ofiary w kompromitujących, ośmieszających je sytuacjach, a następnie umieszczanie tych nagrań w sieci. Czasem takie sytuacje są celowo wywoływane przez sprawcę, który prowokuje lub krzywdzi ofiarę, jednak dokumentowane są jedynie reakcje nagrywanych osób. Zjawisko to określa się pojęciem *happy slapping*[32].

Agresja elektroniczna wobec celebrytów jest kierowana do osób znanych z szeroko rozumianych mediów, m.in. aktorów, piosenkarzy, dziennikarzy, prezenterów telewizyjnych czy sportowców i polityków. Ataki elektroniczne przyjmują najczęściej formę pośrednią i są reali-

---

[31] J. Pyżalski, *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Oficyna Wydawnicza IMPULS, Kraków 2012, s. 157–158.

[32] Por. tamże, s. 158.

zowane z reguły przez obraźliwe komentarze czy rozpowszechnianie plotek i nieprawdziwych informacji na ich temat na tzw. portalach plotkarskich czy profilowych mediach społecznościowych[33].

W przypadku **elektronicznej agresji uprzedzeniowej** agresor atakuje całe grupy ludzi o pewnych poglądach politycznych, określonej narodowości, innego wyznania religijnego, koloru skóry, orientacji seksualnej itp. Agresja jest stosowana zarówno w formie bezpośredniej (np. za pomocą wiadomości wysłanych pocztą elektroniczną) lub pośredniej (przez obraźliwe komentarze na forach internetowych czy przez prowadzenie profilowanych mediów społecznościowych skierowanych przeciwko określonej grupie społecznej reprezentującej cechy znienawidzone przez agresora). Ten rodzaj agresji ujawnia się często w Internecie w postaci tzw. mowy nienawiści (ang. *hate speech*; „każda forma wypowiedzi, która rozpowszechnia, nawołuje, propaguje czy usprawiedliwia nienawiść rasową, ksenofobię, antysemityzm lub inną formę nienawiści opartą na nietolerancji, w tym nietolerancji wyrażanej przez agresywny nacjonalizm i etnocentryzm, dyskryminację i wrogość wobec mniejszości, imigrantów i ludzi o imigranckim pochodzeniu")[34].

Agresja przypadkowa jest kierowana do osób nieznajomych i polega na atakach bez wyraźnego powodu. Do mechanizmów uruchamiających ten rodzaj agresji zalicza się anonimowość w sieci dającą poczucie nierozpoznawalności tożsamości agresora i bezkarności agresywnego działania[35]. Decyzję o podjęciu takiego zachowania sprawca podejmuje często pod wpływem impulsu wywołanego połączeniem cech nastroju sprawcy, cech wizerunku medialnego ofiary czy cech samej konwersacji zapośredniczonej. Tego rodzaju agresja elektroniczna przejawia się w Internecie najczęściej w postaci hejtu („wypowiedzi, które są agresywne, przekraczają granice kultury wypowiedzi, a jednocześnie nie spełniają warunków zakwalifikowania ich do mowy niena-

---

[33] Por. J. Pyżalski, *Agresja elektroniczna wśród…*, s. 47–50.

[34] Rekomendacja nr R (97) 20 Komitetu Ministrów Rady Europy nt. mowy nienawiści (Recommendation No. R (97) 20 of The Committee of Ministers to Member States on „Hate Speech"), https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680505d5b (dostęp: 10.10.2019).

[35] Por. J. Pyżalski, *Agresja elektroniczna i cyberbullying…*, s. 161.

wiści")[36] przez umieszczanie agresywnych, obraźliwych lub ośmieszających komentarzy, wpisów lub prowadzenie płomiennych dyskusji (tzw. *flaming*) przy użyciu wyzwisk, a nie rzeczowych argumentów.

Marzanna Farnicka, Hanna Liberska i Dorota Niewiedział[37], powołując się na przegląd polskich i zagranicznych badań naukowych, wskazują równoległy wzrost zjawiska określanego jako bullying i cyberbullying, doszukując się przyczyn tego stanu rzeczy w podobnych procesach agresji lub możliwości przeniesienia działań agresywnych w zmienione środowisko[38]. W przypadku mobbingu elektronicznego można nawet pokusić się o stwierdzenie, że przestrzeń Internetu jest całkowicie naturalnym środowiskiem młodzieży, realizacja zachowań agresywnych może zatem wynikać zarówno ze swobody działania sprawcy, jak i obecności i dostępności ofiary w środowisku cyfrowym.

Wyniki badań zagranicznych także odnotowują współwystępowanie realizacji zachowań agresywnych w formie tradycyjnej i cyfrowej[39]. Wielu badanych odgrywało jednocześnie role tradycyjnego i cyfrowego sprawcy przemocy (tzw. prześladowcy łączeni). W porównaniu z tradycyjnymi prześladowcami łączeni prześladowcy, nękając innych, kierowali się bardziej motywami instrumentalnymi (tj. moc, przynależność i zabawa), co wskazuje, że ci uczniowie są stosunkowo świadomi swoich działań. Prześladują innych nie tylko po to, by poradzić sobie ze swoim gniewem, ale także po to, by osiągnąć określone cele[40].

Sposoby realizacji cyberprzemocy

Na oficjalnej stronie internetowej rządu Stanów Zjednoczonych poświęconej problemowi cyberbullyingu zjawisko to opisuje się dość szeroko jako „dokuczanie, które ma miejsce na urządzeniach cyfrowych,

---

[36] J. Włodarczyk, *Mowa nienawiści w internecie w doświadczeniu polskiej młodzieży*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2014, 13(2), s. 124.

[37] M. Farnicka, H. Liberska, D. Niewiedział, dz. cyt.

[38] Por. tamże, s. 150.

[39] Za: P. Gradinger, D. Strohmeier, C. Spiel, *Definition and measurement of cyberbullying. Cyberpsychology*, „Journal of Psychosocial Research on Cyberspace" 2010, 4(2), https://cyberpsychology.eu/article/view/4235/3280 (dostęp: 5.10.2019).

[40] Por. tamże.

takich jak telefony komórkowe, komputery i tablety”[41]. Cyberbullying może odbywać się za pośrednictwem smartfonów (SMS, MMS i aplikacje mobilne) lub online (np. w mediach społecznościowych, forach lub grach, w których ludzie mogą przeglądać, współuczestniczyć lub udostępniać treści). Cybernękanie obejmuje wysyłanie, publikowanie lub udostępnianie negatywnych, szkodliwych, fałszywych lub złośliwych treści o kimś innym, co powoduje zawstydzenie lub upokorzenie ofiary. Niektóre wymienione wyżej działania przyjmują charakter przestępczy, niezgodny z obowiązującym prawem[42].

Powyższy opis dość szczegółowo wskazuje narzędzia technologii informacyjno-komunikacyjnych (TIK) oraz możliwy charakter działań, za pomocą których najczęściej dręczy się inne osoby w przestrzeni wirtualnej. Jak już wspomniano, nowoczesne TIK, w tym Web 2.0, dostarczają narzędzi i technik, które w dogodny dla sprawcy sposób umożliwiają realizację zamierzonych, jak i nieumyślnych, form dręczenia. Są one na tyle proste w dostępie oraz intuicyjne w obsłudze, że nawet dzieci stają się ich użytkownikami. Nancy Willard wymienia osiem najczęściej spotykanych sposobów realizacji cyberprzemocy[43]:

- **Płomienna kłótnia** (ang. *flaming*) – termin ten jest używany do opisania kłótni z użyciem obelg i wulgaryzmów między uczestnikami komunikacji internetowej (najczęściej dwójką użytkowników). *Flaming* nie ogranicza się do mediów społecznościowych, takich jak Facebook i Twitter, ale może być również realizowany za pośrednictwem wiadomości tekstowych i e-maili.
- **Zastraszanie** (ang. *harassment*) – polega na wielokrotnym wysyłaniu gróźb lub wulgarnych i obraźliwych wiadomości. Sprawca nieustannie nęka ofiarę, dopóki ta nie ulegnie i będzie bardziej bezbronna. Taki sposób nękania może przybrać formę zarówno

[41] Zob. stopbullying.gov, oficjalna strona internetowa rządu Stanów Zjednoczonych, https://www.stopbullying.gov/cyberbullying/what-is-it/index.html (dostęp: 11.11.2019).

[42] Por. tamże.

[43] Za: C. McCoy, M. Potate, C. McKinney, *Cyberbullying*, w: P. Triggs, *Handbook on bullying: Prevalence, psychological impacts and intervention strategies*, Nova Science Publishers, Inc., New York 2014, s. 46 i stopbullying.gov, oficjalna strona internetowa rządu Stanów Zjednoczonych, https://www.stopbullying.gov/cyberbullying/what-is-it/index.html (dostęp: 11.11.2019).

pośrednią (w mediach społecznościowych), jak i bezpośrednią (przez SMS-y czy e-maile).

- **Oczernianie** (ang. *denigration*, *dissing*) – polega na rozpowszechnianiu o ofierze niepochlebnych plotek i/lub zawstydzających zdjęć, przez wykorzystanie do tego celu mediów społecznościowych. Jest to metoda stosowana przez prześladowców w celu publicznego upokorzenia swojej ofiary, jej deprecjonowania, szkodzenia jej relacjom interpersonalnym lub reputacji. Ofiary często są nieświadome takiego wrogiego działania lub orientują się z opóźnieniem, np. możliwe jest to w sytuacji, gdy sprawca nie oznaczy ofiary na zdjęciu zamieszczonym w mediach społecznościowych, co powoduje, że kompromitujący materiał jest dostępny szerszej publiczności, a jej „bohater" nie zostanie powiadomiony o publikacji.
- **Podszywanie się** lub **maskarada** (ang. *impersonation*/*masquerading*) – polega na tworzeniu fałszywego profilu w mediach społecznościowych lub uzyskaniu do niego dostępu bez świadomości ofiary. W ten sposób sprawca, podszywając się pod ofiarę, tworzy fałszywe wpisy lub zamieszcza kompromitujące zdjęcia, powodując szkody wizerunkowe ofiary oraz komplikacje w relacjach interpersonalych.

  Odmianą tej formy przemocy jest wykorzystanie czyjejś niezabezpieczonej i otwartej strony na Facebooku, aby w imieniu jej właściciela oraz bez jego wiedzy i zgody dokonywać niestosownych, szkodzących i kompromitujących wpisów czy zmian statusu profilu (ang. *fraping*).
- **Ujawnianie tajemnic** (ang. *outing*) – to udostępnianie w Internecie czyichś tajemnic, zawstydzających informacji, prywatnych zdjęć czy osobistych wiadomości zapisanych w prywatnej grupie online (np. ujawniających skrywaną seksualność, intymne szczegóły znajomości i inne wstydliwe sekrety czy dane osobowe) w celu wyrządzenia ofierze krzywdy lub jej zawstydzenia. Cybersprawca, w wyniku oszustwa lub manipulacji ofiary czy wskutek nieuprawnionego dostępu do jej urządzenia (tj. telefon komórkowy, komputer lub ich urządzeń tj. kamera, mikrofon),

wchodzi w posiadanie skrywanych tajemnic ofiary. Wśród rówieśników ten typ przemocy wiąże się często z formą odreagowania odrzuconej miłości czy zazdrości agresora.

Szczególną odmianą tej techniki nękania jest:

- *doxing* – polega na zbieraniu i ujawnianiu w Internecie informacji identyfikujących kogoś (jego prawdziwe imię i nazwisko, adres, miejsce pracy, numer telefonu lub inne informacje identyfikujące daną osobę) w celu atakowania ofiary, z którą nie zgadza się agresor; sprawcy zazwyczaj angażują się w *doxing* ze złośliwym zamiarem upokorzenia, groźby, zastraszenia lub ukarania konkretnej osoby. Publikowanie danych osobowych i wrażliwych naraża pokrzywdzonych na nadużycia czy niebezpieczeństwo utraty zdrowia i życia.

- **Oszustwo** (ang. *trickery*) – polega na nakłonieniu kogoś do ujawnienia zawstydzających informacji lub zdjęć w Internecie. Jest to metoda stosowana przez tradycyjnych prześladowców bez użycia technologii, zwykle przez manipulację lub szantaż.
- **Wykluczenie** (ang. *exclusion*) – polega na celowym i surowym pomijaniu udziału ofiary w wirtualnej grupie lub wydarzeniu, przez zablokowanie jej dostępu do treści, zgody na członkostwo w grupie lub usunięcie z listy członków grupy. Cybersprawcy, wykluczając ofiarę z ekskluzywnej dla ofiary internetowej grupy społecznej, powodują, że osoba ta czuje się niechciana i nieważna.
- **Uporczywe nękanie** (ang. *cyberstalking*)[44] – to intensywne, powtarzające się nękanie ofiary przez groźby i oczernianie jej przy użyciu Internetu i mediów elektronicznych, aby wywołać u niej znaczący strach. Za uporczywe cybernękanie uznaje się m.in. głuche lub obraźliwe telefony, niechciane SMS-y oraz e-maile, pisanie za pomocą komunikatorów, wysyłanie niechcianych wiadomości pocztą elektroniczną, rozsyłanie korespondencji do losowych adresatów w imieniu osoby nękanej oraz wbrew jej woli, jak również komentarze na forach internetowych, wysy-

[44] Więcej na temat cyberstalkingu można przeczytać w następnym rozdziale tej książki.

łanie prezentów przez Internet itp. Cyberstalker wykorzystuje zatem różne formy nękania, które zostały opisane wyżej.

Przyczyny i motywy cyberprzemocy

W literaturze naukowej funkcjonuje wiele stanowisk próbujących wyjaśnić mechanizm powstawania agresji. Badacze zwracają uwagę na szerokie spektrum czynników biologicznych, społecznych oraz psychologicznych. Wyjaśnienie przyczyn agresji jest jednak niezwykle trudne, ponieważ jej uwarunkowania są bardzo złożone, powiązane ze sobą i zależne od kontekstu. W literaturze problemu najczęściej wymienia się uwarunkowania biologiczne, społeczne i sytuacyjne, a jako najlepiej udokumentowane empirycznie wskazuje się uwarunkowania neurofizjologiczne, psychologiczne, sytuacyjne oraz społeczno-kulturowe[45].

Na doświadczanie agresji elektronicznej szczególnie narażona jest dorastająca młodzież. To pokolenie online będące najliczniejszą grupą użytkowników Internetu. Źródła mobbingu elektronicznego można upatrywać w negatywnej konfiguracji czynników warunkujących rozwój młodzieży, ich gotowości do zachowań agresywnych i poziomu kompetencji w obszarze komunikacji elektronicznej.

Okres pomiędzy dzieciństwem a dorosłością (od. ok. 11. roku życia do ok. 21. roku życia) charakteryzuje się pewną niestabilnością zachowań wynikającą z wielu zmian rozwojowych zachodzących w obrębie ciała, intelektu i emocji. „W literaturze z zakresu psychologii rozwojowej okres dorastania bywa określany jako czas intensywnych przeobrażeń we wszystkich sferach rozwoju (fizycznej, seksualnej, poznawczej, emocjonalnej i społecznej) przygotowujących jednostkę do wejścia w dorosłość i podjęcia zadań i wyzwań charakterystycznych dla młodych dorosłych”[46].

---

[45] Więcej informacji na temat etiologii agresji znajduje się w pierwszym tomie książki: B. Siemieniecki, W. Kwiatkowska, L. Wiśniewska-Nogaj, *Agresja – zjawisko, skutki, zapobieganie. Perspektywa pedagogiki kognitywistycznej, psychoprofilaktyki oraz edukacji moralnej*, Wydawnictwo Naukowe UMK, Toruń 2020.

[46] I. Obuchowska, *Drogi dorastania. Psychologia rozwojowa okresu dorastania dla rodziców i wychowawców*, WSiP, Warszawa 1996; H. Liberska, *Perspektywy temporalne*

Młode osoby odczuwają rosnącą siłę, sprawność fizyczną i zdolności intelektualne, jednak nie zawsze sobie z nimi radzą. Nie każdy dorastający akceptuje zachodzące zmiany w obrębie swojego ciała, nie panuje nad nimi. Problemy może potęgować zwiększona aktywność hormonów, przekładająca się także na labilność emocjonalną i zmiany zachowania. Wyzwania rozwojowe stawiane w tym okresie są przyczyną wielu rozterek i trudności młodzieży.

Znaczący rozwój technologii w dziedzinie komunikacji i rozrywki w ciągu ostatnich kilkunastu lat wpływa na sposób socjalizacji młodzieży, wikłając jej interakcje w przestrzeń pełną dowolności, różnorodności, swobody i upozorowania. Dla adolescentów grupą odniesienia są rówieśnicy, którzy zaczynają wyznaczać nową perspektywę poznawczą i aksjologiczną jednostki (czasami odmienną wobec wzorów wyniesionych ze środowiska rodzinnego). Grupa rówieśnicza jest źródłem standardów, względem których jednostka może oceniać siebie i innych, w jej obrębie zaspokajanych jest wiele podstawowych potrzeb młodzieży, tj. bezpieczeństwa, przynależności, uznania, samorealizacji. To w grupie rówieśniczej nastolatki doskonalą własne kompetencje komunikacyjne i społeczne, poznają swoje mocne i słabe strony, potwierdzają własną wartość i kształtują tożsamość. Nie zawsze jednak funkcjonowanie w grupie, zwłaszcza wirtualnej, dostarcza nastolatkowi samych pozytywnych doświadczeń, ponieważ, jak twierdzi Florian Znaniecki: „Każdy członek takiej grupy wnosi do niej ze sobą wpływy, którym podlega w rodzinie, w otoczeniu sąsiedzkim starszych, w zetknięciu z instytucjami wychowawczymi przygotowującymi go do członkostwa w grupach dorosłych; chociaż wpływy te częściowo się równoważą i neutralizują, jednak niektóre z nich, dodając się lub przeważając, mogą uwarunkować w znacznej mierze treść społeczną grupy młodocianych rówieśników”[47]. Przestrzeń internetowa, ze względu na swoje cechy, sprzyja nakładaniu się tych wpływów i eksperymentowaniu z płynnym systemem wartości.

---

młodzieży. Wybrane uwarunkowania, Wydawnictwo Naukowe UAM, Poznań 2004, za: M. Farnicka, H. Liberska, D. Niewiedział, dz. cyt., s. 100.

[47] F. Znaniecki, *Socjologia wychowania*, Wydawnictwo Naukowe PWN, Warszawa 2001, s. 85.

Dorastanie cechuje wysoka dynamika i złożoność procesów rzutujących na jego zachowanie, w tym zachowanie agresywne. Jak wspomniano, czynniki wpływające na stosowanie agresji są różnorodne, złożone i uwarunkowane kontekstem funkcjonowania jednostki. Maria Libiszowska-Żółtkowska wyróżnia czynniki sprzyjające agresji mające swoje uwarunkowania genetyczne i środowiskowe. Ich zestawienie jest widoczne w tabeli 2.

Tabela 2. Czynniki powstawania agresji

Czynniki sprzyjające powstawaniu agresji – „czynniki ryzyka"
obniżony poziom sprawności intelektualnej
niska pozycja w grupie, niskie poczucie własnej wartości
deficyty umiejętności interpersonalnych
brak wsparcia społecznego, izolacja
tzw. trudne zachowania, np. ADHD, zakłócone relacje społeczne
wcześniejsze doświadczenia bycia ofiarą przemocy – bez pomocy specjalistycznej
przynależność do grupy mniejszościowej, np. mniejszość etniczna
akceptacja kar fizycznych i przemocy w danej kulturze
zła sytuacja ekonomiczna rodziny
„odmienność" negatywnie waloryzowana w środowisku (np. niepełnosprawność fizyczna)

Źródło: M. Farnicka, H. Liberska, D. Niewiedział, *Psychologia agresji: wybrane problemy*, Wydawnictwo Naukowe PWN, Warszawa 2016, s. 31.

Można zatem przypuszczać, że wymienione czynniki z jednej strony zwiększają prawdopodobieństwo doświadczenia agresji w charakterze ofiary, z drugiej strony mogą przyczynić się do realizacji zachowań agresywnych i zwiększają prawdopodobieństwo przyjęcia roli sprawcy agresji.

Opisane powyżej uwarunkowania powstawania agresji, także w środowisku cyfrowym, można uznać za czynniki sprzyjające realizacji cyberprzemocy. Wiele doniesień badawczych[48] wskazuje zaangażo-

[48] Zob. m.in. T. Beran, Q. Li, *The relationship between cyberbullying and school bullying*, „Journal of Student Wellbeing" 2007, 1(2), s. 15–33; Q. Li, *New bottle but old wine: A research of cyberbullying in schools*, „Computers in Human Behaviour" 2005, 23, s. 1777–1791; taż, *Cyberbullying in schools: A research of gender differences*,

wanie w przemoc tradycyjną jako predyktor przyjęcia roli sprawcy lub ofiary cyberprzemocy. Tanya Beran i Qing Li[49], przywołując teorie **dominacji i rang społecznych**, opisują związek między nękaniem w szkole a nękaniem w Internecie. Zdaniem tych autorek zachowania ludzkie koncentrują się wokół pragnienia uznania własnej atrakcyjności w umysłach innych lub strachu przed jej utratą[50], a w wyniku procesów stratyfikacji grupowej ustanawiana jest hierarchia, w której niektórzy jej członkowie wykorzystują agresję, aby zdominować innych i uzyskać dostęp do pewnych zasobów społecznych (tj. prestiż, władza, szacunek, podziw i akceptacja przez innych cenionych członków grupy). Kiedy rówieśnicy poddają się tej dominacji (okazując płacz i strach), agresor osiąga założony cel i zaczyna sprawować władzę oraz kontrolę nad ofiarą, jednocześnie budując czy wzmacniając swoją pozycję w grupie. Dla zdobywania lub utrzymania dominacji agresor może nękać rówieśnika także w cyberprzestrzeni, przedłużając niejako swój zasięg i moc działania. Dostęp agresora do cyfrowej formy wizerunku i strach ofiary przed możliwością jego utraty (rodzącej przekonanie o braku akceptacji czy postrzeganiu negatywnych cech i braku wartości) zwiększa bowiem przewagę sił sprawcy oraz skutki cyberprzemocy.

Możliwe jest również, że dzieci zastraszane w szkole będą próbować odwetu za pomocą technologii, ponieważ ta forma może wywoływać mniejszy poziom lęku niż bezpośrednie ataki. Poszkodowane

---

„School Psychology International" 2006, 27(2), s. 157–170; taż, *Bullying in the new playground*, „Australasian Journal of Educational Technology" 2007, 23(4), s. 435––455; H. Vandebosch i in., *Cyberpesten bij jongerenin Vlaanderen: een studie in opdracht van het viWTA*, viWTA, Brussel 2006; J. Wolak, J.M. Mitchell, D. Finkelhor, *Does online harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts*, „Journal of Adolescent Health" 2007, 41(6), s. 51–58; M.L. Ybarra, K.J. Mitchell, *Online aggressor/targets, aggressor and targets: A comparison of youth characteristics*, „Journal of Child Psychology and Psychiatry" 2004, 45(7), s. 1308–1316, za: M. Walrave, W. Heirman, *Skutki „cyberbullyingu" – oskarżenie czy obrona technologii?*, tłum. A. Nowak, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2009, 8(1), s. 3.

[49] T. Beran, Q. Li, dz. cyt., s. 15.

[50] P. Gilbert, *The relationship of shame, social anxiety and depression: The role of the evaluation of social rank*, „Clinical Psychology and Psychotherapy" 2000, 7(3), s. 175.

dzieci mogą zatem uciekać się do tego zachowania jako środka samoobrony. W rzeczywistości ofiary mogą angażować się w zastraszanie, szczególnie jeśli są one poważnie dotknięte tym zjawiskiem, doświadczając cyberagresji w podwójnej roli[51].

Mimo że cyberprzemoc różni się od tradycyjnego zastraszania sposobem realizacji, to motywy są podobne. Na ogół powodem obu typów agresji jest zadanie cierpienia innej osobie z powodu zazdrości lub niechęci[52].

Szukając przyczyn i motywów cyberprzemocy, przywołuje się także społeczną teorię poznawczą i efekt odhamowania w sieci. Zgodnie ze **społeczną teorią poznawczą** postrzeganie zaobserwowanych zachowań agresywnych jako pozytywnych sprawia, że działania te są mniej hamowane u obserwatora, szczególnie jeśli agresor jest nagradzany za agresywne działania. Według Christophera P. Barletta i Douglasa A. Gentile'a[53] świadkowie udanych przypadków cyberprzemocy wnioskują, że cyberprzemoc jest odpowiednim i skutecznym zachowaniem. W społecznym uczeniu się cyberagresji pomagają także unikatowe cechy kontekstu sieciowego. Oznacza to, że zarówno cyberświadkowie, jak i cybersprawcy dowiadują się, że dzięki anonimowości sprawca agresji doznaje niewielkich lub żadnych bezpośrednich konsekwencji za swoje zachowanie, co ośmiela do dalszego stosowania i rozwijania działań agresywnych w sieci oraz przyczynia się do pozytywnego nastawienia młodzieży do takich zachowań i ewentualnego angażowania się w cyberprzemoc w przyszłości[54]. Ponadto skuteczność działań agresywnych zwiększa przekonanie sprawcy i obserwatorów cyberagresji o ich użyteczności.

Efekt odhamowania sugeruje z kolei, że ludzie, dzięki właściwościom cyberprzestrzeni, nie zachowują się w niej podobnie jak w praw-

---

[51] T. Beran, Q. Li, dz. cyt., s. 18.

[52] C. McCoy, M. Potate, C. McKinney, dz. cyt., s. 43.

[53] Ch.P. Barlett, D.A. Gentile, *Attacking others online: The formation of cyberbullying in late adolescence*, „Psychology of Popular Media Culture" 2012, 1(2), s. 123–135.

[54] M.F. Wright, Y. Li, *Normative beliefs about aggression and cyber aggression among young adults: A longitudinal investigation*, „Aggressive Behavior" 2013, 39(3), s. 161–170.

dziwym życiu. Adam Joinson[55] wskazuje, że głównym składnikiem efektu odhamowania w sieci jest dezindywidualizacja. Do dezindywidualizacji dochodzi wtedy, gdy ludzie nie ponoszą odpowiedzialności za swoje działania, zaś anonimowość może dodatkowo zmniejszyć ich odpowiedzialność, co może prowadzić do postępowania nieco innego niż w warunkach normalnych. Poczucie anonimowości pozwala ludziom na minimalizację obaw o ocenę ich działań autoprezentacyjnych i osąd innych, w wyniku czego przejawiają takie zachowania, które w rzeczywistości realnej muszą ograniczać lub hamować. Istnieje wiele badań wykazujących, że ludzie zachowują się bardziej dosadnie podczas komunikacji za pośrednictwem różnych technologii elektronicznych. We wczesnych badaniach Katelyn McKenna i John Bargh[56] stwierdzili, że w komunikacji za pośrednictwem komputera było więcej nieporozumień, większa wrogość i agresywna aktywność w porównaniu z komunikacją twarzą w twarz.

Środowisko internetowe eliminuje także możliwość dostrzegania reakcji emocjonalnych, co może uniemożliwić ludziom modulowanie własnego zachowania, ponieważ nie są oni w stanie doświadczyć konsekwencji swoich działań (tzw. **efekt kabiny pilota**). Jeśli chodzi o cyberprzemoc, jej sprawca z racji cech środowiska sieciowego nie może być świadkiem reakcji ofiary lub doznać dezaprobaty społecznej i kary. Z biegiem czasu zachowania cyberagresora mogą stać się bardziej odhamowane, szczególnie gdy otrzymuje pozytywne wzmocnienia, nie rozpoznaje konsekwencji swoich zachowań i traci kontrolę nad typowymi zahamowaniami występującymi w kontaktach twarzą w twarz[57].

---

[55] A. Joinson, *Disinhibition and the Internet*, w: J. Gackenbach (ed.), *Psychology and the Internet: Intrapersonal, interpersonal, and transpersonal implications*, Academic Press, Amsterdam 2007, s. 84–85.

[56] K.Y.A. McKenna, J.A. Bargh, *Plan 9 from cyberspace: The implications of the Internet for personality and social psychology*, „Personality and Social Psychology Review" 2000, 4(1), s. 57–75.

[57] Por. W. Heirman, M. Walrave, *Assessing concerns and issues about the mediation of technology in cyberbullying*, „Cyberpsychology: Journal of Psychosocial Research on Cyberspace" 2008, 2(2), https://cyberpsychology.eu/article/view/4214/3256 (dostęp: 5.10.2019).

Według Michelle F. Wright anonimowość w kontekście sieciowym, wraz z efektem internetowego odhamowania, pozwala młodym oddzielić swoje działania od realnego świata i ich tożsamości, ułatwiając im cyberkrzywdzenie innych[58].

Wielu autorów zagranicznych jako najczęstsze motywy cybernękania wskazuje zazdrość, uprzedzenia i nietolerancję dla niepełnosprawności, religii, płci, wstyd, dumę oraz poczucie winy i gniewu[59]. Według badania „Nastolatki 3.0" polskie nastolatki najczęściej doświadczają agresji w sieci ze względu na:

- poglądy (14,9%);
- wygląd (13,5%);
- upodobania (11,6%);
- narodowość (8,1%);
- ubiór (8,0%);
- inne motywy, tj. orientacja seksualna (4,6%), religia (4,5%), kolor skóry (4,3%), płeć (4,2%), zła sytuacja finansowa (3,8%)[60].

Charles E. Notar, Sharon Padgett, Jessica Roden[61] wymieniają dodatkowe przyczyny cybernękania, m.in. aprobatę anonimowości, nudę i chęć poprawy nastroju, podżeganie, zazdrość, brak dostrzeganych konsekwencji agresywnego zachowania, projekcję uczuć, zemstę. Te szczególne powody zdaniem autorów mogą tłumaczyć stosowanie cyberagresji przez osoby, które nie skonfrontowałyby swojej ofiary twarzą w twarz.

Znęcanie się może prowadzić do obrażeń fizycznych, stresu społecznego i emocjonalnego, samookaleczenia, a nawet śmierci. Zwiększa także ryzyko depresji, lęku, trudności ze snem, niższych osiągnięć szkolnych i opuszczania szkoły. Młodzież, która nęka innych, jest narażona na zwiększone ryzyko zażywania substancji psychoaktywnych, problemów szkolnych i przemocy w późniejszym okresie dojrzewa-

---

[58] M.F. Wright, *Predictors of anonymous cyber aggression: The role of adolescents' beliefs about anonymity, aggression, and the permanency of digital content*, „Cyberpsychology, Behavior and Social Networking" 2014, 17(7), s. 432.

[59] Ch.E. Notar, S. Padgett, J. Roden, *Cyberbullying: A Review of the literature*, „Universal Journal of Educational Research" 2013, 1(1), s. 3.

[60] M. Bochenek, R. Lange (red.), dz. cyt., s. 64.

[61] Ch.E. Notar, S. Padgett, J. Roden, dz. cyt.

nia i dorosłości. Nastolatki, które nękają innych i są nękane, ponoszą najpoważniejsze konsekwencje i są bardziej narażone na problemy ze zdrowiem psychicznym i problemy behawioralne[62]. Podobne skutki niesie ze sobą nękanie przy użyciu technologii.

Efekty cyberprzemocy wśród młodych mogą różnić się w zależności od tego, czy są oni prześladowcami, ofiarami czy świadkami. Wśród cyfrowo zastraszanych nastolatków odnotowano m.in. depresję, lęk, różne objawy somatyczne i zachowania samobójcze, podczas gdy cyberagresorzy mieli skłonność do agresji, przestępczych zachowań i używania narkotyków[63]. Skutki cyberprzemocy mogą być również zróżnicowane w zależności od płci. W próbie 31 148 azjatyckich uczniów w różnym wieku cyberprzemoc stała się źródłem problemów emocjonalnych u dziewcząt i problemów behawioralnych u chłopców[64].

Obserwowanie cyberprzemocy również nie pozostaje obojętne dla świadków elektronicznych zachowań agresywnych. Analizy korelacyjne badań przeprowadzonych przez Robin M. Kowalski i Susan P. Limber[65] wskazały, że takie objawy, jak depresja, lęk, samoocena, zgłaszane problemy zdrowotne, nieobecności w szkole, również z powodu choroby, oraz słabsze stopnie, były istotnie związane z zaangażowaniem uczniów w cybernękanie zarówno w roli sprawcy, jak i ofiary.

Doświadczanie cyberprzemocy w charakterze ofiary

Znajomość zmiennych, które mogą znacząco wpłynąć na prawdopodobieństwo, że nastolatek stanie się ofiarą cyberagresji, może pomóc

---

[62] Za: Centers for Disease Control and Prevention, *What are the consequences?*, https://www.cdc.gov/violenceprevention/youthviolence/bullyingresearch/fastfact.html (dostęp: 5.10.2019).

[63] Ch.L. Nixon, *Current perspectives: The impact of cyberbullying on adolescent health*, „Adolescent Health, Medicine and Therapeutics" 2014, 5, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4126576/ (dostęp: 28.11.2019).

[64] S. Kim i in., *Cyberbullying victimization and adolescent mental health: Evidence of differential effects by sex and mental health problem type*, „Journal of Youth and Adolescence" 2018, 47(3), s. 663.

[65] R.M. Kowalski, S.P. Limber, *Psychological, physical and academic correlates of cyberbullying and traditional bullying*, „Journal of Adolescent Health" 2013, 53(1), s. S18.

w zapobieganiu, wykrywaniu i terapii skutków cyberwiktymizacji. David Álvarez-García i inni[66] poddali analizie statystycznej związek wybranych czynników socjodemograficznych, psychologicznych, edukacyjnych i technologicznych z ryzykiem doświadczania cyberprzemocy jako ofiara przez hiszpańską młodzież. Jej wyniki pokazały, że **wiek, bycie ofiarą przemocy offline, ryzykowne zachowania w Internecie, korzystanie z sieci społecznościowych lub aplikacji do komunikacji błyskawicznej oraz częstotliwość korzystania z Internetu w weekendy** (pow. trzech godzin na aktywności niezwiązane z zadaniami szkolnymi) są statystycznie istotnymi czynnikami ryzyka doświadczania cyberprzemocy w charakterze ofiary. Podobna zależność zachodziła między **posiadaniem własnego telefonu komórkowego, graniem online z innymi osobami oraz częstotliwością korzystania z Internetu w dni powszednie** (niezwiązanej z aktywnościami dotyczącymi zadań szkolnych). Czas **spędzony online, korzystanie z Internetu w celach społecznych i angażowanie się w ryzykowne zachowania online, w tym gry online,** są zatem znaczącymi czynnikami ryzyka wiktymizacji cyberprzemocy wśród nastolatków. **Poczucie własnej wartości** stanowiło natomiast czynnik ochronny przeciw cyberwiktymizacji okazjonalnej.

Inne międzynarodowe badania ukierunkowane na poszukiwanie związków między samooceną a cyberwiktymizacją często wskazują, że ofiary cyfrowego zastraszania zgłaszają **niską samoocenę**[67]. Ta cecha ofiar cyberprzemocy może być nie tylko predyktorem cyberagresji, ale także jej skutkiem. Osoby o niskiej samoocenie mogą być bowiem postrzegane przez sprawców jako „łatwy cel", a cykliczność cyberprzemocy i wiktymizacji może wpływać na kształtowanie się niskiej samooceny nękanej osoby.

Wśród czynników ryzyka łączących się z cechami i zachowaniem dziecka najczęściej wymienia się m.in.:

---

[66] D. Álvarez-García i in., *Risk factors associated with cybervictimization in adolescence*, „International Journal of Clinical and Health Psychology" 2015, 15(3), s. 231–233.

[67] Np. R.M. Kowalski, S.P. Limber, dz. cyt., s. S13–S20.

- wrażliwość;
- nieśmiałość, niepewność i ostrożność w kontaktach z innymi;
- słabe relacje z rówieśnikami, nieumiejętność nawiązywania przyjaźni;
- lęk;
- bierność, uległość, a szczególnie – brak umiejętności bronienia się w sytuacjach przemocy;
- płaczliwość;
- niską samoocenę;
- negatywne nastawienie do stosowania przemocy;
- słabość lub niską sprawność fizyczną (jeśli chodzi o chłopców)[68].

Liczne badania wykazały zależność między doświadczaniem przemocy jako ofiara w formie tradycyjnej a doświadczaniem przemocy jako ofiara z udziałem mediów. Bycie celem tradycyjnego nękania stanowiło silny czynnik ryzyka wiktymizacji cyberprzemocy[69]. Ofiara cyberprzemocy często wyróżnia się na tle rówieśników, czy to ze względu na wygląd, ubiór, kolor skóry, czy też poglądy, pochodzenie lub orientację seksualną. Ofiary cyberprzemocy można podzielić na dwie zasadnicze grupy:

- ofiary pasywne – cechujące się biernością, lękiem, znacznie obniżonym poczuciem własnej wartości, wycofane, mniej sprawne fizycznie;
- ofiary prowokujące – bardzo aktywne (czasem nadaktywne), mające problemy z koncentracją, które przejawiają agresję; ich zachowania mogą być odbierane jako irytujące i prowokujące, mogą wywoływać negatywne reakcje ze strony innych[70].

Polskie badania wskazują, że na dręczenie szkolne szczególnie narażeni są ci uczniowie, którzy czują się **osamotnieni**, mają niewielu przyjaciół, są przekonani, że rzadko mogą liczyć na pomoc innych, ale

---

[68] J. Węgrzynowska, *Dzieci doświadczające przemocy rówieśniczej*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2016, 15(1), s. 11.

[69] Taki związek odnotowano w 15 międzynarodowych raportach badawczych. Podano za: R.M. Kowalski, S.P. Limber, A. McCord, dz. cyt., s. 21.

[70] Por. D. Olweus, *Mobbing – fala przemocy w szkole. Jak ją powstrzymać?*, tłum. D. Jastrun, Jacek Santorski & Co Agencja Wydawnicza, Warszawa 2007, s. 46–48.

i ci, którym **brakuje wsparcia rodziców**. Zauważono także korelację między **sytuacją materialną ucznia** a doświadczaniem przemocy rówieśniczej. Uczniowie deklarujący, że sytuacja finansowa ich rodziny jest gorsza od przeciętnej w klasie, wyraźnie częściej doświadczają różnych form agresji.

Najbardziej typowymi reakcjami ofiar cyberprzemocy, będącymi skutkami tych działań, są: **uczucie smutku, depresja, samotność, myśli samobójcze, niższy poziom samooceny, słabe wyniki w nauce i niechęć do uczęszczania do szkoły.** Stwierdza się także **wyższy poziom lęku społecznego, większe problemy z zachowaniem, a także przypadki spożywania alkoholu i narkotyków**[71].

Autorzy raportów badawczych wskazują pewne uwarunkowania ograniczające ewentualność doświadczenia cyberprzemocy w charakterze ofiary. Wśród czynników chroniących, oprócz wspomnianego wcześniej poczucia własnej wartości, wymienia się **wsparcie rówieśnicze** oraz **właściwe funkcjonowanie rodziny**. Wsparcie ze strony rówieśników, jak się wydaje, łagodzi związek między wiktymizacją w Internecie a subiektywnymi dolegliwościami zdrowotnymi oraz subiektywnie zmniejsza przewagę sprawcy. Rodzicielskie zachowania, które chronią młodzież przed cybernękaniem, obejmują natomiast ciepło rodzicielskie oraz wsparcie rodzinne. Pozytywne relacje z rodzicem mogą również złagodzić negatywne skutki cybernękania w postaci dolegliwości zdrowotnych i złej samooceny. Zauważono, że nękane nastolatki, które zgłaszały częstszą komunikację z rodzicami, miały wyższy poziom samooceny niż nastoletnie cyberofiary, które wskazywały rzadszą komunikację z rodzicami. W niektórych badaniach **zasady rodzicielskie i monitorowanie przez nich aktywności** nastolatków zaliczano również do czynników chroniących przed cyberwiktymizacją, jednak pomocne były tylko te **strategie rodzicielskie, które były oparte na życzliwym zainteresowaniu, współpracy i wzajemnych dobrych relacjach**[72].

---

[71] Za: R.M. Kowalski, S.P. Limber, dz. cyt., s. S14, S18 oraz R.M. Kowalski, S.P. Limber, A. McCord, dz. cyt., s. 21.

[72] Takie wnioski prezentowano w 12 międzynarodowych raportach badawczych. Podano za: R.M. Kowalski, S.P. Limber, A. McCord, dz. cyt., s. 26.

Nieliczne doniesienia badawcze wykazały także pewne uwarunkowania szkolne, które mogą ograniczać zjawisko mobbingu elektronicznego. Zauważono, że **postrzeganie bezpieczeństwa w szkole, zadowolenie ze szkoły** oraz **istnienie pozytywnego klimatu szkolnego** zmniejszają prawdopodobieństwo cybernękania rówieśniczego, podczas gdy poczucie zagrożenia jest związane ze zwiększonym ryzykiem takich zachowań[73].

Wymienione wyżej czynniki opisują wieloaspektowe uwarunkowania, których indywidualne połączenie może zwiększać lub minimalizować ryzyko cyberwiktymizacji. Ich znajomość pozwoli na wzrost czujności oraz planowanie odpowiednich działań w zakresie prewencji cyberprzemocy i pomocy jej ofiarom. Konsekwencje tego rodzaju przemocy mogą być jeszcze bardziej dotkliwe ze względu na publiczny charakter komunikacji sieciowej, jej trwałość i zasięg, a także anonimowość niejednokrotnie utrudniającą identyfikację sprawcy.

Doświadczanie cyberprzemocy w charakterze sprawcy

Jacek Pyżalski na podstawie analizy 13 dużych projektów badawczych odnotował skalę rozpowszechniania sprawstwa cyberbullyingu w przedziale od 7% do 35% populacji adolescentów (średnio 15%), przy czym najwyższy odsetek cybersprawców występował w grupie wiekowej 13–15 lat[74]. Takie wskazania wieku nie zaskakują z uwagi na dużą aktywność online nastolatków oraz kumulację problemów wynikających z realizowania przez nich zadań rozwojowych związanych z formowaniem własnej tożsamości.

Można przywołać za Anną Borkowską[75] możliwe motywy angażowania się dzieci i młodzieży w agresywne działania w sieci, wymieniając ewentualne przyczyny:

- problem z przestrzeganiem reguł społecznych i respektowaniem granic – np. dziecko pochodzi ze środowiska wychowawczego, w którym dochodzi do przemocy, przymusu lub ignorowania i jednocześnie przyzwala się na antyspołeczne zachowania;

---

[73] Tamże.

[74] J. Pyżalski, *Agresja elektroniczna i cyberbullying…*, s. 145.

[75] Por. A. Borkowska, dz. cyt., s. 27.

- nieprawidłowe zaspokajanie potrzeb rozwojowych, tj. odczuwanie atrakcyjności, akceptacji i przynależności, miłości – dziecko może chcieć zwrócić na siebie uwagę czy też próbować zdobyć akceptację rówieśników; może to być podyktowane także błędną koncepcją kreowania swojego wizerunku bądź ustalania pozycji w grupie, innym powodem bywa zazdrość lub też zerwanie relacji uczuciowej;
- obawa przed przyjęciem roli ofiary wpływająca na decyzję o przyłączeniu się do dręczycieli;
- zemsta na prześladowcach w wyniku doświadczenia przemocy w charakterze ofiary;
- impuls lub silne emocje leżące u podstaw decyzji o publikacji krzywdzącego materiału o kolegach;
- nieumyślność – sprawca nie zdaje sobie sprawy z tego, że stosuje zachowania przemocowe (podejmuje pewne działania z powodu nudy, dla żartu czy z braku empatii, pogłębionego występowaniem wspomnianych efektów: kabiny pilota czy odhamowania).

Powyższe motywy dużo łatwiej jest realizować w środowisku online z powodu przekonania młodych osób o braku kontroli i odpowiedzialności wywołanego poczuciem anonimowości w sieci.

Znaczącymi indywidualnymi predyktorami cyberprzemocy są **empatia** i **samoocena**. Nastolatki o niskim poziomie empatii i poczucia własnej wartości najprawdopodobniej częściej będą angażować się w cyberprzemoc[76]. Empatia obejmuje zarówno komponenty poznawcze (np. rozumienie emocji innych), jak i afektywne (np. doświadczanie emocji innych), które odpowiadają „zimnym" i „gorącym" aspektom empatii omawianym przez innych badaczy. Zarówno empatia poznawcza, jak i afektywna mogą wpływać na interakcje społeczne. Zauważono, że niższa empatia poznawcza jest silniejszym katalizatorem cyberprzemocy niż empatia afektywna[77], chociaż niska empatia afektywna jest nadal znaczącym czynnikiem ryzyka rozwoju zachowań nękających[78].

---

[76] G. Brewer, J. Kerslake, *Cyberbullying, self-esteem, empathy and loneliness*, „Computers in Human Behavior" 2015, 48, s. 258.

[77] Tamże.

[78] R.M. Kowalski, S.P. Limber, A. McCord, dz. cyt., s. 27.

W badaniach poświęconych problemowi sprawstwa cyberprzemocy jako czynniki ryzyka zidentyfikowano **niski poziom samokontroli** oraz **wysoki poziom impulsywności i zachowań poszukujących doznań** u sprawców cybernękania. Osoby te wykazują również znacznie częściej **normatywne przekonania**[79] na temat agresji niż cyberofiary lub osoby niezaangażowane. Wielu badaczy badało **występowanie zachowań przestępczych** (określanych jako zachowania nieprzystosowawcze, nielegalne lub niewłaściwe ze względu na wiek, tj. nadużywanie alkoholu, palenie tytoniu, nadużywanie narkotyków i niewłaściwe zachowanie w szkole) u sprawców cyberprzemocy, odnotowując je jako znaczący czynnik ryzyka cyberprzemocy. Cybersprawcy w wieku dojrzewania mieli znacznie wyższy odsetek problemów związanych z zachowaniem (20,5%) w porównaniu z cyberofiarami (4,7%). Wśród innych czynników sprzyjających doświadczaniu cyberprzemocy w charakterze sprawcy, których wpływ odnotowano w międzynarodowych raportach badawczych, wymienia się m.in. **odrzucenie rówieśników, izolację społeczną, potrzebę dominacji społecznej, normatywność cyberprzemocy, poczucie zaangażowania rówieśników w zachowania agresywne sprawcy**[80].

Zauważono, że dodatkowym predykatorem sprawstwa cyberprzemocy jest **wiek i czas spędzany online, zwłaszcza na działaniach społecznych.** Zarówno korzystanie z technologii, jak i cyberprzemoc **rosły wraz z wiekiem, aż do okresu dorastania**, a następnie malały w dalszym okresie życia. Ponadto rodzaj technologii wykorzystywanych do cyberprzemocy był różny w zależności od wieku sprawców. Podczas gdy większość przypadków cybernękania wśród młodzieży w wieku szkolnym występuje za pośrednictwem gier online, uczniowie szkół średnich dopuszczają się cybernękania zwłaszcza w mediach społecznościowych[81].

W amerykańskiej literaturze wyróżnia się za Parry Aftab cztery typy (i jeden podtyp) cybersprawców (rysunek 4). Każdy z nich charakteryzuje się inną motywacją i rodzajem działania. Tylko dwa z nich funkcjonują zarówno online, jak i offline („głodny władzy" i jego podtyp: „zemsta nerdów"). Pozostałe typy prześladowców mogą działać

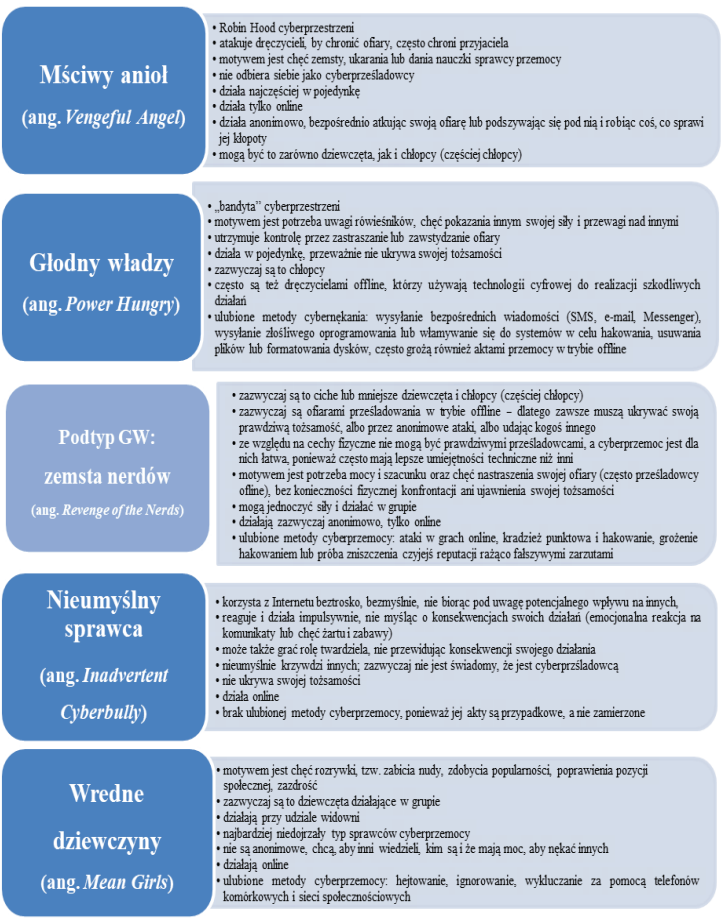
---

[79] Przekonania normatywne istotnie regulują podejmowane przez jednostkę działania przez ocenę społecznego przyzwolenia lub zakazania danego zachowania.

[80] R.M. Kowalski, S.P. Limber, A. McCord, dz. cyt., s. 28.

[81] Tamże, s. 27.

tylko w środowisku online, którego cechy (w głównej mierze anonimowość) pozwalają im osiągać założone cele oraz być kimkolwiek chcą (lub ukryć swoją tożsamość)[82].



Rysunek 4. Typologia sprawców cyberagresji według Parry Aftab (opracowanie własne na podstawie: B.B. Sutton, *Cyberbullying: An interview with Parry Aftab*, „A Journal for Educational Technology & & Change" 2011, https://etcjournal.com/2011/02/17/7299/ (dostęp: 2019.11.28) i www.stopcyberbullying.org.)

[82] B.B. Sutton, *Cyberbullying: An interview with Parry Aftab*, „A Journal for Educational Technology & Change" 2011, https://etcjournal.com/2011/02/17/7299/ (dostęp: 2019.11.28); *What methods work with the different kinds of cyberbullies?*, http://www.stopcyberbullying.org/pdf/howdoyouhandleacyberbully.pdf (dostęp: 2019.11.28).

Sprawcy cyberprzemocy także ponoszą jej długofalowe konsekwencje: utrwalają się u nich zachowania agresywne, obniża się poczucie odpowiedzialności za własne działania, może nasilać się skłonność do zachowań aspołecznych w przyszłości[83].

Do czynników ochronnych, które zmniejszają prawdopodobieństwo sprawstwa cyberprzemocy, zaliczono z kolei **pozytywne wsparcie emocjonalne ze strony rodziny**, zdefiniowane jako zaufanie, komunikacja, poczucie bezpieczeństwa i przywiązania oraz brak wyobcowania między rodzicami a dziećmi. Podobnie **klimat szkolny i postrzeganie bezpieczeństwa w szkole** może oddziaływać na zjawisko cyberprzemocy rówieśniczej. Niskie wsparcie nauczycieli i brak jasnych zasad dotyczących cyberprzemocy oraz poczucie bezpieczeństwa uczniów w szkole mają związek z cyberprzemocą rówieśniczą. Im bezpieczniej czują się uczniowie w szkole, tym mniejsze prawdopodobieństwo angażowania się w cyberprzemoc w każdej z ról[84].

Doświadczanie cyberprzemocy w charakterze świadka

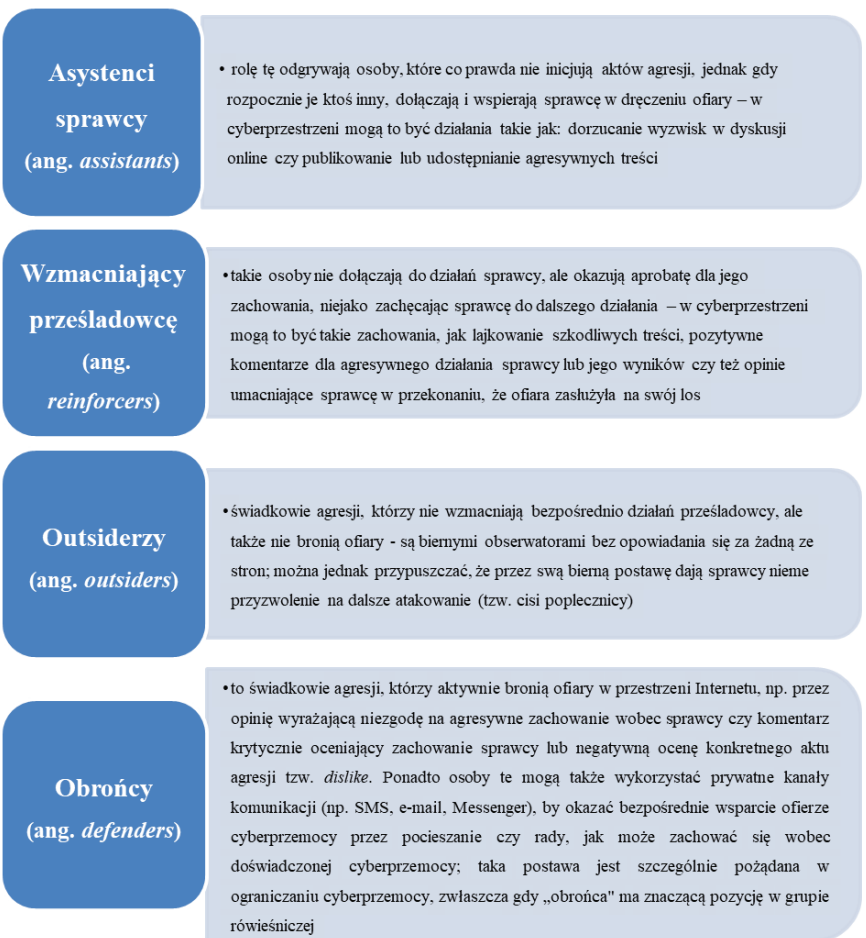
Osoby, które są świadkami zastraszania, zarówno online, jak i offline, odgrywają ważną rolę w utrzymywaniu, eskalacji lub ograniczaniu zachowań zastraszających, w zależności od ich reakcji i gotowości do podjęcia interwencji. Chociaż stosunkowo niewiele badań naukowych uwzględniało rolę osób obserwujących cyberprzemoc, to wiadomo, że zarówno zachowania osobiste, jak i sytuacyjne mogą wpływać na zachowanie świadków. Na przykład mniej prawdopodobne jest, że wsparcie zostanie udzielone ofiarom reagującym biernie na prześladowanie i najprawdopodobniej zapewnione będzie ono przez obserwatorów o wysokim poziomie empatii[85].

Rola świadków w cyberprzestrzeni wydaje się bardziej znacząca niż w kontakcie bezpośrednim, nadaje bowiem tym samym zachowaniom inny wymiar niż w realnej rzeczywistości społecznej. Sposób zachowa-

---

[83] A. Borkowska, dz. cyt., s. 16.
[84] R.M. Kowalski, S.P. Limber, A. McCord, dz. cyt., s. 29.
[85] Zob. G. Brewer, J. Kerslake, dz. cyt., s. 258–259.

nia świadków cyberprzemocy może oddziaływać i na jego ofiarę, i na sprawcę. Dla cyberofiary reakcja świadka może mieć charakter terapeutyczny (gdy wspiera ofiarę) lub toksyczny (gdy wzmacnia zachowania



Rysunek 5. Role świadków przemocy (opracowanie własne na podstawie: C. Salmivalli, *Participant role approach to school bullying: Implications for interventions*, „Journal of Adolescence" 1999, 22(4), s. 669; C. Salmivalli, M. Voeten, E. Poskiparta, *Bystanders matter: Associations between reinforcing, defending, and the frequency of bullying behavior in classrooms*, „Journal of Clinical Child & Adolescent Psychology" 2011, 40(5) s. 669)

sprawcy)[86]. Christina Salmivalli[87] wyróżnia role świadków przemocy, które mogą mieć wpływ na eskalację przemocy, a ich charakter i konsekwencje działania dają się odnieść także do problemu cyberprzemocy.

Wyrażanie niezgody na obserwowane akty cybeprzemocy oraz stawanie w obronie ich ofiary stanowi jeden z najskuteczniejszych sposobów powstrzymania agresji. Niezależnie, czy świadkowie są bliskimi znajomymi ofiary, czy też przypadkowymi widzami, powinni w sposób akceptowalny wyrazić dezaprobatę dla czynu widocznego w sieci. Niestety świadkowie dość rzadko przyjmują rolę „obrońców". Powodami takiej bierności jest często strach przed agresorem i obawa o możliwość podzielenia losu ofiary. Paradoksalnie empatia, która z jednej strony może skłaniać do ograniczenia zachowań przemocowych w sieci, z drugiej może stać się swoistym hamulcem przed podjęciem działania (świadek rozumie emocje ofiary i nie chce przeżywać ich osobiście). Świadkowie podlegają także opisanemu wcześniej efektowi kabiny pilota (nie widzą cierpienia ofiary i nie muszą mierzyć się z jego reakcjami i emocjami) oraz swoistej desensytyzacji (nie reagują na negatywne zachowania, które często obserwują i które często pozostają bezkarne). Świadkowie cyberprzemocy mogliby także wspierać ofiarę, komunikując jej swoje poparcie, oferując pomoc lub zgłaszając incydent osobom dorosłym lub odpowiednim służbom. Niestety w społeczeństwie informowanie o pewnych nieakceptowanych normą zdarzeniach ocenia się często negatywnie i traktuje jako rodzaj donosu. Z powyższych względów w działaniach profilaktycznych i interwencyjnych należy uwzględniać także tę grupę doświadczającą cyberprzemocy.

Skala cyberprzemocy w Polsce

Według raportu badawczego NASK „Nastolatki 3.0" zdecydowana większość badanych nastolatków natknęła się na przejawy przemocy inter-

[86] Por. J. Barlińska, A. Szuster, dz. cyt., s. 17, 19.

[87] Por. C. Salmivalli, M. Voeten, E. Poskiparta, *Bystanders matter: Associations between reinforcing, defending, and the frequency of bullying behavior in classrooms*, „Journal of Clinical Child & Adolescent Psychology" 2011, 40(5), s. 669; C. Salmivalli, *Participant role approach to school bullying: Implications for interventions*, „Journal of Adolescence" 1999, 22(4), s. 454.

netowej, kierowanej przeciwko znajomej lub znajomemu. Młodzi ludzie spotykali się najczęściej z takimi przejawami agresji, jak: wyzywanie (44,6%), ośmieszanie (44,3%) czy poniżanie (43,3%). Znaczna część respondentów obserwowała również rozprzestrzenianie kompromitujących treści na czyjś temat, podszywanie się pod kogoś, straszenie czy nawet szantażowanie. Rolę ofiary w różnych formach przeżyła prawie połowa badanych (48,8%). Blisko co dziesiąty badany twierdzi także, że w przeszłości doświadczył rozpowszechniania kompromitujących materiałów oraz był w Internecie szantażowany[88]. Od 7% do 11% polskich uczniów doznało najpoważniejszych aktów internetowej agresji, czyli regularnego, długotrwałego nękania w sieci przez rówieśników[89].

W 2017 r. Najwyższa Izba Kontroli przeprowadziła kontrolę dotyczącą cyberprzemocy wśród dzieci i młodzieży. Raport NIK zawierał wyniki wybranych badań dotyczących problemu cyberprzemocy (wybrane aspekty), co pozwoliło stwierdzić, że „w zależności od okresu prowadzonych badań, populacji badanych uczniów (jej rozkładu wiekowego oraz struktury), a także sposobu i rodzaju stawianych pytań wynika, że problem cyberprzemocy dotyczy od 6% do 60% ankietowanych"[90].

Tabela 3. Wyniki wybranych badań dotyczących problemu cyberprzemocy (wybrane aspekty)

Badanie	Pytanie badawcze	Wynik/odpowiedzi twierdzące
Badania dr. hab. Jacka Pyżalskiego, publikacja *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży* (2010)	Obrażałem lub wyzywałem podczas gier online	36%
	Przynajmniej raz wysłałem wiadomości przez komunikator, aby kogoś obrazić lub wystraszyć	40%
	Przynajmniej raz celowo wykluczyłem kogoś lub nie dopuściłem do grona znajomych w Internecie, żeby mu dokuczyć	31%
	Byłem zaangażowany w cyberprzemoc jako sprawca, ofiara lub sprawca-ofiara	33%

[88] M. Bochenek, R. Lange (red.), dz. cyt., s. 62–63.

[89] A. Borkowska, dz. cyt., s. 11.

[90] *Informacja o wynikach kontroli. Zapobieganie i przeciwdziałanie cyberprzemocy wśród dzieci i młodzieży*, NIK, Warszawa 2017, s. 19, https://www.nik.gov.pl/plik/id,15249,vp,17730.pdf (dostęp: 25.10.2019).

Tabela 3 (cd.)

Badanie	Pytanie badawcze	Wynik/odpowiedzi twierdzące
Raport EU Kids Online (2010)	Odsetek dzieci w wieku 9–16 lat, które doznały przemocy elektronicznej	6%
Raport Instytutu Socjologii Uniwersytetu Warszawskiego (2011)	Otrzymałem obraźliwy e-mail lub wiadomość gadu-gadu	11%
Raport Net Children Go Mobile (2014)	Doświadczyłem opublikowania wbrew swej woli materiałów na swój temat w Internecie	5%
	Odsetek dzieci w wieku 9–16 lat, które doznały przemocy elektronicznej	12%
Raport IBE Bezpieczeństwo i klimat społeczny w polskich szkołach (2015)	Agresja elektroniczna – gimnazjum	29%
	Agresja elektroniczna – szkoła podstawowa	25%
„Nastolatki 3.0" – badanie NASK (2016)	Zdarzyło się, że ktoś użył Internetu do poniżania, ośmieszania mnie	19,4%
	Zdarzyło się, że ktoś użył Internetu do wyzywania mnie	32,2%
	Spotkałem się z sytuacją, że ktoś użył Internetu do poniżania, ośmieszania mojego znajomego	58,1%
	Spotkałem się z sytuacją, że ktoś użył Internetu do wyzywania mojego znajomego	59,7%
Ankieta w szkołach w trakcie kontroli (2017)	Spotkałem się ze zjawiskiem cyberprzemocy	39,5%

Źródło: *Informacja o wynikach kontroli. Zapobieganie i przeciwdziałanie cyberprzemocy wśród dzieci i młodzieży*, NIK, Warszawa 2017, s. 19.

Poszkodowanymi w wyniku przemocy w sieci równie często stają się uczniowie w różnym wieku. Nie obserwuje się też zależności ze względu na płeć badanych. Tym samym przemoc dotyka nastolatków bez względu na ich zróżnicowanie społeczno-demograficzne.

Tymczasem rodzice nie zdają sobie sprawy ze skali cyberprzemocy. Choć 48,8% nastolatków twierdzi, że było ofiarą agresji słownej w sieci,

to niewielu rodziców wie (15,8%), że ich dziecko doświadczyło tego rodzaju przemocy w Internecie[91]. Dzieje się tak dlatego, że blisko co trzeci poszkodowany nie zgłasza problemu i nie podejmuje żadnego działania (np. rozmowy z bliskimi lub kimś, kto mógłby udzielić wsparcia w takiej sytuacji)[92]. Uczniowie najczęściej w samotności borykają się z problemami nękania. Dzieci nie mówią o swojej sytuacji dorosłym z wielu powodów. Barbara Coloroso wskazała kilka przyczyn zatajania problemu agresji rówieśniczej, m.in.:

- wstydzą się tego, że są dręczone;
- boją się odwetu;
- nie sądzą, że ktokolwiek może im pomóc;
- nie wierzą, że ktoś będzie chciał im pomóc;
- dzieci zastraszane przez dorosłych uwierzyły, że mogą być zastraszane przez rówieśników;
- nauczyły się, że „donoszenie" nie jest w porządku[93].

Na oficjalnej stronie internetowej rządu Stanów Zjednoczonych (stopbullying.gov) uzupełniono repertuar możliwych przyczyn przemilczania problemu doświadczania przemocy i cyberprzemocy w charakterze ofiary. Skrzywdzone osoby nie szukają pomocy u dorosłych, ponieważ:

- czują się bezradne – dzieci mogą chcieć samodzielnie poradzić sobie z problemem, aby znów odzyskać kontrolę; mogą bać się, że będą postrzegane jako słabe lub „skarżypyty";
- prześladowanie może być upokarzającym doświadczeniem – ofiary mogą obawiać się ponownego upokorzenia, gdy dorośli poznają obraźliwe treści na ich temat; mogą się również obawiać, że zostaną źle osądzeni lub ukarani za to, że są słabi;
- czują się odizolowane społecznie – mogą sądzić, że nikogo nie obchodzi ich sytuacja lub, że nikt ich nie zrozumie;

---

[91] Raport „Nastolatki 3.0" za: A. Borkowska, dz. cyt., s. 12.

[92] Za: M. Bochenek, R. Lange (red.), dz. cyt., s. 6.

[93] Por. B. Coloroso, *The bully, the bullied and the bystander*, Quill. Harper Collins, New York 2002; J. Węgrzynowska, dz. cyt., s. 13.

- obawiają się odrzucenia przez rówieśników – przyjaciele mogą pomóc chronić dzieci przed prześladowaniem, ale ofiary mogą obawiać się utraty tego wsparcia[94].

W związku z rosnącym prawdopodobieństwem doświadczania cyberprzemocy w różnym charakterze i formie oraz świadomości negatywnych konsekwencji takich doświadczeń zachodzi potrzeba podjęcia działań profilaktycznych mających na celu redukcję problemu cyberprzemocy oraz podniesienie świadomości rodziców, nauczycieli i wychowawców umożliwiających rozpoznawanie objawów cyberagresji oraz wspieranie wszystkich poszkodowanych w wyniku jej działania.

Profilaktyka cyberprzemocy

Edukacja na rzecz przeciwdziałania zjawisku i skutkom cyberprzemocy

Czynnikiem sprzyjającym minimalizowaniu ryzyka cyberprzemocy i jej skutków jest szeroko rozumiana edukacja. Jej odbiorcami powinni być zarówno młodzi ludzie, jak i ich rodzice oraz nauczyciele. Uzasadnieniem działań edukacyjnych w kontekście profilaktyki zagrożeń przemocy i cyberprzemocy jest potrzeba osobistej ochrony potencjalnych cyberofiar oraz redukcja skali przemocy wirtualnej.

W 2015 r. przeprowadzono w Polsce badania diagnozujące poziom kompetencji związanych z bezpieczeństwem cyfrowym w polskich szkołach, w których udział wzięli uczniowie, nauczyciele i rodzice. Okazało się, że wszystkie grupy badanych wykazują niewystarczający poziom kompetencji do radzenia sobie z zagrożeniami cyfrowymi. Najniższy wynik uzyskali rodzice (55%), a najwyższy poziom kompetencji reprezentują uczniowie (60%). Poziom tychże kompetencji wśród badanych nauczycieli jest nieznacznie wyższy (57%) niż wśród badanych rodziców. Wszystkie grupy najlepiej radzą sobie z kompetencjami technicznymi używania Internetu, najsłabiej z kompetencjami społeczny-

[94] *Why don't kids ask for help?*, stopbullying.gov, oficjalna strona internetowa rządu Stanów Zjednoczonych, https://www.stopbullying.gov/cyberbullying/what-is-it/index.html (dostęp: 11.11.2019).

mi, co stanowi źródło realnego zagrożenia w cyberprzestrzeni, jako że większość najpoważniejszych zagrożeń w sieci ma charakter społeczny. Biorąc pod uwagę rozpiętość skali kompetencji (0–100%), należy stwierdzić, że uzyskane wyniki wszystkich badanych wskazują niewystarczający zasób wiedzy i umiejętności, by skutecznie chronić siebie i innych przed zagrożeniami cyfrowymi[95].

Najważniejsze jest zatem kształcenie w zakresie wartości i umiejętności społecznych, do których należy dodać elementy odnoszące się konkretnie do korzystania z telefonów komórkowych i Internetu. Dzieci i młodzież powinny posiąść odpowiednią umiejętność posługiwania się technologią cyfrową, poznając zalety elektronicznych urządzeń komunikacyjnych, ale także ich potencjalne niebezpieczeństwa i sposoby zapobiegania im. Szkolenie w zakresie tych wartości, wiedzy i umiejętności powinno być obowiązkiem szkoły, rodziny i społeczeństwa.

Mając na uwadze nieprzygotowanie większości członków społeczeństwa na doświadczenie przemocy, trzeba zadbać, by wymienione wcześniej wymiary edukacji na rzecz efektywnego wychodzenia z kryzysów przemocowych uwzględniały realizację działań edukacyjnych w sposób kompleksowy w obrębie trzech poziomów:

- poziom profilaktyczny – obejmujący szeroko pojętą edukację informacyjną, medialną i obywatelską mającą na celu uświadomienie zagrożeń, ich źródeł i mechanizmów działania, potencjalnych skutków szeroko rozumianej przemocy oraz możliwych sposobów jej przeciwdziałania, zarówno w odniesieniu do ofiar, sprawców, jak i świadków przemocy;
- poziom psychologiczno-społeczny – obejmujący działania dążące do kształtowania właściwych postaw wobec przejawów przemocy (zarówno w charakterze ofiary, jak i świadka przemocy) oraz użytkowania mediów, a także ukierunkowanych na treningi: komunikacji interpersonalnej i zapośredniczonej, asertywności, empatii, konstruktywnych sposobów zaspokajania potrzeb

[95] Ł. Tomczyk, Ł. Srokowski, *Kompetencje w zakresie bezpieczeństwa cyfrowego w polskiej szkole*, raport z badań, Stowarzyszenie Miast w Internecie, Tarnów, 2016, s. 4–5, https://www.mwi.pl/uploads/filemanager/publikacje/Raport%20z%20badan_wersja%20finalna.pdf (dostęp: 14.09.2019).

i rozwiązywania problemów oraz radzenia sobie ze stresem czy skutkami zachowań agresywnych;

- poziom interwencyjny – koncentrujący się na działaniach ukierunkowanych na rozpoznawanie objawów przemocy i uświadamianie możliwych sposobów przeciwstawiania się szeroko pojętej przemocy oraz dostarczanie wiedzy w zakresie możliwości zgłaszania problemów, przeciwdziałania im, uzyskiwania pomocy prawnej czy psychologicznej, a także możliwości terapii (zarówno ofiar, jak i sprawców przemocy)[96].

Interwencje powinny mieć także na celu wzmocnienie pozycji uczniów przez ukierunkowanie ich postaw, umiejętności rozwiązywania problemów i poczucia kontroli w skuteczniejszym reagowaniu na cyberprześladowanie. Gayle Brewer i Jade Kerslake[97], powołując się na badania naukowe, uważają, że szczególnie skuteczne mogą być interwencje oparte na poczuciu własnej wartości i empatii. W przywoływanych przez autorów badaniach przypadki interwencji skoncentrowanych na empatii lub inteligencji emocjonalnej zarówno zwiększyły poziom empatii, jak i zmniejszyły częstość zachowań zastraszających. Interwencje psychologiczne mogą natomiast skutecznie podnieść samoocenę, której niska wartość może warunkować zarówno popełnianie, jak i wiktymizację cyberprzemocy. Takie interwencje mogą zatem potencjalnie ograniczać występowanie przypadków cyberprzemocy i wzmacniać odporność sieciową.

Warto zadbać, by działania edukacyjne prowadzili profesjonaliści, jednak również w Internecie można znaleźć wiele profesjonalnych materiałów edukacyjnych. Takim przykładem są zasoby przygotowane przez Fundację Dajemy Dzieciom Siłę, która prowadzi szeroko zakrojone działania edukacyjne dla dzieci, rodziców/opiekunów i profesjonalistów w zakresie przeciwdziałania przemocy wobec dzieci, rozwoju umiejętności reagowania na zagrożenia, podnoszenia kompetencji wychowawczych i podejmowania interwencji w przypadkach podejrzenia

---

[96] D. Siemieniecka, M. Skibińska, *Stalking and cyberstalking as a form of violence*, „Society, Integration, Education" 2019, 3, s. 409–410.

[97] G. Brewer, J. Kerslake, dz. cyt., s. 258–259.

krzywdzenia dzieci. Przygotowane przez Fundację narzędzia edukacyjne (scenariusze zajęć, kursy e-learning) oraz informacje o szkoleniach dla profesjonalistów są dostępne na platformie edukacyjnej pod adresem http://edukacja.fdds.pl[98]. Innym przykładem jest Akademia NASK, która zajmuje się bezpieczeństwem dzieci i młodzieży w Internecie oraz zwiększania kompetencji cyfrowych m.in. przez organizację konferencji i szkoleń oraz publikację webinariów, poradników i multimedialnych materiałów edukacyjnych. Wszystkie materiały są dostępne na stronie Akademii NASK (https://akademia.nask.pl/).

Szerzej na temat programów edukacyjnych i profilaktycznych w zakresie przemocy można przeczytać w pierwszym tomie monografii autorstwa Bronisława Siemienieckiego, Wioletty Kwiatkowskej, Lidii Wiśniewskej-Nogaj pt. *Agresja – zjawisko, skutki, zapobieganie. Perspektywa pedagogiki kognitywistycznej, psychoprofilaktyki oraz edukacji moralnej*[99], w następnym rozdziale prezentowanej książki zostanie natomiast przedstawiony praktyczny przykład procedur przeciwko cyberagresji w szkole.

Atmosfera w rodzinie

Technologia jest wygodnym narzędziem do komunikacji i wymiany informacji, ale tak jak w przypadku wszystkich narzędzi, z których dzieci uczą się korzystać, rodzice powinni zapewnić nadzór i ustalić zasady ich używania, aby zagwarantować swoim dzieciom bezpieczeństwo i satysfakcjonującą pracę z udziałem narzędzi. Podobnie jest z narzędziami informacyjno-komunikacyjnymi, jednak problem może stanowić niewystarczająca wiedza technologiczna rodziców dotycząca możliwości działania i zagrożeń wynikających z korzystania z mediów sieciowych. Świadomi rodzice powinni zatem dążyć do poznania narzędzi, jakimi na co dzień posługują się ich dzieci, oraz stylu ich użytkowania. Dobrą atmosferę w rodzinie budują dobre relacje rodziców i dzieci na podsta-

[98] Oferta edukacyjna, Fundacja Dajemy Dzieciom Siłę, https://fdds.pl/oferta/oferta-edukacyjna/ (dostęp: 25.10.2019).

[99] B. Siemieniecki, W. Kwiatkowska, L. Wiśniewska-Nogaj, dz. cyt.

wie wzajemnego zaufania, szacunku, zainteresowania potrzebami, aktywnościami, możliwościami i trudnościami poszczególnych członków rodziny. W budowaniu właściwych relacji i wspieraniu sieciowej aktywności dzieci i młodzieży pomocne mogą okazać się otwarta i systematyczna rozmowa oraz dbałość o realizację poniższych postulatów[100]:

- **zainteresowanie światem online swoich dzieci,** tak jak każdym innym aspektem ich życia – należy poznać technologię i zainteresowania swoich dzieci, które mogą być nauczycielami rodzica/ /opiekuna, pokazując mu jednocześnie, co robią online; powinno się zaznajomić ze wszystkimi funkcjami używanych przez dzieci narzędzi (telefony komórkowe z dostępem do Internetu trzeba traktować na równi z komputerami domowymi); regularne rozmowy z dziećmi na temat problemów w Internecie pozwolą wspólnie „oswoić" problem i odpowiednio na niego zareagować; dzieci muszą wiedzieć, że zawsze mogą przyjść do rodzica po pomoc, kiedy coś wydaje im się nieodpowiednie, niepokoi je lub przestrasza;
- **ustalenie rozsądnych zasad i limitów** – trzeba pomóc dzieciom nauczyć się podejmować odpowiedzialne decyzje dotyczące korzystania z technologii, wspólnie ustanawiając wytyczne dotyczące korzystania z urządzeń medialnych, sprawując dyskretną kontrolę w razie potrzeby (należy unikać umiejscowienia komputera w pokoju dziecka, dobrze, by w domu korzystało z telefonu w pobliżu rodzica); warto jest także pozyskać informacje na temat kontroli rodzicielskiej we wszystkich technologiach, z których korzystają dzieci;
- **poznaj znajomych online swoich dzieci** – nawiązywanie znajomości w Internecie jest szybkie i łatwe, dlatego rodzic lub starsze rodzeństwo powinni pomóc dzieciom poznać różnicę między prawdziwym przyjacielem a przyjaznym nieznajomym. Należałoby zatem monitorować wirtualne przyjaźnie, zadając pytania

[100] Por. *Parents can prevent cyberbullying*, oficjalna strona internetowa National Parent Teacher Association, https://www.pta.org/home/family-resources/safety/Digital-Safety/Parents-Can-Prevent-Cyberbullying (dostęp: 6.11.2019).

dotyczące ich przyjaciół w świecie fizycznym. Warto zachęcać swoje dzieci, aby nigdy nie upowszechniały żadnych informacji, które ujawniłyby, kim są, gdzie mieszkają lub gdzie chodzą do szkoły itp. Powinno się je poinstruować, aby nigdy nie umawiały się osobiście ze znajomymi online, których nie znały wcześniej ze świata rzeczywistego; warto również zostać ich znajomym[101] (lub poprosić o to innego zaufanego dorosłego), by w razie potrzeby zaobserwować niepokojące sytuacje i móc na nie reagować.

Świadomość zagrożeń sieciowych i znajomość podstawowych reguł korzystania z mediów społecznościowych pozwolą z natury ufnym dzieciom zminimalizować ryzyko stania się ofiarą cyberprzemocy. Warto zatem, by rodzice omówili wspólnie z dziećmi kilka zasad bezpiecznej obecności w sieci. Pomocne mogą być wskazówki z poradnika dla rodziców przygotowanego w ramach kampanii Ministerstwa Cyfryzacji i NASK[102] – „Nie zagub dziecka w sieci" – pt. *Cyberprzemoc – włącz blokadę na nękanie*:

- Rozmawiaj z dzieckiem o zjawiskach, które mają miejsce w internecie. Sprawdź, co twoje dziecko wie o cyberprzemocy i czy zna sposoby reagowania w sytuacji, gdy ktoś jest nękany online.
- Umów się z dzieckiem, że jeśli przydarzy się coś, co je zaniepokoi lub zdenerwuje, może do ciebie ze wszystkim się zwrócić. Zapewnij, że jeśli ktoś dokucza mu w sieci, wystarczy, że cię o tym powiadomi, a ty postarasz się mu pomóc.
- Rozmawiaj z dzieckiem o zasadach ochrony prywatności w internecie. Uświadom mu, jakie zagrożenia wiążą się z nadmiernym publikowaniem informacji o sobie, zamieszczaniem swoich zdjęć i filmów w sieci, dzieleniem się na portalach społecznościowych swoimi myślami i przeżywanymi uczuciami. Porozmawiajcie o tym, w jaki sposób niektórzy internauci mogą wykorzystać takie informacje.

---

[101] Pomocne mogą okazać się materiały edukacyjne opublikowane w ramach projekt edukacyjnego „Zostań znajomym swojego dziecka" dostępne online: https://www.saferinternet.pl/projekty/projekty-edukacyjne/zostan-znajomym-swojego-dziecka.html.

[102] Naukowa i Akademicka Sieć Komputerowa.

- Uczul dziecko, że wszystko, co opublikuje w sieci, może zostać skopiowane i rozpowszechnione niekoniecznie w taki sposób, w jaki byśmy chcieli.
- Jeśli zdecyduje się na publikowanie swoich zdjęć, np. na portalach społecznościowych, doradź mu, aby w statusie prywatności zaznaczyło opcję, która umożliwi oglądanie ich tylko przez znajome osoby.
- Ustal z dzieckiem, jakie materiały może publikować w internecie i z kim może się komunikować.
- Porozmawiaj o ustawieniach prywatności w różnych serwisach, z których korzysta twoje dziecko. Zadbaj, aby tylko znajomi mieli dostęp do jego profilu.
- Przypomnij dziecku, aby zawsze wylogowało się z serwisu (portalu społecznościowego, poczty, komunikatora itp.) po zakończeniu sesji.
- W ten sposób zabezpieczy swoje konto przed niepowołanym dostępem innych osób.
- W przypadku młodszych dzieci, zainstaluj programy ochrony rodzicielskiej i antywirusowe na sprzęcie, z którego dziecko korzysta[103].

Właściwe relacje w rodzinie, oparte na spójnym systemie wartości, akceptacji i miłości, pozwalają każdemu człowiekowi funkcjonować w sposób prawidłowy, zarówno w wymiarze jednostkowym, jak i społecznym. Taki psychospołeczny dobrostan jest niezbędny, by dokonywać wartościowych ocen, decyzji i wyborów. Współczesna cywilizacja wymaga jednak większej mobilizacji sił dorosłych pokoleń, by godnie wprowadzać w życie wybiegające technologicznie, ale zagubione emocjonalnie i moralnie pokolenie najmłodszych.

Reagowanie – ofiara cyberprzemocy

Właściwa atmosfera domowa oparta na wzajemnej więzi i dobrych relacjach, umacnianych dzięki zaufaniu, byciu razem, spędzaniu wolnego czasu, rozmowom i wspólnemu rozwiązywaniu problemów, stanowi nie tylko źródło wzajemnej wiedzy o sobie, ale także czynnik ochron-

[103] A. Borkowska, dz. cyt., s. 17–18.

ny przeciw cyberprzemocy. Prawidłowo funkcjonujące środowisko rodzinne daje również dzieciom i młodzieży swoistą siłę pozwalającą minimalizować ryzyko skutków tego zjawiska. W takim środowisku łatwiej zaobserwować pewne symptomy przemocy online. Według Sameera Hinduja i Justina W. Patchina[104] dziecko może być celem cybernękania, jeśli następuje zauważalna zmiana jego zachowań, np.:

- nieoczekiwanie przestaje korzystać z telefonu, tabletu lub komputera;
- wydaje się nerwowe podczas korzystania z technologii (np. otrzymaniu SMS-a) lub sprawia wrażenie złego, przygnębionego, sfrustrowanego w trakcie lub zaraz po zakończeniu aktywności online;
- odczuwa niepokój związany z chodzeniem do szkoły lub w ogóle z wychodzeniem z domu;
- ciągle śpi lub ma problemy ze snem;
- nieoczekiwanie unika kontaktu z przyjaciółmi i członkami rodziny;
- występują u niego zaburzenia łaknienia (nadmierny lub obniżony apetyt);
- wydaje się stale przygnębione;
- wspomina o samobójstwie lub bezsensowności życia;
- traci zainteresowanie rzeczami, które dotychczas były dla niego ważne i przyjemne (np. hobby, pewne aktywności);
- unika rozmów na temat tego, co robi online;
- pojawiają się informacje ze szkoły dotyczące częstych lub przedłużających się nieobecności;
- pragnie spędzać znacznie więcej czasu z rodzicami niż rówieśnikami;
- staje się skryte, szczególnie gdy chodzi o jego aktywność online.

[104] S. Hinduja, J.W. Patchin, *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*, Corwin Press, Thousand Oaks 2015, s. 180.

Zauważalna i nieuzasadniona znanymi rodzinie okolicznościami zmiana powinna skłonić do podjęcia rozmowy z dzieckiem i zachęcenia go do wyjawienia przyczyn zaobserwowanej przez najbliższe otoczenie zmiany zachowania. Jeśli dziecko milczy lub zaprzecza problemom, jego opiekunowie powinni zapewnić je o swoim uczuciu oraz o tym, że z każdym problemem może się do nich zwrócić. Powinni także zadeklarować swoją pomoc w rozwiązaniu problemu. Można równolegle przeprowadzić wywiad w szkole, u najbliższych znajomych na temat funkcjonowania dziecka w środowisku szkolnym i rówieśniczym. Jeśli wybrani członkowie rodzin znają ulubione aktywności sieciowe dziecka lub w mediach społecznościowych mają status jego znajomych, powinni starannie przyjrzeć się tym aktywnościom. Po uzyskaniu informacji potwierdzających doświadczenie przez dziecko cyberprzemocy w charakterze ofiary należy niezwłocznie podjąć starania mające na celu udzielenie pomocy poszkodowanemu oraz zablokowanie działań sprawcy.

Jeśli dziecko samo wyjawiło problem, trzeba właściwie zareagować, prowadząc z wyczuciem rozmowę i słuchając dziecka bez okazywania zdenerwowania, niepokoju czy złości. To bardzo trudne, jednak dziecko potrzebuje wsparcia dorosłego. W wyniku cybernękania poczucie bezpieczeństwa i własnej wartości dziecka zostało zachwiane. Rolą rodziny jest pomoc w procesie odzyskiwania utraconych wartości oraz w późniejszym czasie wypracowanie strategii ograniczających ponowne doświadczanie cyberprzemocy w jakiejkolwiek z ról. Dlatego trzeba zapewnić ofiarę, że dobrze zrobiła, mówiąc o tym, co jej się przytrafiło, i docenić siłę, dzięki której dzieli się z dorosłym trudnymi dla niej informacjami i przeżyciami. Należy również zaznaczyć, że nikt nie ma prawa jej krzywdzić ani obarczać winą za to, co ją spotkało. Dorosły powinien starać się logicznie oceniać wszystkie uzyskane od ofiary informacje, spokojnie i rzeczowo zdobyć nowe szczegóły oraz zrozumieć cały kontekst sytuacji.

Tabela 4. Wskazówki dla rodziców ofiar cyberprzemocy

CO ROBIĆ, GDY TWOJE DZIECKO JEST OFIARĄ CYBERPRZEMOCY
Świadomość, że Twoje dziecko jest cybernękane, jest bolesna. Oto co można zrobić: 1. UPEWNIJ SIĘ, ŻE TWOJE DZIECKO JEST (I CZUJE SIĘ) BEZPIECZNE. Bezpieczeństwo i dobre samopoczucie Twojego dziecka zawsze powinno być priorytetem. Przekazuj bezwarunkowe wsparcie. Rodzice muszą pokazać swoim dzieciom poprzez słowa i działania, że oboje pragną tego samego rezultatu: powstrzymania cyberprzemocy. 2. POROZMAWIAJ ZE SWOIM DZIECKIEM I POSŁUCHAJ GO. Angażuj dziecko w rozmowę o tym, co się dzieje, w spokojny sposób. Nie panikuj. Poświęć trochę czasu, aby dowiedzieć się dokładnie, co się wydarzyło, poznaj kontekst, w którym to nastąpiło. Nie bagatelizuj sytuacji ani nie usprawiedliwiaj agresora. 3. ZBIERAJ DOWODY. Wydrukuj lub wykonaj zrzuty ekranu lub nagrania rozmów, wiadomości, zdjęć, filmów i wszelkich innych elementów, które mogą stanowić wyraźny dowód na to, że Twoje dziecko jest ofiarą cyberprzemocy. Prowadź rejestr wszystkich incydentów, aby pomóc w dochodzeniu. Zachowaj także notatki dotyczące istotnych szczegółów, takich jak lokalizacja, częstotliwość, stopień szkody, zaangażowanie osób trzecich lub świadków zdarzenia oraz przebieg zdarzeń. 4. WSPÓŁPRACUJ ZE SZKOŁĄ. Polskie prawo oświatowe zobowiązuje szkoły do zapewnienia uczniom bezpieczeństwa i podejmowania interwencji, jeśli to bezpieczeństwo zostanie zagrożone. Szkoły mają także obowiązek współpracy z rodzicami zarówno sprawców przemocy, jak i uczniów, którzy agresji doświadczają. Zwróć się o pomoc do wychowawcy klasy i dyrekcji szkoły, jeśli ofiara i agresor chodzą do tej samej szkoły. Twoje dziecko ma prawo czuć się bezpiecznie w szkole, a wychowawcy i dyrekcja są odpowiedzialni za zapewnienie tego poczucia poprzez dochodzenie i odpowiednią reakcję. 5. POWSTRZYMAJ SIĘ OD KONTAKTOWANIA SIĘ Z RODZICAMI CYBERSPRAWCY. Niektórzy rodzice skonfrontowani z zarzutami, że ich dziecko angażuje się w cyberprzemoc, mogą stać się jego obrońcami i dlatego mogą nie być otwarci na konstruktywną rozmowę. Bądź rozsądny w swoim podejściu, aby uniknąć dodatkowego dramatu i ewentualnych odwetów. 6. SKONTAKTUJ SIĘ Z DOSTAWCĄ TREŚCI. Cybernękanie narusza warunki świadczenia usług wszystkich legalnych dostawców usług (stron internetowych, aplikacji, sieci gier, firm internetowych lub komórkowych). Administrator ma obowiązek zareagować. Do podjęcia działania zobowiązuje go art. 14 Ustawy o świadczeniu usług drogą elektroniczną. Warto pamiętać, aby zgłaszając naruszenie, powołać się na odpowiedni przepis regulaminu danego serwisu oraz dołączyć dowody cyberprzemocy. Bez względu na to, czy Twoje dziecko może zidentyfikować, kto je nęka, skontaktuj się z odpowiednim dostawcą lub zgłoś incydent do CSIRT NASK: https://incydent.cert.pl/. 7. JEŚLI TO KONIECZNE, SZUKAJ RADY. Twoje dziecko może skorzystać na rozmowie ze specjalistą z zakresu zdrowia psychicznego. Dzieci mogą preferować dialog z osobą trzecią, która może być postrzegana jako bardziej obiektywna, lub się jej mniej wstydzić. 8. JEŻELI PODŁOŻEM CYBERNĘKANIA JEST ODMIENNA RASA, SEKSUALNOŚĆ LUB NIEPEŁNOSPRAWNOŚĆ, skontaktuj się z Biurem Rzecznika Praw Obywatelskich lub Rzecznika Praw Dziecka (zgłoszenie sprawy: https://brpd.gov.pl/kontakt/ lub Dziecięcy Telefon Zaufania: 800 12 12 12). 9. SKONTAKTUJ SIĘ Z POLICJĄ. Jeśli uważasz, że wobec twojego dziecka dopuszczono się działań niezgodnych z prawem (zniesławienie lub zniewaga, naruszenie wizerunku, stalking, podszywanie się pod kogoś, groźby, włamania) lub zagrożone jest jego bezpieczeństwo, nie wahaj się i poinformuj policję. 10. ŚRODKI WYKONAWCZE W CELU ZAPOBIEGANIA NIEDOPUSZCZENIU. Jeśli Twoje dziecko jest zastraszane za pośrednictwem mediów społecznościowych (YouTube, Instagram, Snapchat, Twitter itp.), skonfiguruj kontrolę prywatności na każdej platformie, aby uniemożliwić prześladowcy kontakt z dzieckiem i zgłoś incydent (patrz pkt 6).

Źródło: S. Hinduja, J.W. Patchin, *What to do when your child is cyberbullied: Top ten tips for parents*, Cyberbullying Research Center, 2018, https://cyberbullying.org/tips-for-parents-when-your-child-is--cyberbullied.pdf (dostęp: 8.10.2019); tłumaczenie własne uwzględniające polski kontekst oświatowy, prawny i telekomunikacyjny.

Zadaniem rodziny i innych dorosłych jest zatem umiejętność dostrzeżenia problemu dziecka, wspieranego w sytuacji cybernękania, a także reagowanie na zachowania cybersprawcy i pokazanie wszystkim uczestnikom tego procederu, że cybernękanie jest traktowane poważnie. Schemat postępowania bliskich dorosłych powinien więc zawierać się w kilku podstawowych krokach (rysunek 6):

Rysunek 6. Schemat postępowania wobec cyberprzemocy (źródło: opracowanie własne na podstawie: *Prevent cyberbullying*, https://www.stopbullying.gov/cyberbullying/prevention (dostęp: 11.11.2019))

- Dostrzeż – należy rozpoznać, czy nastąpiła zmiana nastroju lub zachowania i sprawdzić, jaka może być tego przyczyna. Trzeba próbować ustalić, czy zmiany te pojawiły się w związku z korzystaniem przez dzieci z ich urządzeń cyfrowych.
- Rozmawiaj – następny krok polega na spokojnym i rzeczowym zadawaniu pytań, aby dowiedzieć się, co się dzieje, jak to się zaczęło i kto jest zaangażowany, jakie są skutki tego doświadczenia. Należy poradzić ofierze, by nie utrzymywała kontaktu ze sprawcą, nie odpowiadała na jego e-maile, telefony itp., zablokowała sprawcę w możliwych urządzeniach i usługach, w jakich próbował się z nią kontaktować.
- Dokumentuj – warto prowadzić rejestr tego, co i gdzie się dzieje. W miarę możliwości powinno się gromadzić wszystkie dowody cyberprzemocy, np. zapisywać wszystkie wiadomości w pamięci telefonu (zarówno tekstowe, jak i nagrane na pocztę głosową), archiwizować rozmowy z komunikatora (przez wydruk lub skopiowanie ich i zapisanie w dowolnym edytorze tekstu), robić wydruki lub zrzuty ekranu szkodliwych stron, postów lub treści z mediów społecznościowych (klawisze Ctrl i Print Screen lub wybierając opcję przeglądarki „Wykonaj zrzut ekranu"), archiwizować wiadomości z poczty elektronicznej (przez ich drukowanie lub robienie zrzutów ekranu, tak by widoczne były także

takie dane, jak data i nadawca wiadomości) oraz wszystkie załączniki – pomoże to nie tylko identyfikować sprawcę, ale także w razie konieczności ścigać go i ukarać.

- Zgłoś – większość platform społecznościowych i szkół ma określone zasady i procedury zgłaszania nieprawidłowych zachowań. Jeśli kolega z klasy jest cybersprawcą, należy powiadomić o tym szkołę. Można także skontaktować się z administratorem usługi telekomunikacyjnej lub platformy mediów społecznościowych, aby zgłosić obraźliwe treści i żądać ich usunięcia. Jeśli to nie skutkuje lub bezpieczeństwo dziecka jest zagrożone czy też dochodzi do potencjalnego przestępstwa lub zachowania niezgodnego z prawem, trzeba zgłosić to na policję.
- Wspieraj – rówieśnicy, znaczący i zaufani dorośli mogą czasem interweniować publicznie, aby pozytywnie wpłynąć na sytuację, w której rozpowszechniane są negatywne lub szkodliwe treści na temat dziecka. Interwencja publiczna może obejmować publikowanie pozytywnych komentarzy na temat krzywdzonej osoby, aby spróbować zmienić wydźwięk rozmowy na bardziej pozytywny. Może także pomóc w rozpoznaniu i dotarciu do cyberofiary lub do cybersprawcy, by wyrazić swoje obawy wynikające z niewłaściwego zachowania. Jeśli to możliwe, należy postarać się ustalić, czy potrzebne jest bardziej profesjonalne wsparcie dla osób zaangażowanych, takie jak rozmowa z psychologiem[105].

Najważniejszym wyzwaniem dla środowiska rodzinnego jest jednak umiejętne wspieranie ofiary w procesie odbudowy jej poczucia bezpieczeństwa, własnej wartości i kontroli sytuacji, a także to, by uwierzyła, że to nie ona jest winna zaistniałej sytuacji i nie musi sama zmagać się z problemem. Poszkodowana osoba powinna wiedzieć, że jest dostępna pomoc, z której może skorzystać, a co najważniejsze, może samodzielnie wykonać pewne działania, dzięki którym przejmie kontrolę nad sytuacją, by ostatecznie poradzić sobie z problemem.

---

[105] *Prevent cyberbullying*, stopbullying.gov, oficjalna strona internetowa rządu Stanów Zjednoczonych, https://www.stopbullying.gov/cyberbullying/prevention (dostęp: 11.11.2019).

Pomoc cyberofiarom

Najważniejszym zagadnieniem w przeciwdziałaniu cyberprzemocy i niwelowaniu jej skutków wydaje się poczucie kontroli. Badania przeprowadzone w Zakładzie Psychologii Osobowości i Psychologii Sądowej UG[106] wskazują, że ofiary cyberprzemocy reagują na stres, prezentując ekstremalnie zewnętrzne umiejscowienie poczucia kontroli nad zdarzeniami. Można zatem przypuszczać, że większość cyberofiar nie postrzega swojej mocy sprawczej w przeciwdziałaniu i niwelowaniu skutków przemocy online. Wniosek ten potwierdzają także inne wyniki badań, które uzyskali Trijntje Völlink i współpracownicy, dowodząc, że u ofiar przemocy dominują strategie radzenia sobie ze stresem skoncentrowane na emocjach, których skutkiem jest skupienie na własnych emocjach, myślenie życzeniowe i wycofanie[107], a nie racjonalna ocena sytuacji i mobilizacja działań.

Strategie radzenia sobie z cyberprzemocą powinny zatem koncentrować się na zwiększaniu kompetencji społecznych, komunikacyjnych i cyfrowych oraz odporności ofiary. Odporność to zdolność radzenia sobie z negatywnymi doświadczeniami online lub offline. Według Leen d'Haenens, Sofie Vandoninck i Verónici Donoso[108] odporność online oznacza wyposażenie w umiejętności radzenia sobie z negatywnymi doświadczeniami w sieci przez aktywne rozwiązywanie problemów, a nie pasywność, unikanie lub odwet na sprawcy[109].

---

[106] M. Szulc, *Sposoby radzenia sobie ze stresem i umiejscowienie poczucia kontroli u ofiar cyberprzemocy*, „Pomeranian Journal of Life Sciences" 2018, 64(3), http://ojs.pum.edu.pl/pomjlifesci/article/view/449 (dostęp: 20.01.2019).

[107] T. Völlink i in., *Coping with cyberbullying: Differences between victims, bully-victims and children not involved in bullying*, „Journal of Community & Applied Social Psychology" 2013, 23(1), s. 7–24.

[108] L. d'Haenens, S. Vandoninck, V. Donoso, *How to cope and build online resilience?*, United Kingdom, Europe: EU Kids Online, 2013, s. 1, http://eprints.lse.ac.uk/48115/1/How%20to%20cope%20and%20build%20online%20resilience%20%28lsero%29.pdf (dostęp: 5.10.2019).

[109] V. Skye Wingate, J.A. Minney, *Cyberbullying requires more than a virtual response*, w: M.F. Wright (ed.), *A Social-ecological approach to cyberbullying*, Nova Science Publishers, Inc., New York 2016, s. 367.

Strategie radzenia sobie z problemem są rozumiane jako myśli i zachowania przystosowujące do stresujących lub niepokojących sytuacji, w celu ochrony własnej przed dalszymi psychologicznymi szkodami. Wyróżnia się trzy kategorie takich strategii:

- fatalistyczne lub pasywne (np. żywienie nadziei, że problem sam zniknie lub ktoś inny go rozwiąże; chwilowe zaprzestanie korzystania z urządzenia, Internetu);
- komunikacyjne (rozmowa z kimś na temat problemu);
- proaktywne (nastawione na rozwiązywanie problemów, np. usuwanie niepożądanych treści, blokowanie sprawcy, zgłaszanie problemu)[110].

Strategie radzenia sobie z problemem, które zwiększają poczucie kontroli ofiar w sytuacjach cyberprzemocy, mają większe szanse powodzenia, ułatwiają rozwój odpowiednich umiejętności społecznych oraz zmniejszają skalę skutków cyberprzemocy. Badania międzynarodowe wykazały, że młodzież odporna online najczęściej radzi sobie z negatywnymi doświadczeniami w sieci za pomocą strategii komunikacyjnych i proaktywnych, szukając wsparcia przyjaciół, będąc cyfrowym sojusznikiem w zakresie ochrony siebie, dzieląc się informacjami o szkodliwej komunikacji i rozmawiając z osobą dorosłą na temat incydentów cyberprzemocy[111].

Strategie proaktywne obejmują także działania wymagające nie tylko właściwej postawy, ale również odpowiedniej wiedzy i umiejętności cyfrowych oraz pewnej świadomości prawnej. Ofiara i jej najbliżsi powinni wiedzieć, że należy gromadzić wszelkie dowody cyberprześladowania (opisane we wcześniejszej części rozdziału), zgłaszać incydenty odpowiednim służbom, takim jak administratorzy usług telekomunikacyjnych, ośrodki interwencyjne, wychowawca klasy i dyrekcja szkoły (jeśli agresor jest znany ofierze ze szkoły) itp. Ponadto należy mieć świadomość, że „niektóre akty internetowej agresji naruszają obecnie obowiązujące prawo (są uznawane za przestępstwo lub wykroczenie) i mogą zostać zgłoszone na policję, do prokuratury lub

---

[110] Na podstawie L. d'Haenens, S. Vandoninck, V. Donoso, dz. cyt., s. 2.

[111] Por. tamże, s. 3.

do sądu. Są to: zniesławienie lub zniewaga, naruszenie wizerunku, stalking, podszywanie się pod kogoś, groźby, włamania. W przypadku tych przestępstw/wykroczeń ściganie sprawcy cyberprzemocy następuje po złożeniu wniosku przez osobę pokrzywdzoną”[112].

W przypadku, gdy potrzebna jest specjalistyczna pomoc lub bliscy dorośli nie wiedzą, jak postąpić w danej sytuacji, można skorzystać z dostępnej pomocy telefonicznej umożliwiającej fachowe wsparcie i konsultacje (Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci: 800 100 100; Telefon Zaufania dla Dzieci i Młodzieży: 116 111; Dziecięcy Telefon Zaufania Rzecznika Praw Dziecka: 800 12 12 12).

Reagowanie – sprawca cyberprzemocy

Zazwyczaj ofiara cyberprzemocy zna sprawcę lub podejrzewa, kim on jest. Czasem jednak tożsamość sprawcy może być fałszywa lub anonimowa. Gdy pojawiają się problemy z identyfikacją agresora, a jego działania noszą znamiona przestępstwa, należy jak najszybciej zgłosić incydent policji i poprosić funkcjonariuszy o pomoc w ustaleniu jego danych.

Gdy tożsamość sprawcy jest znana, należy bezwzględnie zażądać od niego zaprzestania nękania i usunięcia szkodliwych treści. W przypadku odmowy lub gdy ustalenie sprawcy nie jest możliwe, trzeba skontaktować się z dostawcą usługi, by zgłosić incydent, żądać usunięcia krzywdzących materiałów. Administrator ma obowiązek zareagować, do podjęcia działania zobowiązuje go art. 14 Ustawy o świadczeniu usług drogą elektroniczną.

Znając tożsamość sprawcy, można podjąć kroki mające na celu w pierwszym rzędzie nakłonienie go do zaprzestania szkodliwych działań, a następnie zaplanowanie działań interwencyjnych, skutkujących świadomą refleksją sprawcy na temat niepoprawności i negatywnych skutków swojego postępowania oraz chęcią zaniechania podobnych zachowań w przyszłości. Planowanie interwencji powinno uwzględniać skalę poczynań sprawcy, tj. świadomość i celowość agresywnej aktywności, czas jej trwania oraz rozmiar wyrządzonej szkody.

---

[112] A. Borkowska, dz. cyt., s. 31.

Należy przeprowadzić rzeczową rozmowę, podczas której znaczący dorosły (np. rodzic, opiekun, nauczyciel) wyrazi brak akceptacji dla jakichkolwiek form przemocy i zażąda zaprzestania szkodliwego działania. Należy wspólnie omówić, jakie straty poniosła ofiara, ale także on sam, oraz poinformować o konsekwencjach, które zostaną wobec niego zastosowane lub jakie poniesie w wyniku ponownego incydentu. Rezultatem rozmowy powinno być zobowiązanie sprawcy do usunięcia krzywdzących materiałów i ustalenie możliwości naprawienia szkód odniesionych przez ofiarę cyberprzemocy oraz jej zadośćuczynienia[113]. Od tej pory aktywność sprawcy w cyberprzestrzeni oraz jego funkcjonowanie w przestrzeni realnej powinny podlegać monitoringowi, by w razie recydywy jego zachowań móc odpowiednio wcześnie zareagować.

Praca ze sprawcą

Ustalenie motywacji postępowania pozwala wytyczyć kierunek działań interwencyjnych wobec sprawcy cyberagresji. Jeśli sprawca świadomie przejawia niewłaściwą aktywność w Internecie, należy zidentyfikować przyczynę takiego zachowania. We wcześniejszej części tego rozdziału wśród możliwych powodów sprawstwa cyberagresji wymieniono wiele nieprawidłowości, m.in. brak empatii (zarówno poznawczej, jak i afektywnej), zaniżoną samoocenę, impulsywność i problem z kontrolą zachowań, a także nieodpowiednie relacje w grupie czy w rodzinie. Kompleksowa interwencja wobec cybersprawcy, a jednocześnie możliwa forma pomocy powinna zatem obejmować także starania ukierunkowane na treningi komunikacji interpersonalnej i zapośredniczonej, asertywności, empatii, konstruktywnych sposobów zaspokajania potrzeb i rozwiązywania problemów oraz radzenia sobie ze stresem czy skutkami zachowań agresywnych. Wyłączne karanie sprawcy, bez udzielonego mu wsparcia i pomocy psychologicznej, może okazać się krótkotrwałym odroczeniem jego dalszych działań o charakterze przemocy.

---

[113] Por. tamże, s. 27–29.

Cyberprzemoc to bardzo złożony problem współczesności. Rzeczywistość płynnie przechodząca z realności do wirtualności, dominujący w niej supermarket wartości, kultura upozorowania[114], kult wolności i przyjemności stały się swoistym placem zabaw, w którym pozostawiono dzieci bez opieki. Tu zabawa bardzo szybko może przerodzić się w konflikt, złość lub agresję, z którą młode pokolenie nie nauczyło się jeszcze sobie radzić. Internet, będący synonimem środowiska życia dzieci i młodzieży, to zatem bardzo przyjemne, ale i niebezpieczne narzędzie, którego na nowo muszą nauczyć się młodzi członkowie społeczeństwa przy mądrej i uczestniczącej obecności dorosłych.

---

[114] Koncepcję współczesności opisał Zbyszko Melosik, dz. cyt., s. 19–37.

Rozdział 2

Stalking

Wstęp

W art. 47 konstytucji, czytamy że: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym". Do polskiego Kodeksu karnego 6 czerwca 2011 r. została wprowadzona kategoria przestępstwa stalkingu (uporczywego nękania). Dorota Siemieniecka i Małgorzata Skibińska w tekście *Stalking and cyberstalking as a form of violence*[1] przytaczają dane statystyczne za Wydziałem Statystycznej Informacji Zarządczej Departamentu Strategii i Funduszy Europejskich Ministerstwa Sprawiedliwości. Dane te ukazują, że w 2015 r. na podstawie art. 190a, § 1 („Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności do lat 3") w Polsce ogółem osądzono 1163 osoby, w tym 972 mężczyzn i 191 kobiet. Kary te obejmowały: grzywnę samoistną, ograniczenie wolności, pozbawienie wolności, warunkowe umorzenie. Na podstawie § 2 („Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej") ogółem sąd skazał 69 osób, w tym 43 mężczyzn i 26 kobiet. Na podstawie § 3 („Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne

[1] D. Siemieniecka, M. Skibińska, *Stalking and cyberstalking as a form of violence*, „Society, Integration, Education" 2019, 3, s. 409–410.

życie, sprawca podlega karze pozbawienia wolności od roku do lat 10") osądzono 3 mężczyzn. W latach 2012–2015 na karę pozbawienia wolności za stalking skazano 255 osób (w poszczególnych latach 5–9%)[2].

Stalking – znaczenie pojęcia

Pojęcie stalkingu odnosi się do przestępstwa uporczywego nękania, przez które rozumie się świadome, celowe i często złośliwe prześladowanie drugiej osoby spowodowane chęcią odtworzenia lub nawiązania przez prześladowcę intymnego kontaktu ze swoją ofiarą. Celem sprawcy jest zdobycie kontroli nad ofiarą. Zróżnicowane działania, podejmowane przez stalkera, realnie zagrażają poczuciu bezpieczeństwa i wywołują u ofiary silny strach oraz poczucie zagrożenia[3]. Działania sprawcy można więc zaliczyć do zachowań o charakterze przemocy, które charakteryzuje powtarzalność, intencja skrzywdzenia drugiej osoby, nierównomierność sił, poczucie zagrożenia u ofiary. Według *Merriam-Webster Dictionary* angielska etymologia pojęcia jest związana z rzeczownikiem *stalk* oznaczającym „obsesyjne nękanie" (po raz pierwszy odnotowane w 1991 r.) lub czasownikiem o tym samym brzmieniu rozumianym jako „poruszanie się lub ściganie ukradkiem" i używanym często w żargonie myśliwskim w odniesieniu do potajemnego skradania się i osaczania zwierzyny.

Ofiary stalkingu

Charakter stalkingu rzeczywiście przyjmuje cechy polowania, w którym myśliwy-sprawca z zaangażowaniem tropi i osacza upragnioną zdobycz-ofiarę. Większość ofiar stalkingu stanowią kobiety (72–95%),

---

[2] B. Szopa, *Nowelizacja przepisów dot. nękania? Surowsze kary dla stalkerów?*, 2018, https://stalking.com.pl/2018/10/15/nowelizacja-przepisow-dot-nekania-surowsze-kary-dla-stalkerow/ (dostęp: 3.05.2020).

[3] K. Tomaszek, *Stalker – psychologiczna charakterystyka sprawców przestępstw „uporczywego nękania"*, „Studia z Psychologii w KUL" 2012, 18, s. 135–137, https://www.kul.pl/files/55/Stud_psych_18-2012_Tomaszek.pdf (dostęp: 3.05.2020).

większość sprawców (79–87%) to mężczyźni[4]. Badania ukazują, że 49% ofiar pozostawało w relacji ze stalkerem. Wskazuje się, że ofiarami stalkerów są zwykle byli partnerzy (30%) i osoby im znane z relacji zawodowych (23%) lub pracy (11%)[5].

Jarosław Groth[6] pisze, że „niemal 60% kobiet i 30% mężczyzn, stających się przedmiotem nękania, to byli partnerzy stalkerów, a większość ofiar (77% kobiet, 64% mężczyzn) znała wcześniej swych prześladowców"[7].

Wyniki badań realizowanych na zlecenie European Union Agency for Fundamental Rights i opublikowane w raporcie *Przemoc wobec kobiet. Badanie na poziomie Unii Europejskiej*, które objęło 42 tys. kobiet z 28 krajów UE (2012 r.)[8], ukazują, że „jedna na pięć kobiet doświadczyła nękania po ukończeniu 15. roku życia, przy czym 5% tych kobiet doświadczyło takiego nękania w okresie 12 miesięcy poprzedzających badanie"[9].

W UE-28 18% kobiet po ukończeniu 15. roku życia doświadczyło nękania (stalkingu)[10]. Jak można przeczytać w raporcie: „[…] około 14% kobiet otrzymywało wielokrotnie od tej samej osoby obraźliwe wiadomości, wiadomości lub telefony z groźbami, a 8% było śledzonych lub ktoś krążył wokół ich domu czy miejsca pracy. Spośród wszystkich badanych kobiet 3% doznało nękania, które wiązało się z wielokrotnym niszczeniem ich mienia przez tę samą osobę. Jedna na 10 kobiet (9%) doświadczyła nękania przez swego poprzedniego partnera"[11].

---

[4] P. Mullen i in., *A study of stalkers*, „The American Journal of Psychiatry" 1999, 156, s. 1244–1249, https://www.ncbi.nlm.nih.gov/pubmed/10450267 (dostęp: 3.05.2020); J. Groth, *Cyberstalking – perspektywa psychologiczna*, „Forum Oświatowe" 2010, 2(43), s. 91.

[5] P. Mullen i in., dz. cyt., s. 1244–1249; por. D. Siemieniecka, M. Skibińska, dz. cyt., s. 409–410.

[6] J. Groth, dz. cyt., s. 85–98.

[7] Tamże, s. 91; por. D. Siemieniecka, M. Skibińska, dz. cyt., s. 409–410.

[8] *Przemoc wobec kobiet. Badanie na poziomie Unii Europejskiej*, Urząd Publikacji Unii Europejskiej, Luksemburg 2014, http://europe-direct.kolobrzeg.eu/wp-content/uploads/2010/12/Przemoc-wobec-kobiet.pdf (dostęp: 3.05.2020).

[9] Tamże, s. 12.

[10] Tamże, s. 28; por. D. Siemieniecka, M. Skibińska, dz. cyt., s. 409–410.

[11] *Przemoc wobec kobiet…*, s. 28.

Za pomocą e-maili, wiadomości tekstowych lub Internetu było nękanych 4% kobiet w UE. Spośród badanych kobiet w wieku 18–29 lat (1,5 mln) 4% doświadczyło nękania za pomocą nowych technologii w okresie 12 miesięcy poprzedzających badania. Spośród wszystkich kobiet będących ofiarami nękania jedna na pięć (21%) była nękana przez ponad dwa lata, również jedna na pięć (23%) musiała zmienić numer telefonu lub adres e-mailowy wskutek nękania. Aż 74% nękanych kobiet nie zgłaszało tego faktu policji[12]. Dagmara Woźniakowska-Fajst w książce *Stalking i inne formy przemocy emocjonalnej. Studium kryminologiczne*[13] (2019) zwraca uwagę na istotne znaczenie płci sprawców i ofiar, pisze, że przewaga mężczyzn wśród sprawców „każe zastanowić się nad podłożem społecznym i kulturowym tych zachowań"[14]. Warto dodać, że badacze wskazują na istnienie grup podwyższonego ryzyka wiktymizacją (stalking, uporczywe nękanie). W tej grupie są nie tylko celebryci, ale też nauczyciele, lekarze i osoby pełniące funkcje publiczne[15].

Badania przeprowadzone na grupie 50 stalkerów wykazały, że „w 22 przypadkach sprawca dopuścił się w stosunku do ofiary brutalnej przemocy w postaci: spowodowania poważnych uszkodzeń ciała, poważnych ran, usiłowania zamordowania, doprowadzenia do śmierci"[16]. Niepokojące są również dane, które mówią, że „27% sprawców skazanych za brutalną przemoc było porzuconym kochankiem lub znajomym ofiary. W grupie stalkerów, którzy mieli intymną relację z ofiarą, aż w 70% przypadkach sprawca fizycznie znęcał się nad ofiarą […]", zaś „na 20 przypadków brutalnej agresji stosowanej przez stalkerów, aż w 1/4 przestępstw (5 przypadków) sprawca zabił swoją ofiarę, a w 3 przypadkach usiłował to zrobić"[17]. Dane te ukazują, z jak poważnym problemem zmagają się

---

[12] Tamże; por. D. Woźniakowska-Fajst, *Nękanie emocjonalne (stalking) w doświadczeniu studentów Uniwersytetu Warszawskiego*, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-6c12e957-42fc-4884-8eb0-382a78532e77 (dostęp: 3.05.2020).

[13] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej. Studium kryminologiczne*, Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 2019.

[14] Tamże, s. 15.

[15] Tamże, s. 235.

[16] K. Tomaszek, dz. cyt., s. 135–156, za: F.R. Farnham, D.J. James, P. Cantrell, *Association between violence, psychosis, and relationship to victim in stalkers*, „The Lancet" 2000, 355(9199), s. 151; por. D. Siemieniecka, M. Skibińska, dz. cyt., s. 409–410.

[17] K. Tomaszek, dz. cyt., s. 151–152.

osoby, które są ofiarami stalkingu. Aktywność stalkera nie tylko oddziałuje na ich samoocenę, poczucie bezpieczeństwa i sferę emocjonalną, ale może też zakończyć się tragicznie. Zachowanie stalkera przysparza ofierze cierpień na tle somatycznym i psychicznym. W literaturze zwraca się uwagę na wpływ działań stalkera na system wartości ofiary, ograniczenie wolności osobistej[18]. Wyjaśnia się, dlaczego ofiary nie informują o aktach przemocy (połowa ofiar nie zgłasza sprawy organom ścigania) – badacze doszukują się przyczyn w mechanizmach psychologicznych, takich jak zaprzeczenie, obwinianie siebie, przekonanie, że same sobie poradzą z sytuacją, oraz chęć ochrony najbliższych osób, brak wiary w to, że organy ścigania mogą pomóc. Często towarzyszy im uczucie wstydu[19]. W badaniach wyróżniono pięć rodzajów taktyk, jakie stosują ofiary nękania, są to: bezpośrednia konfrontacja polegająca na próbach rozmowy, odwet (grożenie sprawcy), unikanie prześladowcy, wzmacnianie siebie (psychoterapia, samoobrona, techniki relaksacyjne, religijność), szukanie pomocy na zewnątrz[20].

Warto wspomnieć, że jedynie 12% ofiar udało się rozwiązać problem nękania samodzielnie[21].

Wykorzystywanie przez stalkerów mediów społecznościowych, komunikatorów i narzędzi technologii informacyjnych w celu nękania, śledzenia i zastraszania ofiar wymaga przeciwdziałania temu zjawisku i współdziałania wielu instytucji i organizacji (np. policji, prokuratury oraz pomocy świadczonej przez pracowników Niebieskiej Linii).

Media w rękach sprawcy – cyberstalking

Rozwój telefonii komórkowej i Internetu pozwolił stalkerom zwiększyć szybkość i skalę swojego działania, dostarczając im dogodnych narzędzi nękania swoich ofiar. Ze względu na rosnące znaczenie i po-

---

[18] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej*…

[19] Tamże, s. 274.

[20] Tamże, s. 279, za: W.R Cupach, B.H. Spitzberg, *The dark side of relationship pursuit*, Lawrence Erlbaum Associates, Inc., Mahway 2004, s. 144–146.

[21] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej*…, s. 274.

wszechność odbioru mediów skutki działania prześladowcy są przez ofiary jeszcze bardziej odczuwane jako dotkliwe, bolesne i zagrażające ich bezpieczeństwu.

Przeniesienie aktów prześladowczych do przestrzeni wirtualnej określa się mianem cyberstalkingu. Analogicznie do przedstawionych wcześniej definicji stalkingu cyberstalking „pojmowany jest jako uporczywe i niesprowokowane przez ofiarę zachowanie, obejmujące wielokrotne groźby i zachowania nękające ofiarę, mimo jej cierpienia i próśb o zaprzestanie, przy użyciu narzędzi komunikacji i informacji, skutkiem którego ofiara obawia się o swoje bezpieczeństwo”[22].

Media mogą być zarówno dobrodziejstwem, jak i przekleństwem. Popularny portal społecznościowy Facebook ma już ponad 2,2 mld użytkowników. Stanowi on ogromną bazę danych o osobach zawierającą zdjęcia, materiały filmowe, GIF-y animowane, wiadomości tekstowe. Sami użytkownicy decydują o tym, jakie treści zostają zamieszczone na portalu i jaką rangę dostępu im przypisują. Zwraca się uwagę, że 5–15% kont na Facebooku (stanowiących od 100 do 300 mln kont) to konta fałszywe[23]. Są one często wykorzystywane przez przestępców tworzących nieprawdziwe tożsamości lub podszywających się pod istniejące realnie osoby. Mamy więc do czynienia z zafałszowaniem tożsamości i niepewnością dotyczącą innych użytkowników sieci. Jak podają dane FB, 175 mln użytkowników korzysta w reakcjach z opcji Super, codziennie użytkownicy oznaczają informacje 600 mln lajków, zaś 750 mln internautów zawiera nowe znajomości[24].

Bywa, że narzędzia, takie jak Facebook, komunikatory czy też narzędzia określające miejsce pobytu, mogą pozwalać na kontrolowanie i obserwowanie aktywności innych osób (czasu logowania, aktywności, odbioru wysyłanych wiadomości). Możliwości te są często wykorzystywane przez cyberstalkerów. Dagmara Woźniakowska-Fajst przytacza za Parry Aftab formy nękania, są to: „[…] napastowanie, które odbywa

---

[22] J. Groth, dz. cyt., s. 87.

[23] T. Brusik, *Rysuję fejsbuki*, https://rysujefejsbuki.pl/rysunek/2-mld-uzytkownikow-facebooka/ (dostęp: 3.05.2020).

[24] *Facebook z dwoma miliardami użytkowników miesięcznie*, https://www.wirtualnemedia.pl/artykul/ilu-uzytkownikow-ma-facebook-dwa-miliardy# (dostęp: 3.05.2020).

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"[25].

Cyberstalkerzy nękają swoje ofiary przez rozpowszechnianie w Internecie osobistych lub intymnych zdjęć ofiary, danych personalnych (miejsca zamieszkania, pełnionej funkcji, miejsca pracy), nieprawdziwych informacji, nagrań rozmów, relacji intymnych (zarejestrowanych bez jej zgody i wiedzy), podszywanie się pod ofiarę (na czatach, listach dyskusyjnych) i korzystanie z jej kont (poczty elektronicznej, komunikatorów), instalowanie oprogramowania szpiegującego, wysyłanie wirusów, niszczenie sprzętu komputerowego[26]. Działania cyberstalkerów w przestrzeni portali społecznościowych mogą dodatkowo być potęgowane przez hejterów, którzy zamieszczają obraźliwe komentarze. Stalkerzy często podszywają się pod osobę prześladowaną.

Warto tu przywołać badania realizowane przez Dagmarę Woźniakowską-Fajst na próbie 358 sprawców. Ich wyniki ukazują, że prawie 67% ofiar otrzymywało niechciane wiadomości w formie elektronicznej, 66% było nękanych przez telefon komórkowy, 5,4% stalkerów publikowało w Internecie informacje o swojej ofierze i 4,8% publikowało komentarze, 4,3% zamieszczało zaś w sieci zdjęcia ofiary[27].

Wszystkie cechy zachowań cyberstalkerów mieszczą się w definicji zaproponowanej przez Justynę Skarżyńską-Sernaglię, która określa je jako „powtarzające się uporczywe nękanie poprzez rozmaite formy naruszenia wolności osobistej i prywatności drugiej osoby, wywołujące u prześladowanego niepokój, skrępowanie, dyskomfort fizyczny i psy-

---

[25] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej*…, s. 52, za: P. Aftab, *Internet a dzieci. Uzależnienia i inne niebezpieczeństwa*, tłum. B. Nicewicz, Prószyński i S-ka, Warszawa 2003, s. 140–141.

[26] J. Skarżyńska-Sernaglia, *Stalking: od miłości do zbrodni – nowe wyzwanie dla psychologii, kryminologii i zespołów interdyscyplinarnych przeciwdziałających przemocy*, Львівського державного університету внутрішніх справ НАУКОВИЙ ВІСНИК 1/2009 (Lviv State University of Internal Affairs, Collection of scientific works), s. 1–15, http://www2.lvduvs.edu.ua/documents_pdf/visnyky/nvsp/01_2009/09ssjipp.pdf (dostęp: 3.05.2020); por. D. Siemieniecka, M. Skibińska, dz. cyt., s. 409–410.

[27] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej*…, s. 53.

chiczny, szereg dolegliwości zdrowotnych, fizycznych i psychicznych, trudności w kontaktach interpersonalnych i uzasadnione obawy o własne bezpieczeństwo”[28]. Dostrzega się związki stalkingu z przemocą emocjonalną, nękaniem, obsesyjnym pożądaniem, patologiczną miłością, prześladowaniem. Celem stalkera jest przejęcie kontroli nad ofiarą przez zastraszanie, szantaż, prześladowanie, co często prowadzi do izolowania osoby od jej otoczenia społecznego (przez uczucie wstydu, sprawienie najbliższym zawodu). Sytuacje te mają w ofierze wzbudzać lęk, bezsilność i poczucie osamotnienia[29].

Motywami działania sprawcy są również: odzyskanie kontroli nad ofiarą, sprawowanie władzy, zyski psychologiczne, zemsta za krzywdy. Stalking stanowi formę przemocy emocjonalnej[30]. Zdaniem Dagmary Woźniakowskiej-Fajst „stalking, mobbing, bullying, jak i molestowanie seksualne mają wiele wspólnego. Wszystkie one łączą się z nękaniem, dokuczaniem innym osobom w bardziej skrajnej formie przyjmują postać prześladowania”[31].

Cyberstalker może publikować lub wysyłać za pośrednictwem sieci treści nielegalne lub szkodliwe. Jolanta Kosińska pisze, że „treści nielegalne to materiały, których umieszczanie w sieci stanowi czyn zabroniony przez prawo karne. Treściami szkodliwymi są materiały, których umieszczanie lub rozsyłanie w sieci nie jest zabronione przez prawo karne, lecz mogą wywołać szkody materialne lub niematerialne, zwłaszcza w zakresie dóbr osobistych”[32]. Publikowanie takich materiałów na FB może być zablokowane przez osobę poszkodowaną przez zgłoszenie posta, zdjęcia lub filmu (wybierając opcję ˅ w prawym górnym rogu posta; kliknięcie „Zgłoś post” lub „Zgłoś zdjęcie”). Można również wy-

---

[28] J. Skarżyńska-Sernaglia, *Stalking: od miłości do zbrodni…*, s. 1–15; por. D. Siemieniecka, M. Skibińska, dz. cyt., s. 409–410.

[29] J. Pielichowski, *Kompendium prawno-psychologiczne z zakresu stalkingu*, „Wiedza Prawnicza” 2013, 6(201), s. 30–31, http://www.wiedzaprawnicza.pl/teksty/6-2013/6-2013.pdf (dostęp: 3.05.2020), za: B. Hołyst, *Kryminologia*, Lexis Nexis, Warszawa 2004, s. 211.

[30] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej…*, s. 35.

[31] Tamże.

[32] J. Kosińska, *Prawnokarna problematyka stalkingu*, „Prokuratura i Prawo” 2008, 10, s. 34.

korzystać w tym celu inną możliwość: powiększyć zdjęcie lub film, ustawić kursor na zdjęciu lub filmie i kliknąć pozycję „Opcje" w prawym dolnym rogu, następnie zaznaczyć opcję „Zgłoś zdjęcie" w przypadku zdjęć lub „Zgłoś film" w przypadku filmów (pomoc FB). W odniesieniu do komentarzy należy wybrać opcje , „Ukryj to", następnie „Zgłoś". FB oferuje również możliwość przesłania linków. W razie niechcianych połączeń każdy smartfon ma możliwości blokowania numerów przez opcje: „Blokuj kontakt" lub „Dodaj do czarnej listy". Istnieje możliwość korzystania z następujących aplikacji: Odebrać telefon?, Calls Blacklist, Safest Call Blocker, SMS Blocker, Truecaller, BlackList:caller ID&blocker, Call Blocker, Hiya Caller ID and Block. Niektórzy operatorzy sieci komórkowych udostępniają opcję blokowania połączeń anonimowych, innym rozwiązaniem jest filtrowanie treści oraz ustalenie ISP sprawcy i jego blokowanie przez dostawcę usług internetowych, lub opcję filtrowania spamu przez blokowanie adresów IP nadawców wiadomości (konfiguracja ustawień antyspamowych). Jarosław Groth w tekście *Cyberstalking – perspektywa psychologiczna* wymienia formy działania cyberstalkerów, do których zaliczył: nękanie za pośrednictwem serwisów czatowych, przeprowadzanie ataków na komputer ofiary (przesyłanie: wirusów, rootkitów, keyloggerów, programów szpiegujących, trojanów, backdoorów), poszukiwanie informacji o ofierze w Internecie, publikowanie w Internecie informacji na temat osoby prześladowanej, rozpowszechnianie za pośrednictwem Internetu fałszywych informacji, zamawianie towarów lub usług w imieniu ofiary, kradzież tożsamości, skłanianie innych do dręczenia ofiary, *stalking-by-proxy*.

Cechy i charakterystyka psychologiczna stalkera

W literaturze odnajdujemy charakterystykę sprawców przestępstw „uporczywego nękania". Stalkerami są najczęściej mężczyźni w wieku 35–40 lat, to osoby samotne, niepozostające w związku małżeńskim lub innym[33]. Stalkerzy w większości to ludzie wykształceni, o wyższym

[33] K. Tomaszek, dz. cyt.; S. Forward, C. Buck, *Toksyczne namiętności*, tłum. K. Drozdowski, Jacek Santorski & CO, Warszawa 1997; R.D. Hare, *Psychopathy: A clin-*

ilorazie inteligencji, często bezrobotni, bez własnego mieszkania, nieusamodzielnieni. Wielu z nich ma przeszłość kryminalną, już wcześniej mogli być sprawcami przemocy domowej. Działanie stalkera jest wywołane najczęściej zerwaniem przez ofiarę intymnej relacji i wyzwala u sprawcy zachowania o cechach obsesyjnej miłości[34]. Początkowo przez swoje działania (prezenty, aranżowanie spotkań) stalker usiłuje odzyskać utraconą relację, jednak kierunek jego działań ulega zmianie, gdy ofiara nadal odmawia powrotu do poprzedniej sytuacji[35]. Jak pisze Katarzyna Tomaszek, „początkowo pozytywne uczucia, jakie żywi sprawca, ulegają przeobrażeniu. Nadal w centrum jego uwagi znajduje się ofiara, ale zaczyna on obwiniać ją o swe porażki. Dominującymi stają się wówczas pragnienie zemsty i wyrządzenia krzywdy ofierze"[36]. Celem stalkera jest ukaranie ofiary przez niszczenie jej życia osobistego i zawodowego. Zwraca się uwagę, że u podstaw jego zachowania leży lęk przed samotnością i pragnienie bycia kochanym, zaś utracona relacja „ulega wyidealizowaniu i nabiera nierzadko wręcz mistycznego znaczenia"[37]. Ofiara i relacja z nią jest przez niego idealizowana i postrzegana jako niezbędna do życia przy równoczesnym jej uprzedmiotowieniu. Stalker dąży do „stworzenia, odbudowania czy narzucenia związku innej osobie, która wyraziła brak zainteresowania"[38]. Definicje wskazują na następujące cechy stalkingu: śledzenie, przebywanie w pobliżu osoby, drażnienie, długotrwałe prześladowanie, napaści w formie agresji słownej i fizycznej[39].

Motywem działań stalkera jest chęć powrotu do utraconego związku i/lub zazdrość o potencjalnego partnera ofiary. Zachowania stalkerów wkraczają w obszar naruszania dóbr publicznych (np. publikują w sieci oszczerstwa, które mają na celu zniszczenie reputacji ofiary, tre-

ical construct whose time has come, „Criminal Justice Behavior" 1996, 23, s. 25–54; K.S Douglas, D.G. Dutton, *Assessing the link between stalking and domestic violence*, „Aggression and Violent Behavior" 2001, 6, s. 519–546; J. Skarżyńska-Sernaglia, *Ciemna strona relacji interpersonalnych*, www.stalking.it (dostęp: 3.01.2019).

[34] K. Tomaszek, dz. cyt.

[35] Tamże.

[36] Tamże, s. 147–148.

[37] Tamże.

[38] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej*…, s. 38, za: P. Mullen i in., dz. cyt., s. 1244–1249.

[39] Por. D. Siemieniecka, M. Skibińska, dz. cyt., s. 409–410.

ści zamieszczane w Internecie odnoszą się do osobistych lub intymnych zdjęć, fragmentów korespondencji lub seksualnych opisów)[40]. Podkreśla się, że stalkerów cechują trudności w relacjach i problemy z wchodzeniem w związki interpersonalne i intymne, niski poziom empatii[41]. Osoby te nie biorą pod uwagę potrzeb innych osób i ich prawa do decydowania o własnym życiu i szczęściu. Sprawcy często postrzegają siebie jako ofiarę, podkreślają własne prawa do decydowania o relacji. Duży procent sprawców (70–80%) charakteryzuje się osobowością narcystyczną, antyspołeczną, nieprzystosowaniem społecznym, egoizmem i egocentryzmem[42]. U 30% badanych stalkerów (N = 145) stwierdzono zaburzenia o charakterze urojeniowym (co dotyczyło grupy poszukującej intymności), wśród grup odrzuconych dominowali zaś ci z zaburzeniami osobowości[43]. Obraz rzeczywistości stalkerów jest zniekształcony, nieprawidłowo percypują oni komunikaty innych osób o tym, że nie chcą utrzymywać znajomości. Zwraca się uwagę na wysoki poziom impulsywności i nieadekwatną reaktywność do bodźców (bywa, że osoby te pod wpływem sytuacji mogą stać się sprawcami brutalnych aktów agresji). Osoby te cechuje niskie poczucie własnej wartości, bywają one również sfrustrowane swoim życiem. Badania wykazują, że ofiary przed pojawieniem się stalkingu doświadczały ze strony sprawcy: poniżania, kontrolowania, zabraniania bądź uniemożliwiania spotkań z rodziną i znajomymi, niedowartościowania relacji, próby wpływania i kontroli na ich życie, prowokowania kłótni i sprzeczek, wybuchów złości, zastraszania osoby niechcącej podporządkować się ich woli[44].

W literaturze[45] wyróżnia się pięć typów stalkerów, są to: a) osoby odrzucone, które cechuje chęć zemsty za zwolnienie, rozpad związku,

---

[40] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej*…, s. 40.

[41] J. Skarżyńska-Sernaglia, *Stalking: od miłości do zbrodni*…

[42] K. Tomaszek, dz. cyt., s. 147, za: J. Skarżyńska-Sernaglia, *Ciemna strona relacji interpersonalnych*…

[43] P. Mullen i in., dz. cyt., s. 1244–1249.

[44] J. Pielichowski, dz. cyt., s. 30–31, za: S. Walby, J. Allen, *Domestic violence, sexual assault and stalking: Findings from the British Crime Survey*, Home Office Research, 2004, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.477.2558&rep=rep1&type=pdf (dostęp: 3.05.2020).

[45] J. Pielichowski, dz. cyt., s. 30–31, za: P. Mullen i in., dz. cyt., s. 1246.

dążące do powrotu do wcześniejszej relacji; b) osoby urażone, które charakteryzuje poczucie krzywdy, stosują szantaż i zastraszanie; c) osoby poszukujące intymności – kieruje nimi przeświadczenie, że partner jest im przeznaczony; d) niewłaściwi zalotnicy – osoby charakteryzujące się trudnościami w nawiązywaniu relacji, skłonne do obsesji; e) stalkerzy drapieżni prześladowcy – szpiegujący ofiary, planujący atak na tle seksualnym. Wyniki badań prowadzone przez Paula Mullena, Michele Pathé, Rosemary Purcell, Geoffreya Stuarta[46] ukazują, że „63% prześladowców (N = 84/145) spełniło swoje groźby, a 36% ich aktywności miało charakter napaści. Zagrożenia i uszkodzenia mienia występowały częściej u urażonych prześladowców, ale w grupie odrzuconych i drapieżnych prześladowców zanotowano więcej ataków na ofiary"[47]. Większe ryzyko podejmowania działań stalkerów zanotowano w grupie, która już wcześniej była skazana. Inne rozróżnienie przywołuje Jarosław Groth[48], wymieniając:

- prześladowców-erotomanów przekonanych, że ofiara darzy ich uczuciem (większość tej grupy stanowią kobiety),
- osoby obsesyjne na punkcie miłości (zdają sobie sprawę, że ofiara nie odwzajemnia ich uczuć – większość tej grupy to mężczyźni),
- sprawcy obsesyjni – byli partnerzy lub osoby pozostające w innych relacjach z ofiarą (są w tej grupie zarówno kobiety, jak i mężczyźni)[49].

Prześladowców z obsesją miłości za względu na stopień znajomości i zażyłości ze swoją ofiarą można podzielić na trzy kategorie: a) bliskich znajomych, partnerów lub dawnych partnerów – sprawca i ofiara utrzymywali formalne lub okazjonalne kontakty, ich relacje miały charakter towarzyski lub seksualny; b) znajomych – znajomość sprawcy i ofiary ma charakter przypadkowy, okazjonalny, czasem formalny, mogli być part-

---

[46] P. Mullen i in., dz. cyt., s. 1244–1249, https://ajp.psychiatryonline.org/doi/pdf/10.1176/ajp.156.8.1244 (dostęp: 3.05.2020).

[47] Tamże.

[48] J. Groth, dz. cyt., s. 92, za: M.A Zona, K.K Sharma, J. Lane, *A comparative study of erotomanic and obsessional subjects in a forensic sample*, „Journal of Forensic Sciences" 07/1993, 38(4), s. 894–903.

[49] J. Groth, dz. cyt., s. 92.

nerami seksualnymi; c) obcych – prześladowca nie zna osobiście ofiary, tego rodzaju stalkerzy prześladują często osoby popularne w mediach[50]. Formy nękania ofiary przybierają postać[51]: częstych telefonów, wysyłania niezliczonej liczby wiadomości (e-mail, SMS), przesyłanie niechcianych prezentów, paczek, natrętnych propozycji spotkań, wyjazdów, propozycji seksualnych, śledzenia ofiary, nachodzenia w miejscu pracy czy miejscu zamieszkania, podsłuchiwania, nagrywania ofiary (rozmów i wideo), zaczepiania w miejscach publicznych, szantażu emocjonalnego (np. próby samobójcze sprawcy, groźby ujawnienia intymnych zdjęć, materiałów) i wszelkich aktów agresji i wandalizmu (niszczenie przedmiotów, krzywdzenie zwierząt należących do ofiary). Zdarza się, że osoby te podszywają się pod ofiarę, zakładając konta na serwisach społecznościowych lub portalach erotycznych, podając jej dane osobowe, wysyłając e-maile w jej imieniu. Dokonują również zakupów i zamawiają przesyłki na jej koszt. Rozpowszechniają fałszywe informacje, niekiedy grożą założeniem spraw sądowych, ukazując siebie jako osobę pokrzywdzoną. Kierują wobec ofiary groźby śmierci, uszkodzenia ciała, ponadto stosują przemoc słowną: wulgaryzmy, obelgi i pomówienia. Pomówienia zamieszczone w sieci mogą być opatrzone kompromitującymi zdjęciami[52]. W przypadku publikacji treści w sieci zwykle zamieszczają treści osobiste, intymne zdjęcia, nagrywane rozmowy lub ich fragmenty, często informacje te opatrują wyznaniami miłości, opisami aktów seksualnych, podają intymne fakty z życia (wraz z danymi osoby, jej miejscem pracy, jej stanowiskiem, adresem). W wiadomościach lub postach można odnaleźć wulgarne określenia, wyzwiska. Treści SMS-ów, które mają skłonić ofiarę do kontaktu, przybierają charakter szantażu związanego np. z rozesłaniem informacji do współpracowników, groźbą wizyty oprawcy w miejscu pracy (często

---

[50] National Institute of Justice Research Report 1998, *Domestic violence and stalking: The third annual report to Congress under the Violence against Women Act*, US Department of Justice, Office of Justice Programs, s. 2, https://babel.hathitrust.org/cgi/pt?id=osu.32437121067694;view=1up;seq=12 (dostęp: 3.05.2020).

[51] D. Woźniakowska-Fajst, *Nękanie emocjonalne (stalking)*…

[52] J. Skarżyńska-Sernaglia, *Stalking w Polsce – występowanie i charakterystyka zjawiska*, http://psychologia.net.pl/artykul.php?level=415 (dostęp: 3.05.2020); K. Tomaszek, dz. cyt., s. 140–150; D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej*…

oprawca dodaje np., że nie będzie to miła wizyta), stawianiem warunków zaprzestania działalności, jeśli ofiara skontaktuje się i spełni wymagane przez stalkera warunki. Stalker może również formułować groźby śmierci lub okaleczenia ofiary. Niebezpieczeństwo polega na tym, że osoby te posiadają lub mogą posiadać ostre przedmioty zagrażające ofierze (np. żyletki, noże)[53]. Warto podkreślić, że stalking jest często powiązany z cyberstalkingiem. Sprawcy korzystają z różnych strategii i sposobów nękania swoich ofiar zarówno w świecie realnym, jak i wirtualnym[54]. Wart przywołania jest fragment opisu działania sprawcy wobec pokrzywdzonej zamieszczony w aktach sprawy sądowej (stanowiącej materiał badawczy zaprezentowany w książce Dagmary Woźniakowskiej-Fajst)[55]:

> Sprawca przez sześć lat, od 2008 roku, uporczywie nękał pokrzywdzoną poprzez wielokrotne rozsyłanie zniesławiających, znieważających ją, zawierających oszczerstwa listów tradycyjnych, wiadomości tekstowych za pośrednictwem poczty internetowej i portali społecznościowych, zarówno na adres pokrzywdzonej, jak i na adresy członków jej rodziny i znajomych. Rozsyłał także listy do organów państwowych zawiadamiające o możliwości popełnienia przez pokrzywdzoną czynów zabronionych lub o posiadaniu przez pokrzywdzoną wiedzy na temat różnych przestępstw. Prześladowca groził swojej ofierze wyrządzeniem jej krzywdy, pozbawieniem życia oraz wywieszeniem billboardów na terenie Trójmiasta z obraźliwą treścią i jej zdjęciem. Elementem cyberprzemocy w działaniach sprawcy było zamieszczanie bez zgody pokrzywdzonej w sieci internetowej jej zdjęć, filmów z jej udziałem, ogłoszeń dotyczących oferowanych rzekomo przez pokrzywdzoną usług lub wysyłanie wiadomości do różnych osób znających pokrzywdzoną, dotyczących chęci zakupu informacji z jej życia prywatnego. Stalker dopuścił się także kradzieży tożsamości swojej ofiary, podszywając się pod nią w celu wyrządzenia jej szkody oso-

---

[53] J. Skarżyńska-Sernaglia, *Stalking w Polsce…*

[54] J. Groth, dz. cyt., s. 93, za: J.R. Meloy (ed.), *Forensic perspectives*, Academic Press, London 1998, s. 11 i W.R. Cupach, B.H. Spitzberg, dz. cyt., s. 80.

[55] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej…*, s. 57.

bistej. Wszystkie te złożone, trwające wiele lat, działania doprowadziły do próby targnięcia się pokrzywdzonej na życie[56].

Badania ukazują, że stalkerzy stanowią grupę bardzo zróżnicowaną, wśród nich są osoby cechujące się zaburzeniami psychotycznymi, schizoafektywnymi, chorobami psychicznymi, zaburzeniami osobowości (osobowość niedojrzała, borderline, paranoidalna, schizoidalna, depresyjna, zależna)[57].

W erze mediów cyfrowych i powszechnego dostępu do Internetu zjawisko stalkingu podlega rozszerzeniu, zarówno ze względu na szybkość, zakres i skalę działań prześladowczych, jak i rozmiar szkód wyrządzanych ofierze. Technologie komunikacyjno-informacyjne w rękach sprawcy stają się niebezpiecznym i często łatwo dostępnym narzędziem nękania, prześladowania i torturowania, których skutków niejednokrotnie nie sposób kontrolować i niwelować. Niepokojące jest to, że często ufne zachowania informacyjne użytkowników mediów dostarczają stalkerom niebezpiecznej broni przeciw wybranym ofiarom[58]. W dość prosty sposób sprawca gromadzi informacje dotyczące swojej ofiary, jej życia osobistego i zawodowego, poznając jej zwyczaje, upodobania i słabości. Zyskuje także materiały wizualne w postaci zdjęć, filmów, które w przyszłości wykorzysta przeciwko niej.

Stalking i cyberstalking – przeciwdziałanie

Wobec gwałtownego rozwoju i popularności mediów społecznościowych nie sposób całkowicie uniknąć ryzyka stalkingu, jednak możliwe jest niwelowanie jego skali i skutków. Skutecznym sposobem przeciwdziałania temu zjawisku jest szeroko pojęta edukacja, obejmująca

[56] Tamże, s. 194.

[57] K. Tomaszek, dz. cyt., s.135–156; I. Nowicka, *Zjawisko stalkingu w kontekście resocjalizacji penitencjarnej kilka uwag*, „Humanistyczne Zeszyty Naukowe – Prawa Człowieka" 2017, 1(20), s. 165–175, http://www.humanrights.com.pl/pdf/Tom20/10.%20Izabela%20NOWICKA%20-%20Zjawisko%20stalkingu%20w%20kontek%C5%9Bcie%20resocjalizacji%20penitencjarnej.%20Kilka%20uwag.pdf (dostęp: 3.05.2020).

[58] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej…*

różne grupy społeczne i wiekowe. Strategię edukacyjną w profilaktyce zagrożeń cyberprzemocą promuje wielu naukowców z kraju i zagranicy[59]. Uzasadnieniem działań edukacyjnych w kontekście profilaktyki zagrożeń przemocy i cyberprzemocy jest potrzeba osobistej ochrony potencjalnych ofiar przestępstw o podłożu przemocowym oraz redukcja skali tychże przestępstw. Analizując przytoczone badania, można wnioskować, że ofiary przemocy cechuje pasywna postawa myślenia i działania oraz że nie mają wystarczających kompetencji zwalczania przemocy i reagowania na nią. Istnieje zatem konieczność podjęcia działań edukacyjnych ukierunkowanych na budowanie poczucia własnej kontroli nad zdarzeniami, opartej na wiedzy i świadomości zagrożeń, ich profilaktyce i możliwym postępowaniu w sytuacji konkretnego zagrożenia. Nabyte kompetencje zmniejszają ryzyko wiktymizacji. Bezsilność i brak działania ofiary umacnia sprawcę w poczuciu bezkarności i agresywnym zachowaniu.

Relatywnie do różnych poziomów wpływu cyberprzemocy edukacja na rzecz przeciwdziałania i skutków przemocy powinna odbywać się w trzech wymiarach:

- indywidualnym – dla poprawnego funkcjonowania psychologicznego i zdrowotnego uwikłanych w proceder jednostek[60];

---

[59] Np. K. Knol, J. Pyżalski, *Mobbing elektroniczny: analiza rozwiązań profilaktycznych i interwencyjnych*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2011, 1(34); L. Cox, B. Speziale, *Survivors of stalking: Their voices and lived experiences*, „Affilia" 2009, 24(1); C. Southworth i in., *Intimate partner violence, technology, and stalking*, „Violence Against Women" 2007, 13(8); L. Cattaneo, S. Cho, S. Botuck, *Describing intimate partner stalking over time: An effort to inform victim-ventered service provision*, „Journal of Interpersonal Violence" 2011, 26(17); S.L. Miller, N.L. Smolter, *"Paper abuse": When all else fails, batterers use procedural stalking*, „Violence Against Women" 2011, 17(5), za: D. Lindberg, *Prevention of cyberstalking: A review of the literature*, Criminology and Criminal Justice Senior Capstone Project, Portland State University 2012.

[60] A. Fletcher i in., *Brief report: Cyberbullying perpetration and its associations with socio-demographics, aggressive behaviour at school, and mental health outcomes*, „Journal of Adolescence" 2014, 37(8), s. 1393–1398, za: J. Barlińska, D. Lalak, A. Szuster, *Jak skutecznie ograniczyć cyberprzemoc rówieśniczą? – o efektywności metod aktywizujących kompetencje społeczne ze szczególnym uwzględnieniem empatii*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2018, 17(1), http://dzieckokrzywdzone.fdds.pl/index.php/DK/article/view/659/516 (dostęp: 3.05.2020),

- społecznym – dla minimalizacji ryzyka przemocy interpersonalnej prowadzącej do pogorszenia relacji społecznych[61];
- globalnym – jako wyzwanie dla szkół i otoczenia społecznego[62].

Każdy z wymienionych wyżej wymiarów powinien obejmować działania na rzecz rozwoju wiedzy, umiejętności i postaw wszystkich obywateli, bez względu na wiek i płeć. Zagrożenie przemocą potencjalnie dotyczy wszystkich członków grup społecznych, poczynając od przemocy domowej, po przemoc rówieśniczą, w miejscu pracy, sąsiedzką itp., na przemocy elektronicznej kończąc (a czasem zaczynając).

Jak zaznaczono we wstępie, liczba wyroków skazujących za przestępstwo uporczywego nękania w Polsce przekroczyła w 2015 r. 1 tys. i systematycznie wzrasta z roku na rok (od 2011 do 2014 r. zwiększyła się 22-krotnie)[63]. Należy więc dołożyć wszelkich starań, by ograniczyć prawdopodobieństwo doświadczenia uporczywego nękania. Coraz częściej media elektroniczne służą stalkerowi jako źródło informacji o ofierze i narzędzie jej prześladowania. Trzeba więc zadbać o bezpieczeństwo w przestrzeni medialnej.

Korzystając z usług internetowych, trzeba być rozważnym i pamiętać, że nie każdy jest tak samo uczciwy i miły, jak my sami. Należy chronić informacje na swój temat, by nie posłużyły prześladowcy do budowania strategii nękania dzięki dostępowi do danych teleadresowych, opisowi zwyczajów i zainteresowań, oraz by uniemożliwić prze-

---

[61] J. Barlińska, A. Szuster, *Cyberprzemoc. O zagrożeniach i szansach na ograniczenie zjawiska wśród adolescentów*, Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 2004; J. Pyżalski, *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Oficyna Wydawnicza IMPULS, Kraków 2012, za: J. Barlińska, D. Lalak, A. Szuster, dz. cyt.

[62] R.M. Kowalski i in., *Bullying in the digital age. A critical review and meta-analysis of cyberbullying research among youth*, „Psychological Bulletin" 2014, 140, s. 1073–1137; I. Zych, R. Ortega-Ruiz, R. DelRey, *Systematic review of theoretical studies on bullying and cyberbullying: Facts, knowledge, prevention and intervention*, „Aggressive Violent Behaviour" 2015, 23, s. 1–21, za: J. Barlińska, D. Lalak, A. Szuster, dz. cyt.

[63] B. Szopa, *Stalking w Polsce – trochę statystyki*, 2015, https://stalking.com.pl/2015/09/29/stalking-w-polsce-statystyka/ (dostęp: 3.05.2020).

jęcie tożsamości i wykonywanie pewnych działań i czynności w naszym imieniu. Dlatego niezbędne jest zadbanie o to, by[64]:

- każdy komputer miał aktywny program antywirusowy i włączoną zaporę sieciową, należy zabezpieczyć domową sieć wi-fi;
- aktualizować system operacyjny, przeglądarki internetowe oraz oprogramowanie używane na urządzeniu;
- korzystać z zaufanych, szyfrowanych stron internetowych (https://);
- po skończonej pracy wylogowywać się z kont profilowych i wybranych usług; samodzielnie ustalać złożone hasła, które co pewien czas należy zmieniać – niedopuszczalne jest używanie tego samego hasła do kilku kont oraz udostępnianie ich osobom trzecim czy zapisywanie w łatwo dostępnych miejscach;
- korzystanie z otwartych sieci wi-fi ograniczyć do minimum, a używając ich, nie powinno się dzielić informacjami osobistymi, wrażliwymi danymi, logować się do kont bankowych, mediów społecznościowych czy poczty elektronicznej; nie należy również otwierać podejrzanych załączników dołączonych do wiadomości pocztowej ani odpowiadać na takie wiadomości;
- dokonać przeglądu informacji dostępnych w Internecie na swój temat, pozwalających pozyskać prywatne dane teleadresowe oraz ujawniające rozkład dnia i zwyczaje – trzeba niezwłocznie je usunąć.

Dodatkowo, korzystając z portali społecznościowych, warto usunąć zdjęcia i informacje o sobie, starać się nie publikować nowych informacji lub nie zamieszczać ich w ogólnym dostępie, stworzyć bezpieczne konto, nie przyjmować do niego nieznanych kont i użytkowników, zmienić hasła dostępu do własnego profilu, skrzynki e-mail. Istotne jest zawiadomienie o nękaniu służb (policję, prokuraturę)[65]. Z 360 sprawców 130 (42%) zaprzestało lub ograniczyło swoje zacho-

---

[64] Por. K. Kupczyk, *Stalking w Polsce jest coraz częstszy. Czym jest cyberstalking i jak mu zapobiegać?*, 2016, Spy Shop blog, https://www.spyshop.pl/blog/infografiki-stalking-w-polsce-jest-coraz-czestszy-czym-jest-cyberstalking-i-jak-mu-zapobiegac/ (dostęp: 3.05.2020).

[65] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej…*

wania w stosunku do ofiary po zgłoszeniu sprawy na policję. Badania ujawniają, że „nie każdy typ sprawcy w równym stopniu daje się w ten sposób zatrzymać. Najczęściej odstąpieniem od stalkingu reagowali sprawcy w typie nieudolnego admiratora, najrzadziej zaś – poszukiwacze bliskości”[66]. Badania ukazały również, że wydany przez prokuratora zakaz zbliżania się w 4–7% przypadków jest łamany w pół roku po jego wydaniu; 80% sprawców nie przestrzega zakazu zbliżania się do ofiary (i kontaktu z nią)[67].

Każdy użytkownik mediów społecznościowych powinien dokonać rewizji treści, jakie udostępnia w Internecie, by zadbać o bezpieczeństwo swoje i najbliższych oraz chronić swoją tożsamość[68]. Warto zwrócić uwagę na następujące zalecenia:

- ustawienia prywatności – należy upewnić się, że dostęp do upowszechnianych informacji ma wąskie grono zaufanych osób; jeśli pozwala się na dostęp znajomym znajomych – traci się kontrolę nad upublicznianymi danymi;
- im mniej, tym lepiej – nie należy dzielić się szczegółami z życia prywatnego, informować szczegółowo o planach i zwyczajach, nie powinno się zamieszczać zdjęć prezentujących twarze oraz wnętrza i okolice domu;
- trzeba sprawdzić ustawienia profilu w mediach społecznościowych, by nie było możliwe ustalenie harmonogramu dnia (np. Facebook – informacje o ulubionych miejscach, zainteresowaniach, Twitter – informacje o aktualnej lokalizacji);
- nie powinno się dołączać do grona znajomych osób nowo poznanych lub poznanych tylko w Internecie.

Nauczyciele, rodzice oraz dzieci i młodzież mogą skorzystać z materiałów edukacyjnych online dotyczących bezpiecznego użytkowania Internetu na stronach Fundacji Orange[69] czy Fundacji Dajemy Dzieciom Siłę[70].

---

[66] Tamże, s. 289.
[67] Tamże, s. 291.
[68] K. Kupczyk, dz. cyt.
[69] Fundacja Orange, https://fundacja.orange.pl/strefa-wiedzy/ (dostęp: 3.02.2020).
[70] Zob. https://www.edukacja.fdds.pl/ (dostęp: 3.05.2020).

W przypadku doświadczenia przemocy, mimo strachu oraz rozchwianych emocji, należy także pamiętać o kilku zasadach postępowania pomocnych w walce z prześladowcą[71]:

Gromadź dowody – zaleca się, by pod wpływem emocji nie niszczyć żadnych dowodów, a mogą być nimi wiadomości w formie tradycyjnej i elektronicznej, np. e-mail, SMS, wpis na czacie czy komentarz w mediach społecznościowych; mogą to być wiadomości tekstowe, graficzne lub głosowe. Wszystkie dowody nękania rejestruj, zapisuj, przechowuj i archiwizuj (np. rób zdjęcia, nagrywaj rozmowy, gromadź rachunki, by można było prawidłowo ocenić wielkość strat itp.), bo szczególnie w przypadku cyberstalkingu sprawca może usunąć niektóre dowody swojego przestępstwa – a te będą potrzebne, by go ścigać i ukarać. Możesz także skontaktować się z administratorem strony/ /forum/portalu w celu zabezpieczenia treści i pozostawienia logów lub poprosić o to policję.

Wyraź sprzeciw – jeśli znasz sprawcę, poinformuj go przy zaufanych świadkach o swoim sprzeciwie wobec jego działań oraz żądaj ich zaprzestania; jeśli możesz, udokumentuj to (rejestracja rozmowy).

Kontroluj emocje – to trudne, ale może wpłynąć na postępowanie sprawcy; słabość ofiary wzmacnia stalkera, jej agresywna postawa prowokuje do dalszych działań, nie należy więc wdawać się w dyskusje i kłótnie, dochodzić przyczyn postępowania stalkera czy o coś go prosić itp.

Sprawdź swoje urządzenia i otoczenie – jeżeli znasz stalkera, mógł w Twoim najbliższym otoczeniu umieścić urządzenia rejestrujące głos czy obraz lub zainstalować na Twoich urządzeniach cyfrowych oprogramowanie szpiegujące, by poznać Twoje plany oraz kontrolować cię; zmień dane logowania przy użyciu innych, zaufanych urządzeń.

Zadbaj o towarzystwo – dla własnego samopoczucia, bezpieczeństwa i możliwości świadczenia o twoim problemie podziel się z bliską osobą swoim problemem, postaraj się przebywać z innymi, znanymi sobie ludźmi. Izolacja i ukrywanie problemu na pewno nie pomoże.

Zawiadom organy ścigania – do tego będą potrzebne dowody oraz złożenie zawiadomienia o uporczywym nękaniu. Można to zrobić

---

[71] K. Kupczyk, dz. cyt.

w formie pisemnej lub ustnej, podając kilka podstawowych informacji dotyczących tego procederu, np. kiedy stalking się zaczął, jak długo trwa, jakie jest miejsce lub miejsca przestępstwa, kim jest sprawca lub co o nim wiesz, jakie posiadasz dowody – e-maile, SMS-y, bilingi, zdjęcia, wydruki wiadomości z Facebooka lub innych portali itp., czy znasz dane świadków (imię, nazwisko, adres). Każdy funkcjonariusz policji ma obowiązek przyjąć zawiadomienie bez względu na to, do jakiego komisariatu uda się ofiara. Wraz z zawiadomieniem o stalkingu nie zapominaj również o złożeniu wniosku o ściganie, wzory wniosków znajdziesz w Internecie[72].

W literaturze podjęto próbę wskazania, jak ofiary powinny się zachowywać w sytuacji zagrożenia przez stalkera. Zostały one opisane w książce *Stalking i inne formy przemocy emocjonalnej. Studium kryminologiczne*[73]. Jej autorka zwraca uwagę na stanowczość komunikatów adresowanych do stalkera (może być sformułowany w wiadomości, np. „Nie chcę utrzymywać z tobą żadnych kontaktów. Proszę nie dzwoń do mnie, nie pisz, nie przychodź pod mój dom"). Należy odciąć się, ignorować próby wszelkiego kontaktu, zatrzymać numer telefonu, by móc gromadzić dowody, zmienić nagranie poczty głosowej, powiadomić najbliższych, wymienić zamki w drzwiach, poinformować sąsiadów, unikać samotnego wychodzenia z domu, unikać bezpośrednich kontaktów ze sprawcą.

Ofiary stalkingu potrzebują wsparcia oraz pomocy w radzeniu sobie ze stresem oraz emocjami. Utrata pewności siebie, poczucia własnej wartości, poczucia bezpieczeństwa i kontroli, strach przed oceną innych oraz tendencja do izolacji mogą prowadzić do obniżenia samopoczucia, a nawet myśli i prób samobójczych.

W tych sytuacjach rośnie znaczenie rodziny oraz właściwych relacji w niej panujących, dzięki nim uda się zaobserwować u ofiary objawy nękania, skłonić ją do mówienia, zapewnić bliskość i pełne poparcie, a także namówić do przeciwdziałania.

---

[72] B. Szopa, *Uporczywe nękanie – gdzie zgłosić?*, 2015, https://stalking.com.pl/2015/07/10/uporczywe-nekanie-gdzie-zglosic/ (dostęp: 3.05.2020).

[73] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej…*

Upatruje się także znaczącą rolę świadków przemocy i ich wpływu na ocenę sytuacji zarówno przez sprawcę, jak i ofiarę przemocy. Obecność świadków i ich reakcje mogą być nie tylko „terapeutyczne", gdy stają w obronie ofiary, ale też toksyczne, gdy wzmacniają działania sprawcy. Szczególnie w przypadku cyberstalkingu granica między byciem sprawcą a świadkiem przemocy jest niezwykle płynna[74]. Z tego powodu należy zagadnienia kształtowania właściwych postaw wobec obserwowanej przemocy uwzględniać w zabiegach edukacyjnych na rzecz przeciwdziałania agresji.

Osoby dorosłe mogą poszukiwać pomocy w różnych placówkach, np. Ośrodkach Interwencji Kryzysowej oraz poradniach specjalizujących się w pomocy terapeutycznej. Kiedy ofiarą stalkingu staje się dziecko, ważne jest, aby w oddziaływania włączona była np. szkoła oraz poradnia psychologiczno-pedagogiczna. Niezbędny jest także kontakt z psychologiem, który oceni stopień wpływu tego, co się zdarzyło, na emocje dziecka i funkcjonowanie w życiu.

Działają także bezpłatne telefony zaufania: Telefon Zaufania dla Dzieci i Młodzieży (116 111, czynny codziennie od 12.00 do 2.00), Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci (800 100 100, czynny od poniedziałku do piątku w godz. 12.00–15.00) oraz Kryzysowy Telefon Zaufania (116 123) udostępniony dla osób doświadczających kryzysu emocjonalnego, samotnych, cierpiących z powodu depresji, bezsenności, chronicznego stresu, które z różnych powodów nie mają możliwości bezpośredniego kontaktu z psychologiem. Osoby potrzebujące pomocy mogą korzystać z telefonu codziennie w godz. 14.00–22.00. Ofiary stalkingu niewątpliwie doświadczają chronicznego stresu i znajdują się w kryzysie emocjonalnym[75].

Współczesny świat pod wpływem globalizacji nadającej rzeczywistości cechy kultury mozaikowej, obrazkowej i masowej, mimo wielu

---

[74] J. Barlińska, *Cyberprzemoc u adolescentów – o roli medium, własnych doświadczeń i empatii w zachowaniach świadków rówieśniczej przemocy elektronicznej*, praca doktorska napisana pod kier. dr hab. Anny Szuster-Kowalewicz, prof. UW, Warszawa 2013, s. 19, http://depotuw.ceon.pl/bitstream/handle/item/265/doktorat.pdf?sequence=1 (dostęp: 3.05.2020).

[75] Zob. https://biuroprasowe.orange.pl/ (dostęp: 3.05.2020).

zalet, wywołuje niestety w obywatelach poczucie osamotnienia i zagubienia w tej globalnej i natychmiastowej przestrzeni zmieniającej znaczenie czasu, co przekłada się na spłycenie relacji międzyludzkich oraz obniżenie poziomu umiejętności komunikacji i współodczuwania. Wyraża się to niejednokrotnie w problemach emocjonalnych, międzyludzkich nieporozumieniach komunikacyjnych, nieumiejętności nawiązywania i utrzymywania głębokich i bezpośrednich relacji partnerskich, niewłaściwym zaspokajaniu własnych potrzeb czy daleko posuniętej wyobrażeniowości. Swoista wolność, poczucie anonimowości i braku kontroli przerastają wielu, którzy niewłaściwie próbują odnaleźć się w tej nowej rzeczywistości, przejawiając swoją „bezradność" w formie agresji i przemocy. Czy to już patologia, czy wołanie o pomoc? Trzeba reagować: edukować, wychowywać, przeciwdziałać i pomagać znów stać się istotą społeczną.

W literaturze zwraca się również uwagę na rolę działań terapeutycznych zarówno wobec ofiary, jak i sprawcy. Podkreśla się, że obie te osoby były w bliskiej relacji. Pomoc powinna być ukierunkowana na ochronę ofiary i zaprzestanie stosowania przemocy przez sprawcę (co wymaga wypracowania sposobów radzenia sobie z emocjami)[76]. Dagmara Woźniakowska-Fajst przytacza wyniki badań za Paulem Mullenem, Michele Pathé, Rosemary Purcell zawartych w publikacji *Stalkers and their victims*[77], które wskazują na konieczność zindywidualizowanej terapii wobec sprawców uwzględniającej typ stalkera. Stalkerzy z kategorii odrzuconych potrafią racjonalnie ocenić sytuację (zyski i straty), skonfrontowani ze skutkami swoich czynów potrafią zaprzestać nękania (tu skuteczna może być kara w zawieszeniu). Kara w zawieszeniu orzeczona wobec stalkerów z grupy urażonych będzie niewystarczająca, racjonalizują oni bowiem zasadność swojego znęcania się nad ofiarą, nie mają poczucia winy, kara wymierzona przez sąd jest przez nich traktowana jako niesprawiedliwość, często postrzegają oni siebie w kategoriach osoby pokrzywdzonej. Sprawcy z tej grupy

[76] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej*…, s. 291.
[77] P. Mullen i in., dz. cyt., s. 1244–1249.

mają trudności z samokontrolą, bywają impulsywni, agresywni (często są oni uzależnieni od środków psychoaktywnych)[78].

Niezwykle ważne dla przewidywań dotyczących zachowań stalkerów wobec ofiar jest rozpoznanie motywów ich postępowania. Bardzo niebezpieczne mogą być zachowania stalkerów skategoryzowanych jako odrzuceni (najczęściej są nimi byli partnerzy ofiar). Mogą oni stosować przemoc fizyczną, niszczyć mienie ofiary, ich groźby zazwyczaj są przez nich spełniane. Należy unikać wszelkich kontaktów, spotkań z tym typem sprawcy. Typ sprawcy zakochanego wymaga działań edukacyjno-poznawczych i odseparowania fizycznego od osoby prześladowanej. „Najbardziej niebezpieczni sprawcy mają za sobą historię zachowań kryminalnych (także seksualnych i uprzedniego stalkingu) lub leczenie psychiatryczne. Są to na przykład osoby chore na schizofrenię lub o osobowości typu borderline"[79]. Osoby te cechuje fiksacja urojeniowa, są one niepodatne na racjonalną argumentację, w przypadku terapii zaleca się leczenie psychiatryczne. Najniebezpieczniejszą grupę stalkerów stanowią tzw. drapieżcy. Wszelkie próby wymuszania zmiany ich zachowania są nieskuteczne, mogą wywoływać jeszcze większe natężenie zachowań agresywnych. Ofiara powinna w takiej sytuacji zmienić miejsce zamieszkania[80].

Hejt

Słownik języka polskiego PWN definiuje słowo „hejt" jako „obraźliwy lub agresywny komentarz zamieszczony w Internecie"[81]. Inna definicja hejtera określa go jako osobę, „która umieszcza w Internecie wpisy, w których źle o kimś (rzadziej o czymś) pisze, obrażając tego

---

[78] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej*…, s. 295.

[79] Tamże, s. 296, za: L. Sheridan, J. Boon, *Stalkers typologies: Implications for law enforcement*, w: L. Sheridan, J. Boon (eds.), *Stalking and psychosexual obsession. Psychological perspectives for prevention, policing and treatment*, John Wiley & Sons, Chichester 2002, s. 69.

[80] Tamże.

[81] *Hejt*, https://sjp.pwn.pl/sjp/hejt;5580544.html (dostęp: 3.05.2020).

kogoś i nie zamieszczając przy tym żadnej rzeczowej krytyki; słowo potoczne”[82].

Hejt jest definiowany również jako „1. *pot., dezapr.* «a) obraźliwe, agresywne, prowokacyjne lub skrajnie krytyczne komentarze zamieszczane w internecie; b) także taki komentarz» 2. *pot., dezapr.* «to samo, co hejter»”[83]. Hejter to „ktoś nienawidzący”, „osoba w nieuzasadniony sposób niechętna jakiemuś zjawisku”[84].

Hejt to „agresja destrukcyjna o podłożu psychicznym, społecznym i kulturowym”[85]. Wypowiedź hejtera cechuje agresja językowa o niskiej wartości informacyjnej[86], u której podstaw leży „intencja zdeprecjonowania odbiorcy”[87]. W literaturze mamy do czynienia z następującymi pojęciami: język wrogości, mowa agresji, hejting. Język wrogości charakteryzuje się przekazem zawierającym negatywne w opinii agresora przyrodzone cechy przeciwnika (mogą być one tworzone jako skojarzenie, metafory)[88]. Bardzo często nadawca, którego przekaz słowny można uznać za mowę agresji, prezentuje spójny obraz wroga, nacechowany brakiem szacunku o charakterze destrukcyjnym[89]. Język ten opiera się na emocjach i sądach wartościujących[90]. Hejting odnosi się do agresji inter-

---

[82] *Hejter*, https://dobryslownik.pl/slowo/hejter/218709/ (dostęp: 3.05.2020).

[83] *Hejt*, http://www.nowewyrazy.uw.edu.pl/haslo/hejt.html (dostęp: 3.05.2020).

[84] A. Naruszewicz-Duchlińska, *Nienawiść w czasach Internetu*, Novae Res, Gdynia 2015, s. 13, za: P. Fliciński, S. Wojtowicz, *Hip-hop słownik*, Wydawnictwo Naukowe PWN, Warszawa 2007, s. 16, 66.

[85] A. Naruszewicz-Duchlińska, dz. cyt., s. 25, za: J. Gajda, *Agresja językowa w stosunkach międzyludzkich*, w: W. Gruszczyński (red.), *Język narzędziem myślenia i działania*, Dom Wydawniczy ELIPSA, Warszawa 2002, s. 61.

[86] A. Naruszewicz-Duchlińska, dz. cyt., s. 26.

[87] Tamże, s. 11, za: M. Peisert, *Formy i funkcje agresji werbalnej. Próba typologii*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2004, s. 40.

[88] A. Naruszewicz-Duchlińska, dz. cyt., s. 22, za: B. Markowska, *Jacy „my” i jacy „oni”? Analiza semantyczna nazw i etykiet*, w: X. Bukowska, B. Markowska (red.), *To oni są wszystkiemu winni… Język wrogości w polskim dyskursie publicznym*, Trio, Warszawa 2013, s. 52.

[89] A. Naruszewicz-Duchlińska, dz. cyt., s. 22, za: M. Nowicka, *Dyskurs o dyskursie, czyli o mowie wrogości przy pomocy mowy wrogości*, w: X. Bukowska, B. Markowska (red.), dz. cyt., s. 123.

[90] A. Naruszewicz-Duchlińska, dz. cyt., s. 22, za: J. Puzynina, *Słowo – wartość – kultura*, Towarzystwo Naukowe Katolickiego Uniwersytetu Lubelskiego, Lublin 1997.

personalnej[91], ma charakter intencjonalny, hejter stara się swoimi wypowiedziami urazić odbiorcę[92]. Pojęcie hejtu różni się od cyberbullyingu. Jak pisze Jacek Pyżalski, „wielu aktom cyberbullyingu, czy szerzej agresji elektronicznej w ogóle, towarzyszy brak negatywnych intencji"[93], uczniowie często ośmieszają kolegów, nie mając intencji ich skrzywdzenia.

Zwraca się uwagę, że „agresywny ton i obraźliwe sformułowania pojawiają się tylko w 2,5% wypowiedzi"[94].

Odpowiedzialność karna

W Kodeksie karnym hejt może być rozpatrywany w odniesieniu do artykułów zawartych w rozdziale XXVII. W art. 196 czytamy: „Kto obraża uczucia religijne innych osób, znieważając publicznie przedmiot czci religijnej lub miejsce przeznaczone do publicznego wykonywania obrzędów religijnych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2"; według art. 257: „Kto publicznie znieważa grupę ludności albo poszczególną osobę z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości lub z takich powodów narusza nietykalność cielesną innej osoby, podlega karze pozbawienia wolności do lat 3". W art. 133 zawarto znieważenia dotyczące narodu polskiego i Rzeczpospolitej Polskiej: „Kto publicznie znieważa Naród lub Rzeczpospolitą Polską, podlega karze pozbawienia wolności do lat 3". Artykuł 212, § 1 infor-

---

[91] A. Naruszewicz-Duchlińska, dz. cyt., s. 45, za: A. Frączek, *Czynności agresywne jako przedmiot studiów eksperymentalnej psychologii społecznej*, w: A. Frączek (red.), *Studia nad psychologicznymi mechanizmami czynności agresywnych*, Ossolineum, Wrocław 1979, s. 196.

[92] A. Naruszewicz-Duchlińska, dz. cyt., s. 26.

[93] J. Pyżalski, *Polscy nauczyciele i uczniowie a agresja elektroniczna – zarys teoretyczny i najnowsze wyniki badań*, w: M. Jędrzejko, D. Sarzała (red.), *Człowiek i uzależnienia*, Akademia Humanistyczna im. Aleksandra Gieysztora, OficynaWydawnicza ASPRA-JR, Pułtusk–Warszawa 2010.

[94] A. Naruszewicz-Duchlińska, dz. cyt., za: Ł. Jonak, *Dlaczego boimy się jednego procenta? O braku agresji w Internecie*, w: K. Krejtz (red.), *Internetowa kultura obrażania?*, Interactive Advertising Bureau Polska, Szkoła Wyższa Psychologii Społecznej oraz Ośrodek Przetwarzania Informacji, 2012, s. 58, http://komentuj-nieobrazaj.pl/media/KOraport.pdf. (dostęp: 3.05.2020).

muje z kolei: „Kto pomawia inną osobę, grupę osób, instytucję, osobę prawną lub jednostkę organizacyjną niemającą osobowości prawnej o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności, podlega grzywnie albo karze ograniczenia wolności"; art. 212, § 2 zaś: „Jeśli sprawca dopuszcza się czynu określonego w § 1 za pomocą środków masowego komunikowania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku". W § 4 jest mowa o tym, że „ściganie przestępstwa określonego w § 1 lub § 2 odbywa się z oskarżenia prywatnego"[95].

W Kodeksie cywilnym odnajdujemy paragraf, który chroni dobra osobiste człowieka. Jest to art. 23: „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"; oraz art. 24, § 1: „Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadość-uczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny"; i § 2: „Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych"[96].

W raporcie, który powstał w ramach projektu „Media against hate"[97], odnajdujemy statystyki odnoszące się do naruszenia art. 256

---

[95] Zob. http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU19970880553/U/D19970553Lj.pdf (dostęp: 3.05.2020).

[96] Tamże.

[97] *Polska – reagowanie na mowę nienawiści*, 2018, https://www.article19.org/wp-content/uploads/2018/04/Poland-Hate-Speech-report%E2%80%94-Polish.pdf (dostęp: 3.05.2020)

i art. 119. W art. 256, § 1 czytamy: „Kto publicznie propaguje faszystowski lub inny totalitarny ustrój państwa lub nawołuje do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". W § 2: „Tej samej karze podlega, kto w celu rozpowszechniania produkuje, utrwala lub sprowadza, nabywa, przechowuje, posiada, prezentuje, przewozi lub przesyła druk, nagranie lub inny przedmiot, zawierające treść określoną w § 1 albo będące nośnikiem symboliki faszystowskiej, komunistycznej lub innej totalitarnej"; art. 119, § 1 informuje natomiast: „Kto stosuje przemoc lub groźbę bezprawną wobec grupy osób lub poszczególnej osoby z powodu jej przynależności narodowej, etnicznej, rasowej, politycznej, wyznaniowej lub z powodu jej bezwyznaniowości, podlega karze pozbawienia wolności od 3 miesięcy do lat 5". Wiele komentarzy hejterów ma charakter dyskryminujący inność. Liczba skazań z art. 256, § 1 w 2014 r. wyniosła 34 (z liczby 398 zgłoszonych przez policję) oraz z art. 256, § 2 w 2015 r. sięgnęła 75 (z 299 zgłoszonych przez policję)[98]. Jak pokazują statystyki, liczba zgłoszeń i skazań osób, których zachowanie i komentarze były sklasyfikowane jako przestępstwo, jest wysoka.

Agresja werbalna – opis zjawiska

Alina Naruszewicz-Duchlińska w książce pt. *Nienawiść w czasach Internetu* przywołuje (za: Krzysztofem Krejtzem i Pawłem Kolendą)[99] cechy wypowiedzi hejterów, które odnoszą się do:

- treści – przedstawia ona negatywny stosunek do osoby lub przedmiotu wypowiedzi, w treściach pojawiają się: wyszydzanie, lżenie, poniżanie, ubliżanie, dyskredytowanie, umniejszanie, wypowiedź cechuje brak szacunku, stereotypizacja, lekceważenie, ogólny stosunek negatywny;

---

[98] Tamże.

[99] K. Krejtz, P. Kolenda, *W jaki sposób badać kulturę wypowiedzi w internecie?*, w: K. Krejtz (red.), dz. cyt., s. 17–24.

- opisu – obejmującego agresję, grożenie, obrażanie;
- formy – cechują ją ton sarkastyczny, ironia, negatywny ładunek emocjonalny;
- języka wypowiedzi – wulgaryzmy, groźby, wykluczanie, depersonalizacja, określenia obraźliwe, trolling, prowokacje;
- ogólnej oceny komunikatu – przekraczanie granicy kultury wypowiedzi[100]. Hejt obejmuje gamę uczuć: gniew, złość, niechęć[101]. Zachowania hejterów cechują: celowość, świadomość, powtarzalność, cykliczność, lekceważenie netykiety[102], wrogość, agresja, obniżenie wartości osoby, destruktywna deprecjacja[103].

Przyczyn zachowań agresywnych doszukuje się w niezadowoleniu, odreagowywaniu frustracji, strachu lub chęci wywoływania tych stanów u innych osób[104] oraz popędzie agresywnym. Agresja może wiązać się z przyjmowanym przez agresora modelem redukcji lęku[105]. U podłoża przemocy werbalnej leży agresja ukierunkowana na dominację, wynika ona z wrogich motywów. Przyczyny zachowań agresywnych widzi się również w sytuacji sprawcy, którą cechuje silne psychiczne lub fizyczne obciążenie[106]. W literaturze przedmiotu wymienia się wiele teorii i koncepcji, które wyjaśniają genezę zjawiska agresji. Jedne upatrują przyczyny tych zachowań w czynnikach biologicznych, socjobiologicznych, inne w psychologicznych (behawioralnych, poznawczych, socjopsychologicznych). Agresja może być zatem wynikiem ewolucji, popędu, reakcją na bodziec, funkcją przetwarzania informacji, może być także skutkiem wyuczonego wzmocnienia lub rezultatem procesu podejmowania decyzji. Jedną z teorii, która ma silne umocowanie w eksperymentach, jest Społeczna Teoria Uczenia się Alberta Bandury. Autor ten zwrócił uwagę na rolę obserwowania zachowań modelowych

---

[100] A. Naruszewicz-Duchlińska, dz. cyt., s. 9–10.

[101] Tamże, s. 16.

[102] Tamże, s. 18.

[103] Tamże, s. 22.

[104] M. Peisert, dz. cyt., s. 22, za: A.S. Reber, *Słownik psychologii*, red. nauk. I. Kurcz, K. Skarżyńska, Scholar, Warszawa 2000, s. 28.

[105] Tamże, s. 23.

[106] Tamże, s. 157.

i późniejsze ich odtwarzanie w działaniach agresywnych. To ujęcie pozwala na szukanie przyczyn zachowań agresywnych w środowisku rodzinnym lub strefie najbliższego rozwoju człowieka. Psychoterapeuci podkreślają rolę uzależnień w uruchamianiu aktów agresywnych.

Akt przemocy słownej odznacza się brakiem empatii hejtera, chęcią sprawienia cierpienia innej osobie. Maria Peisert zwraca uwagę na uczucia, takie jak gniew, oraz czerpanie przez sprawcę agresji pewnych korzyści. Hejter może odczuwać tzw. złośliwą radość (formę gratyfikacji za jego brak osiągnięć) lub jego zachowania mogą zmierzać ku wzmocnieniu pozycji w grupie (przez chęć dominacji), zwrócenia na siebie uwagi lub autoprezentacji[107].

Język ten opiera się na kategoryzacji my–oni, nienawiść ta jest ukierunkowana na dyskryminowanie grup[108] i jednostek. Hejt (mowa nienawiści) charakteryzuje się: redukcją osoby lub grupy społecznej do przypisywanej im cechy pomijającej różnice indywidualne, warto dodać, że wnioskowanie hejtera opiera się na stereotypach[109]. Hejt wyróżnia konflikt, wrogość interakcji, zachowania destrukcyjne i wykluczające porozumienie[110]. Akt komunikowania jest zaburzony, swoje agresywne komunikaty hejter prezentuje na forum publicznym i często przewiduje reakcje audytorium[111]. Jego działania są ukierunkowane na przyciągnięcie uwagi, nie chodzi tu o konstruktywną krytykę zmierzającą do poprawy stanu, pozytywnej zmiany, komentarze mają bowiem na celu wzbudzanie „niekonstruktywnych i nierealistycznych konfliktów służących ekspresji agresji ukierunkowanej na zaszkodzenie, pokonanie”[112]. Hejterzy w swoich wypowiedziach podkreślają przypisywane jednostkom lub grupom cechy, które mają wpłynąć na negatywne po-

---

[107] Tamże.

[108] A. Naruszewicz-Duchlińska, dz. cyt., s. 21.

[109] A. Bulandra, J. Kościołek, *Przeciwdziałanie mowie nienawiści. Podręcznik dla środowiska politycznego*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=11&cad=rja&uact=8&ved=2ahUKEwjBnKDOgKXpAhXPy6YKHQmVBsI4ChAWMAB6BAgBEAE&url=http%3A%2F%2Finterkulturalni.pl%2Fplik.php%3Fid%3D148&usg=AOvVaw2uSqLzbu9svAT2iV19FDi4 (dostęp: 3.05.2020).

[110] A. Naruszewicz-Duchlińska, dz. cyt., s. 13.

[111] Tamże.

[112] Tamże, s. 26.

strzeganie swoich ofiar[113]. Hejterzy łamią tabu językowe, stosują wyzwiska, szyderstwo, ironizują. Ich język cechuje się niecenzuralną wypowiedzią, grubiańskim i obraźliwym słownictwem[114]. Warto zwrócić uwagę, że świadkowie hejtu odznaczają się różnym stopniem wrażliwości na język, którym operuje hejter. Wrażliwość ta zależy m.in. od płci, wieku, wykształcenia, pochodzenia społecznego, religii[115]. W literaturze zwraca się uwagę na grupę obrońców hejterów. Osoby te postrzegają otaczający je świat jako niesprawiedliwy i zły, a siebie jako ofiary[116]. Hejterzy, jak pisze Naruszewicz-Duchlińska, nie tworzą grup czy też wspólnot. Ich komunikację cechuje brak więzi osobistej. Motywacją hejtera jest zaznaczenie swojej obecności w społeczności sieciowej, narzucenie własnego zdania, wciągnięcie odbiorców w emocjonalną dyskusję, kontrola i korzyści emocjonalne, takie jak: „poczucie mocy słuszności i skuteczności"[117], dominowanie dyskusji (przez ataki, obelgi, powtarzanie argumentów)[118]. Agresja słowna ma charakter czynny, impulsywny lub jest wywołana czynnikami sytuacyjnymi[119], u jej podstaw leżą „potrzeby egocentryczne, rozładowanie napięcia, potrzeba akceptacji, przynależności, tożsamości, uznania, osiągnięć czy niezależności"[120]. Wśród mechanizmów wymienianych w literaturze, na których hejt się opiera, wymienia się: poczucie władzy i prawa do czegoś, chęć zaznaczenia, że jest się lepszym, skromność i pamięć o dawnych czasach i osobach[121], chęć dominacji grupy przez narzucanie własnych

---

[113] A. Bulandra, J. Kościołek, dz. cyt.

[114] A. Różyło, *Agresja werbalna. Próba klasyfikacji o inspiracji kognitywnej*, http://pedkat.pl/images/czasopisma/pk8/art19.pdf (dostęp: 3.05.2020).

[115] M. Peisert, dz. cyt., s. 31.

[116] A. Naruszewicz-Duchlińska, dz. cyt., s. 60.

[117] Tamże, s. 34–35.

[118] Tamże, s. 41.

[119] M. Peisert, dz. cyt., s. 178.

[120] A. Naruszewicz-Duchlińska, dz. cyt., s. 51, za: A. Jasik, *Wyzwiska, obelgi, pogróżki w gwarze uczniowskiej (próba typologii gatunku)*, w: A. Dąbrowska, A. Nowakowska (red.), *Język a Kultura*, t. 17: *Życzliwość i agresja w języku i kulturze*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2005, s. 259.

[121] A. Naruszewicz-Duchlińska, dz. cyt., s. 52.

wartości i wizji świata[122]. Hejter traktuje obiekt ataku w sposób instrumentalny i intencjonalny. Reakcja hejtera może być ukierunkowana na: medium (telewizja, Internet), autora posta, wpisu, bloga lub artykułu, może odnosić się do innych ludzi lub do osoby będącej bohaterem treści tekstu, posta, filmu, hejter może oceniać też wytwór (piosenkę, film, tekst, pracę graficzną lub artystyczną). Zwykle formy językowe dotyczące osób hejterzy formułują następująco: imię i nazwisko łączą z negatywnymi określeniami, zastępują imię i nazwisko osoby obraźliwym określeniem związanymi z tabu, fizjologicznymi lub płciowymi czynnościami, stosują przezwiska, określają osoby nazwami roślin lub zwierząt, sformułowaniami wskazującymi na naruszanie przez obiekt hejtu norm społecznych lub mającymi podkreślać brak wiedzy[123]. Język hejtu charakteryzuje subiektywność i „styl potoczny lub emocjonalny cechowany antropocentrycznie"[124]. W komunikatach hejterów odnajdujemy uzasadnienia ich działań dyskryminacyjnych[125].

Hejterzy powołują się często na ich prawo do wyrażania opinii, wolność słowa, uważają również, że osoba hejtowana zasługuje na atak. Świadomie łamią zasady i regulaminy obowiązujące na forach lub portalach społecznościowych. Osoby te postrzegają siebie jako „orędowników wolności słowa i wyrazicieli nieprzyjemnych prawd […], reprezentantów tradycji, walczących o sprawiedliwość i demokrację, zagrożonych przez cenzurę"[126]. Często hejterzy czerpią satysfakcję z wrogości i reakcji ofiary[127]. Ofiara jest odhumanizowana, nie posiada ona żadnych walorów i wartości, opinie o niej w komentarzu hejtera są skrajne, wyrażane z pogardą i złością. Hejter daje sobie prawo do oceny

---

[122] Tamże, s. 61, za: B. Witosz, *O dyskursie wykluczenia i dyskursach wykluczonych z perspektywy lingwistycznej*, „Tekst i Dyskurs – Text und Diskurs" 2010, 3, s. 15.

[123] M. Peisert, dz. cyt., s. 156–157.

[124] A. Naruszewicz-Duchlińska, dz. cyt., s. 145, za: J. Bartmiński, *Styl potoczny*, w: J. Anusiewicz, Fr. Nieckula (red.), *Język a Kultura*, t. 5: *Potoczność w języku i kulturze*, Wiedza o Kulturze, Wrocław 1992, s. 43.

[125] A. Bulandra, J. Kościołek, dz. cyt.

[126] A. Naruszewicz-Duchlińska, dz. cyt., s. 35–38.

[127] Tamże, s. 50, za: J. Reykowski, *Autorytaryzm a agresja wobec swoich i obcych*, w: Ł. Jurasz-Dudzik (red.), *Człowiek i agresja. Głosy o nienawiści i przemocy. Ujęcie interdyscyplinarne*, Sic!, Warszawa 2002, s. 57.

osoby lub grupy osób. Zwraca się uwagę, że „każde zachowanie i cecha osobnicza mogą być określone przez hejterów jako niewłaściwe. Niezależnie od tego, co się zrobi, jaki model życia wybierze, którą popiera się partię i jaką wyznaje religię, w którym kraju się urodziło i w którym się żyje, jaką nosi się odzież itd. […] wystarczającym powodem krytyki jest istnienie jej obiektu”[128].

Negatywne opinie formułowane przez inne osoby nie powinny wpływać na samoocenę. Zaleca się[129], by zaakceptować swoją indywidualność i wyjątkowość i być sobą. Inna technika jest określana jako asocjowanie i dysocjowanie – to zmiana spojrzenia na sytuację od wewnątrz (z pozycji ja) na zewnątrz z pozycji obserwatora. Negatywne opinie są bodźcami wywołującymi negatywną reakcję, zatem można zmniejszyć siłę ich oddziaływania na emocje. Wymaga ona przywoływania wrogich komentarzy tak długo, aż reakcja na nie straci na intensywności. Technika znajdowania przekonań opiera się na zapisie czyjegoś szkodliwego stwierdzenia w formie zdania, potem należy zadać pytanie „i co to oznacza?” (równoważności), „dlaczego tak myślisz?”, „do czego to prowadzi?”, „bo…”, „gdzie i kiedy się tego nauczyłeś?” (zasada przyczynowości A → B).

Podstawą testu kamery jest opisane sytuacji na kartce i jej analiza, ważne, by była pozbawiona emocji i odnosiła się do faktów. Osoba korzystająca z tej techniki raz jeszcze spisuje sytuację, opierając się na faktach rejestrowanych w oku kamery.

Technika kontrastu pozwala na spojrzenie na swoją sytuację, przyjmując jej jeszcze gorszą perspektywę. Integracja przeciwieństw polega na narysowaniu tabel – w jednej z nich wypisujemy obelgi, w drugiej zaś ich przeciwieństwa. Ważne jest, by efekt miał charakter integralny. Mateusz Grzesiak proponuje również ćwiczenie pozwalające na uwolnienie się od negatywnych emocji towarzyszących ocenie innych osób. Należy pomyśleć o sytuacji, która wywołała negatywny stan emocjonalny, na podłodze umieścić symbol tej emocji i stanąć przy nim, prezen-

---

[128] A. Naruszewicz-Duchlińska, dz. cyt., s. 134.

[129] M. Grzesiak, *8 sposobów na uwolnienie się od opinii innych*, https://mateuszgrzesiak.pl/8-sposobow-uwolnienie-sie-opinii-innych/ (dostęp: 3.05.2020).

tując ciałem tę emocję, potem wyobrazić sobie emocję przeciwną do tej odczuwanej, narysować symbol w innym miejscu i kolejno przedstawić go pozycją ciała. Wrócić do pierwszego symbolu i przyjąć pozycję ciała z sytuacji drugiej[130].

Agresja słowna może mieć również charakter pośredni, hejter stosuje wtedy wyszukane określenia świadczące o wyrobieniu językowym, może również podejmować próby wykluczenia jakiejś osoby z rozmowy[131].

Do reakcji użytkowników na hejt zalicza się: dyskusję z hejterem (chęć przedstawienia argumentów, przekonania hejtera), ignorowanie wypowiedzi, reagowanie przez humorystyczne i ironiczne komentarze, dystans. Blokowanie lub usuwanie komentarzy hejterskich jest podejmowane przez moderatorów strony lub forum. Sposobem na ograniczenie hejterskich komentarzy jest obowiązek rejestracji. Zwraca się uwagę na rolę działań edukacyjnych odnoszących się do netykiety i prowadzenia merytorycznej dyskusji.

Wymienione działania są skuteczne, jednak najważniejsze jest zdanie sobie sprawy, że hejter pragnie uwagi i podejmowania z nim dyskusji. Innymi poza wymienionymi strategiami radzenia sobie z tym zjawiskiem są asertywność lub celna riposta[132]. Jak wspomniano, źródłem agresji słownej jest lęk, przekonanie o konieczności walki, złość, niezadowolenie, deprecjonowanie cudzych potrzeb, utrata szacunku dla innych. Relacje te opierają się na strachu[133]. Zachowanie asertywne „to zespół zachowań interpersonalnych, sposobów, w jaki człowiek komunikuje się z innymi, pokazuje, co czuje, myśli, chce, na co się zgadza"[134]. Osoba powinna jasno komunikować, jak chce być traktowana i na jakie zachowania nie wyraża zgody. W książce pt. *Asertywność w przykładach. Jak się zachowywać w typowych sytuacjach* Dorota Gromnicka

---

[130] Tamże.

[131] A. Różyło, dz. cyt.

[132] M. Nöllke, *Asertywność i sztuka celnej riposty*, tłum. A. Komin, Wydawnictwo BCedu, Warszawa 2010.

[133] D. Gromnicka, *Asertywność w przykładach. Jak się zachowywać w typowych sytuacjach*, „Samo Sedno", Edgard, [b.m.] 2015, s. 20.

[134] Tamże, s. 25.

opisuje wiele przykładów asertywnych zachowań. Wśród wypowiedzi, które można by skierować wobec hejtera, przytacza następujące: „nie życzę sobie…", „nie pozwalam…", „nie zgadzam się na to, abyś…", „uważam…", „oczekuję…". W przypadku reakcji na krytykę autorka ta zaleca: a) odniesienie do faktów, b) wzięcie odpowiedzialności, c) przedstawienie własnego punktu widzenia, d) ustalenie zasad i norm. Podkreśla również rolę wyrażania emocji, np. „nie lubię, kiedy…", „nie podoba mi się, gdy…", „drażni mnie, kiedy…", „złości mnie…", „jestem wściekła, kiedy się tak odnosisz, i nie mam ochoty…". Podkreśla, że asertywność pozwala na zachowanie własnej godności i szacunku do siebie. Istotne jest, by być konsekwentnym w słowach (np. „jeśli raz jeszcze tak się do mnie zwrócisz, nie będę się do ciebie odzywał/a").

Inne przykłady walki z hejtem odnajdujemy w książce Matthiasa Nöllkego *Asertywność i sztuka celnej riposty*[135]. Z wielu opisanych przykładów kilka propozycji można by zastosować w komunikacji z hejterem. Autor przede wszystkim wskazuje, że w sytuacji agresji słownej należy stworzyć świadomą przestrzeń bezpieczeństwa, np. wyobrazić sobie, że wokół nas rozciąga się ochronna fizyczna bariera, takiemu wyobrażeniu powinny towarzyszyć myśli: „jestem bezpieczny", „nie rusza mnie to", „wszelkie negatywne słowa odbijają się od mojej przestrzeni". Warto wyuczyć się kilku stwierdzeń, które można użyć, odpowiadając na złośliwe lub agresywne komentarze, np. „to ciekawe!", „biorę z Ciebie przykład", „nie masz innych problemów?", „umiesz to powiedzieć od tyłu?", „to zbyt okrągłe na moją kwadratową głowę", „popatrzymy, to zobaczymy", „gdy będę chciała poznać Twoją (hejtera) opinię, to ci ją przekażę", „podejmowałam dobre decyzje w przeszłości i w przyszłości", „Biblia mówi: też nie będziesz…", „no i dobrze!", „ja nie mam z tym żadnego problemu!", „jeśli to ci poprawi humor…", „po prostu zadziwiające!", „to Twoja opinia". Autor zwraca uwagę na rolę świadomego milczenia w relacjach międzyludzkich.

W książce *Hejtoholik, czyli jak zaszczepić się na hejt, nie wpaść w pułapkę obgadywania oraz nauczyć się zarabiać na tych, którzy Cię oczerniają* Michał Wawrzyniak przedstawia metody radzenia sobie

[135] M. Nöllke, dz. cyt., s. 65–113.

z hejterem. Jedna z nich opiera się na przygotowaniu merytorycznej odpowiedzi odwołującej się do faktów. Metodą opisywaną przez wspomnianego autora jest Z-W+, zgodnie z którą wyszukuje się w wypowiedzi hejtera pozytywnych aspektów. Zaleca się również operowanie humorem. Jeszcze inna metoda jest określana jako kwarantanna i polega na zaprzestaniu jakichkolwiek kontaktów z hejterem, w tym przypadku zalecane jest blokowanie możliwości odczytywania treści zamieszczanych przez hejtera[136].

Warto wspomnieć o innych metodach[137], do których zalicza się: metodę Skłodowskiej (dowodzi się w niej, że „hejt to głupie zachowanie lub nie przystoi danej osobie"), metodę ignorowania (niereagowanie), metodę „oko za oko" (odpowiada się na hejt hejtem – jednak ze względu na to, że może ona uruchomić spiralę agresji, nie należy jej zalecać uczniom). Stosując metodę na Piotra K. (znanego milionera) – należy reagować na hejt przez podkreślanie swoich zalet i wyjątkowości. Metoda racjonalna (na Donalda Tuska) wymaga wykazania, że komunikat zamieszczony przez hejtera jest nieracjonalny i niezgodny z rzeczywistością. Kolejna jest metoda Kuźniara – opiera się na wyciąganiu konsekwencji z hejtu i informowaniu hejtera, że poinformuje się jego pracodawcę o jego zachowaniu. Metoda na Peszek (cierpię jak Maria Peszek w Bankoku) wykorzystuje strategię polegającą na włączeniu wypowiedzi hejtera w sympatyczne komunikaty mające na celu nawiązanie kontaktu z fanami. Metoda na dyskutanta sprowadza się do podejmowania rozmowy z hejterem (co raczej, jak pisze autorka raportu, jest mało skuteczne)[138].

W tym miejscu warto zauważyć, że problematyka hejtu w przestrzeni Internetu ma swoją ciemną stronę wyraźnie widoczną w przykładach działań nieuczciwej konkurencji między firmami. Firmy lub

---

[136] M. Wawrzyniak, *Hejtoholik, czyli jak zaszczepić się na hejt, nie wpaść w pułapkę obgadywania oraz nauczyć się zarabiać na tych, którzy Cię oczerniają*, Helion, Warszawa 2015, s. 190–206.

[137] M. Czaplicka, *Hejt w internecie. Raport ilościowy*, https://prowly-uploads.s3.amazonaws.com/uploads/landing_page_image/image/11744/raport-o-hejcie-w-sieci.pdf (dostęp: 3.05.2020).

[138] Tamże.

zwolennicy partii politycznych opłacają aktywność hejterów i osób zajmujących się trollingiem. Działania tych osób często wiążą się z rozpowszechnianiem pomówień i nieprawdziwych informacji. Niektóre wskazania skierowane do osób zwalczających nieuczciwą konkurencję w przestrzeni Internetu mogą być zaadaptowane przez innych użytkowników sieci (uczniów i nauczycieli). Zaleca się, by na hejt nie odpowiadać w sposób emocjonalny, ważne jest też, by oczerniających informacji nie pozostawiać bez komentarza. Poniżej przedstawiono tabelę, której treści zostały zmodyfikowane (oryginalna tabela-źródło)[139] tak, by odnosiły się do podejmowania działań przez nauczycieli i uczniów.

Hejt	Polecana reakcja
Zarzuty nietaktowne lub zaczepne (np. zarzuty wobec osoby)	Podanie jasnych argumentów na naszą korzyść
Niemerytoryczne i obraźliwe treści bazujące na oszczerstwie lub domniemaniach np. pomówienia)	Warto podać twarde dowody przeczące zarzutom, sprawdzić regulamin serwisu, zgłosić obraźliwy komentarz do administratora
Powielanie obraźliwego komentarza na wielu forach, serwisach	Nie wchodzić w dyskusję z hejterem, odnieść się do tego na swojej stronie FB lub Twitterze
Nieuzasadniony hejt, który się nasila	Przestępstwo, które można ścigać

Umiejętności komunikacyjne wymagają jednak treningu. Warto, by nauczyciel, pedagog lub psycholog objął uczniów zajęciami rozwijającymi te kompetencje. Niestety sama analiza sytuacji agresywnej nie wystarczy, potrzebne jest nauczenie się zasad postępowania i reagowania.

Praktyczny przykład procedur przeciwko cyberagresji w szkole

W 2018 r. ukazała się publikacja pt. *Standard bezpieczeństwa online placówek oświatowych* przygotowana przez zespół autorów w ramach zleconego przez Ministerstwo Cyfryzacji i Administracji zadania publicznego „Działania na rzecz bezpiecznego korzystania z intenetu"

[139] Zob. https://nowymarketing.pl/a/21720,hejt-nieuczciwej-konkurencji (dostęp: 3.05.2020).

realizowanego przez Fundację Odkrywców Innowacji oraz Fundację Drabina Rozwoju. Publikację przygotowywał zespół ekspertów z NASK i WSP im. Janusza Korczaka pod redakcją Joanny Lizut i Agnieszki Wrońskiej[140].

W 2017 r. w ramach prac Departamentu Wychowania i Kształcenia Integracyjnego Ministerstwa Edukacji Narodowej udostępniono zbiór rekomendacji i wytycznych skierowanych do dyrektorów szkół i organów prowadzących szkoły zatytułowany *Bezpieczna Szkoła. Procedury reagowania w przypadku wystąpienia wewnętrznych i zewnętrznych zagrożeń fizycznych w szkole*[141]. Na podstawie tego dokumentu szkoły mogą wypracowywać wewnętrzne rozwiązania bezpieczeństwa cyfrowego.

Poniżej zaprezentowano fragment przywołanego dokumentu odnoszący się do cyberzagrożeń. Materiał ten autorki książki zdecydowały się zacytować w znacznej części ze względu na wartość poznawczą i praktyczną.

PROCEDURY REAGOWANIA W PRZYPADKU WYSTĄPIENIA W SZKOLE ZAGROŻEŃ BEZPIECZEŃSTWA CYFROWEGO

1. W przypadkach wystąpienia incydentu naruszenia bezpieczeństwa cyfrowego, działania szkoły cechować powinna otwartość w działaniu, szybka identyfikacja problemu – określenie szkodliwych lub niezgodnych z prawem zachowań – i jego rozwiązywanie adekwatnie do poziomu zagrożenia, jakie wywołało w szkole.

Warto przy tym podkreślić, iż nie istnieje „złota recepta", którą zastosować można we wszystkich przypadkach wystąpienia zagrożeń spowodowanych przez uczniów. Dyrektorzy i nauczyciele muszą uwzględniać kontekst indywidualnych przypadków, a także ich szkolne i środowiskowe tło i reagować adekwatnie do poziomu odpowiedzialności.

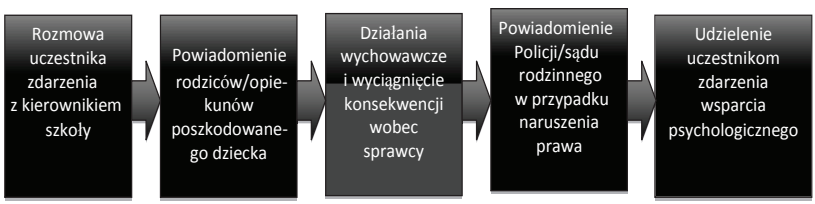
---

[140] Publikacja jest dostępna pod adresem: https://akademia.nask.pl/publikacje/ost_Standard_bezpieczenstwa_online_placowek_oswiatowych.pdf.

[141] *Bezpieczna Szkoła. Procedury reagowania w przypadku wystąpienia wewnętrznych i zewnętrznych zagrożeń fizycznych w szkole*, https://www.cyfrowa-szkola.info/wp-content/uploads/2017/10/Procedury-reagowania-w_2.pdf (dostęp: 3.05.2020).

Na każdą procedurę reakcji na wystąpienie danego typu zagrożenia cyberbezpieczeństwa w szkole muszą składać się działania tego typu – podjęte przez dyrekcję szkoły oraz nauczycieli, pedagoga/psychologa szkolnego.

Standardową procedurę reakcji w przypadku wystąpienia zagrożenia bezpieczeństwa cyfrowego prezentuje następujący schemat:



Rysunek 7. Standard procedury reakcji na zagrożenie bezpieczeństwa cyfrowego

Źródło: Agnieszka Wrońska, Zuzanna Polak, NASK, 2015; www.sp12.szczecin.pl

Sprawców wszystkich rodzajów zagrożeń bezpieczeństwa cyfrowego w szkole należy objąć poniższymi działaniami:

1) Sprawca musi otrzymać od przedstawicieli szkoły komunikat o braku akceptacji dla działań, jakich dokonał. W trakcie takiej rozmowy uczeń powinien poznać możliwe skutki swojego postępowania, a także konsekwencje, jakie mogą zostać wobec niego wyciągnięte (np. wynikające z wewnętrznego regulaminu szkoły). W trakcie rozmowy sprawca powinien zostać wezwany do zaprzestania podejmowania podobnych działań w przyszłości, w tym usunięcia skutków swoich działań (np. publikacji na portalu społecznościowym). Sprawca powinien również zostać objęty odpowiednią pomocą psychologiczną/ /pedagogiczną w celu zrozumienia konsekwencji jego zachowania oraz zmianie postawy i dalszego postępowania. Jeśli sprawców jest więcej, to z każdym z nich należy rozmawiać osobno.
2) Należy zadbać o to, żeby osoba reprezentująca szkołę (psycholog, pedagog, wychowawca) ograniczała się do podjęcia interwencji, a nie wymierzała karę. Decyzję o tym, jaką karę wymierzyć sprawcy, powinna podejmować dyrekcja szkoły, po zasięgnięciu opinii kapituły. Ważne jest zatem oddzielenie osoby pedagoga, nawiązującego relację z uczniem, od organu wymierzającego karę.

Celem sankcji wobec sprawcy jest przede wszystkim: zatrzymanie jego działań i zapewnienie poczucia bezpieczeństwa ofierze oraz zmiana postawy sprawcy. Podejmując decyzję o sankcjach, należy wziąć pod uwagę:

- **rozmiar i rangę szkody** – np. czy w przypadku cyberprzemocy materiał został upubliczniony w sposób pozwalający na dotarcie do niego wielu osobom (określa to rozmiar upokorzenia, jakiego doznaje ofiara), czy trudno jest wycofać materiał z sieci itp.;
- **czas trwania prześladowania** – czy było to długotrwałe działanie, czy pojedynczy incydent;
- **świadomość popełnianego czynu** – czy działanie było zaplanowane, a sprawca był świadomy, że postąpił nagannie, np. czy wie, że wyrządza krzywdę koledze, jak wiele wysiłku włożył w ukrycie swojej tożsamości itp.;
- **motywację sprawcy** – należy sprawdzić, czy działanie sprawcy nie jest działaniem odwetowym w odpowiedzi na uprzednie doświadczenia sprawcy.

Aktywność wobec sprawcy powinna także obejmować rozmowę z jego rodzicami lub opiekunami prawnymi – powinni oni zostać poinformowani o zdarzeniu, zapoznani z materiałami oraz decyzją na temat dalszego postępowania ze sprawcą (np. na temat sankcji).

Jeśli sprawca pochodzi spoza szkoły, należy zapewnić bezpieczeństwo ofierze i poinformować ją (jej rodziców) o przysługujących jej prawach (np. zgłoszenie popełnienie przestępstwa na Policję). Jeśli sprawca jest z innej szkoły, należy rozważyć nawiązanie współpracy między placówkami i wspólne rozwiązanie kryzysowej sytuacji.

W przypadku wystąpienia większości rodzajów zagrożenia w szkole w procedurę reagowania zaangażowani muszą być: uczeń i jego rodzice lub opiekunowie prawni, dyrektor oraz pedagog lub psycholog.

2. Wyróżniono 9 podstawowych zagrożeń bezpieczeństwa cyfrowego w środowisku szkolnym, którym przypisano opracowane według jednego standardu opisu procedury reagowania[142].

---

[142] Tamże.

W tabeli zamieszczonej w *Aneksie* (zob. *Aneks*, tabela 1) zaprezentowano siedem wybranych zagrożeń, są to:

- dostęp do treści szkodliwych, niepożądanych i nielegalnych;
- cyberprzemoc;
- zagrożenie dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu;
- nawiązywanie niebezpiecznych kontaktów w Internecie – uwodzenie, zagrożenie pedofilią;
- seksting, prowokacyjne zachowanie i aktywność seksualna jako źródło dochodu nieletnich;
- bezkrytyczna wiara w treści zamieszczone w Internecie; umiejętność odróżniania treści prawdziwych od nieprawdziwych, szkodliwe reklamy;
- łamanie prawa autorskiego.

Wypracowane i zaprezentowane powyżej procedury są niezwykle cenne. Nauczyciele, stając w obliczu przemocy kierowanej w stosunku do uczniów, potrzebują jasnych instrukcji określających postępowanie zarówno wobec sprawców, jak i ofiar.

Ciekawe zalecenia praktyczne zawarto również w materiale edukacyjnym przeznaczonym dla ucznia i nauczyciela opracowanym w ramach projektu „Global Dignity Poland Hejt Nauczyciel". Ważne jest, by nauczyciel zwrócił uwagę na cechy ucznia, który może paść ofiarą hejtu. Zalicza się do nich: bycie nowym uczniem w klasie, nieśmiałość, słabe albo bardzo dobre wyniki w nauce, wyróżniający go ubiór, wygląd odróżniający go od innych (nadwaga, okulary), niepełnosprawność, brak przyjaciół lub kolegów w klasie, słabszy fizycznie. Wśród zachowań charakteryzujących uczniów, którzy doświadczają hejtu, wymienia się: apatyczność, agresywność lub płaczliwość, pogorszenie wyników w nauce, problemy z koncentracją, izolowanie się, opuszczanie lekcji, objawy psychosomatyczne, ból brzucha, głowy[143]. Głównymi przyczy-

[143] *Jak radzić sobie w sytuacji doświadczania przez ucznia zjawiska hejtu?*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjg2Nq8mMfnAhWl_CoKHVWABpMQFjAAegQIAxAB&url=https%3A%2F%2Fwww.nowaera.pl%2Fpobieranie-pliku-6cf4bb224f7ed5fe5771a5c384058c28.pdf&usg=AOvVaw3X_Y_B77aJN2Q1yLNIkhVK.

nami częstego braku informowania nauczyciela przez ucznia doświadczającego przemocy słownej są: poczucie winy, wstyd, nieprawidłowy obraz sytuacji i samego siebie, obawy przed reakcjami rówieśników (eskalacją agresji, odrzuceniem). W przytoczonym materiale zaleca się podejmowanie następujących działań:

- rozmowa z uczniem – poinformowanie ucznia o zaobserwowanych sytuacjach („widzę, że ostatnio…");
- wyrażenie odczuć – „niepokoję się, czy ktoś zrobił coś…";
- wysłuchanie relacji ucznia (tu zaleca się stosować techniki aktywnego słuchania, parafrazy, rozumienie, dostrzeganie emocji i ich odzwierciedlanie);
- zwrócenie uwagi na to, że wypowiedź danej osoby (hejtera) jest jej opinią; w wypowiedzi należy podać motywy i przyczyny agresji tej osoby (np. doświadczenie przemocy w domu);
- zaproponowanie pomocy, należy poprosić ucznia o poinformowanie rodziców;
- zgłoszenie sprawy na policję.

Wobec sprawcy hejtu proponuje się następujące działania:

- rozmowa ukierunkowana na próbę wyjaśnienia powodów takiego zachowania (hejtu);
- poinformowanie ucznia o konsekwencjach jego czynu;
- odwołanie do emocji dziecka, które doznało hejtu (wyjaśnienie skutków hejtu, propozycja wspólnego zastanowienia się nad zadośćuczynieniem ofierze przemocy).

W procesie rozwiązywania problemu (jakim jest przemoc słowna i hejt) przez nauczyciela istotne są: bycie obecnym, aktywne słuchanie, nazywanie uczuć, nazywanie potrzeb drugiego człowieka[144].

Na zakończenie warto zwrócić uwagę na kilka projektów profilaktycznych i kampanii społecznych przeciwko hejtowi zamieszczonych w Internecie, są to:

- akcja „Przytul hejtera": http://www.przytulhejtera.pl/;
- kampania „Stop mowie nienawiści": http://stopmowienienawisci.pl/;

[144] Tamże.

- projekt #jestnaswiecej: https://jestnaswiecej.pl/;
- kampania „Nie hejtuję – reaguję": https://fdds.pl/nie-hejtuje-reaguje-nowa-kampania-fundacji-dajemy-dzieciom-sile-przeciwko-cyberprzemocy-i-mowie-nienawisci/;
- kampania Amnesty International: https://amnesty.org.pl/kampanie/nienawisc/;
- kampania „H(ej!)t to słabość": http://porebaw.niedzwiedz.pl/upload/File/nauczyciela/Materia%C5%82y%20dydaktyczne-%20hejt%20to%20s%C5%82abo%C5%9B%C4%87.pdf;
- projekt „Mow@ Miłosci": http://klamra.org/projekty/prawa-czlowieka/mowamilosci/;
- *Jak zamalowywać hejty. Podręcznik* (podręcznik PDF): https://docplayer.pl/6664716-Jak-zamalowywac-hejty-podrecznik.html;
- komiks przeciwko mowie nienawiści: http://www.mowanienawisci.info/wp-content/uploads/2016/11/komiks-3Z.pdf;
- *Nieobojętnik antyprzemocowy*: http://solidarnizuchodzcami.pl/wp-content/uploads/2015/10/Nieobojetnik.pdf.

Rozdział 3

Hakerstwo

Narodziny hakerstwa

Wzrost znaczenia cyberprzestrzeni w życiu społeczeństwa przyniósł wiele zmian na różnych płaszczyznach. Firmy zyskały nowe kanały dystrybucji, urzędy uprościły liczne procedury, jak również przeniosły możliwość aplikowania wniosków do sieci. Szkoły zaczęły korzystać z nowych form e-kształcenia. W Internecie możemy zrobić zakupy, zagrać na giełdzie, odbyć sesje psychoterapeutyczne, a nawet potrenować z fizjoterapeutą. Ta bogata przestrzeń, odwzorowująca życie realne, określana jako międzysieć (*inter* – „między", *net* – „sieć"), otworzyła nowe możliwości osobom nieuczciwym. W konsekwencji pojawili się tam także włamywacze i złodzieje. W sieci mamy do czynienia z osobami rozpowszechniającymi *fake news*, pozyskującymi dostęp do cudzych danych, przywłaszczającymi sobie wiele dóbr należących do innych. Ludzie działający nielegalnie lub na pograniczu prawa są rozpoznawani przez ogół społeczności jako hakerzy.

Analiza historii hakerstwa wykazuje, że środowisko to nie zawsze wywoływało negatywne skojarzenia oraz miało tak pejoratywne konotacje. Pierwsi hakerzy, jak opisuje Jon Ericson, wywodzili się z klubu modelarstwa kolejowego funkcjonującego przy Massachussets Institute of Technology. Na przełomie lat 50. i 60. XX w. na rzecz zgrupowania przekazane zostało stare oprzyrządowanie telefoniczne. Posłużyło ono do skonstruowania centrali pozwalającej na sterowanie różnymi częściami torów, co było możliwe dzięki podpinaniu się do właściwej sekcji. Opisana forma wykorzystania urzą-

dzenia była określana mianem hackingu[1] (stąd pochodzi angielskie słowo *hacker*).

W MIT w ówczesnym czasie instalowano pierwsze komputery współdzielone. Należy podkreślić, że poprawna obsługa wspomnianych urządzeń wymagała licznych zabiegów, w tym synchronizacji pracy użytkowników, podziału zadań oraz czasu korzystania z urządzenia. Dla wielu osób forma ta stała się pierwowzorem i głównym wyznacznikiem towarzyszącej do dziś potrzeby dzielenia się wiedzą. Jak podkreśla Atshushi Akera, idea ta w przeszłości była podsycana sytuacją związaną z zimną wojną oraz rosnącym w jej kontekście znaczeniem techniki komputerowej[2].

Innym czynnikiem wpływającym na środowisko hakerów był gwałtowny rozwój przemysłu komputerowego, który nastąpił na przełomie lat 70. i 80. XX w. Szczególną rolę w tym kontekście odegrali członkowie klubu Homebrew Computer założonego w marcu 1975 r. Spotkania intelektualne działaczy wsparły rozwój rewolucji mikrokomputerowej i powstanie kompleksu przemysłowego Doliny Krzemowej. Z szeregów HCC wyłoniło się kilku znanych hakerów, m.in. założyciele Apple Computer[3]. Specjaliści zaczęli konstruować prywatne jednostki, a także analizować zmieniające się systemy komputerowe. Z czasem ich zainteresowanie skierowało się na zagadnienia związane z siecią telefoniczną. Grupie tej przypisano miano phreakerów. Nielegalne działania zaczęły być kontrolowane i poddawane sankcjom karnym.

Następna istotna zmiana dotyczyła przenikania myśli hakerskiej do kultury informatyków Doliny Krzemowej[4]. W środowisku widoczna była pasja i zaangażowanie przejawiające się w wielogodzinnych mara-

---

[1] J. Ericson, *Hacking. Sztuka penetracji*, tłum. M. Rogóż, Helion, Gliwice 2008, s. 14.

[2] A. Akera, *Calculating a natural world. Scientists, engineers, and computers during the rise of U.S. cold war research*, MA: MIT Press (Inside technology), Cambridge 2007.

[3] The Homebrew Computer Club, *Computer History Museum*, https://www.computerhistory.org/revolution/personal-computers/17/312 (dostęp: 20.05.2019).

[4] S. Levy, *Hackers. Heroes of the computer revolution. 1st (25th anniversary edition)*, rozdział 2, O'Reilly, Beijing–Cambridge, UK–Farnham–Koeln–Sebastopol–Tokyo 2010.

tonach programowania. Pracujący w firmach specjaliści zaczęli powoli zapominać o otwartości kodu i idei dzielenia się wiedzą, którą osnuły tajemnice przemysłowe zatrudniających ich firm. Opracowywanie oraz dystrybucja gier komputerowych czy też specjalistycznego oprogramowania stały się intratnym biznesem, wpływając na podział wewnątrz środowiska hakerów. Dysonans objął dwie grupy – współpracującą z korporacjami oraz zwalczającą je.

Wraz z upowszechnianiem się sieci komputerowych oraz Internetu hakerzy zaczęli koncentrować się na idei otwartego oprogramowania[5]. Projekty inicjowane w ramach filozofii *open source* stawały się coraz bardziej popularne, łącząc tym samym uczestników z różnych rejonów świata.

Pierwsza w historii konferencja zrzeszająca hakerów odbyła się w 1984 r. w Kalifornii (hrabstwo Marin). W spotkaniu wzięło udział około 150 uczestników[6]. Z czasem spotkania o charakterze edukacyjnym stawały się coraz bardziej popularne. Cykliczność wielu z nich ułatwiała nawiązywanie trwałych relacji oraz współpracę środowiska zrzeszającego grupę osób pochłoniętych problematyką szeroko rozumianego zastosowania sprzętu komputerowego. Do obecnie popularnych konferencji należą m.in. DEFCON w Las Vegas[7], PumpCon w Filadelfii[8], H.O.P.E w Nowym Jorku[9], THOTCON w Chicago[10]. To cenione w środowisku miejsca wymiany informacji, doświadczeń oraz elementów kultury hakerskiej.

---

[5] G.E. Coleman, *Coding freedom. The ethics and aesthetics of hacking*, Princeton University Press, Princeton–New York 2013, s. 64–88.

[6] F. Turne, *From counterculture to cyberculture. Stewart brand, the Whole Earth Network, and the rise of digital utopianism*, University of Chicago Press, Chicago 2006, s. 132.

[7] Defcon, https://www.defcon.org/?ref=infosec-conferences.com (dostęp: 15.07.2019).

[8] Pumpcon, https://www.pumpcon.org/?ref=infosec-conferences.com (dostęp: 15.07.2019).

[9] Hope, https://viii.hope.net/ (dostęp: 15.07.2019).

[10] THOTCON, https://thotcon.org/?ref=infosec-conferences.com (dostęp: 15.07.2019).

Wśród pozostałych, wartościowych źródeł wiedzy wskazuje się:
- książki opracowane oraz polecane przez innych hakerów;
- czasopisma elektroniczne o charakterze informatycznym;
- fora poświęcone specjalistycznej tematyce;
- analizę kodów źródłowych gotowych programów;
- czaty internetowe (IRC) itp.[11]

Czy to był haker?

Pytania o hakerów oraz ich działania coraz częściej pojawiają się w codziennej pracy pedagogów. Stąd tak ważne staje się nieustanne dokształcanie i uzupełnianie wiedzy oraz śledzenie bieżących trendów, również w środowisku nauczycielskim. Szczególnie że Internet i związane z nim aktywności towarzyszą im na każdym kroku, począwszy od planowania zajęć, poprzez sprawdzenie obecności, przeprowadzenie lekcji, testów wiedzy, a skończywszy na przygotowaniu świadectw[12].

Słowo „haker" w powszechnym użyciu ma niezmiernie pejoratywne znaczenie. Zgodnie ze Słownikiem języka polskiego PWN to „osoba włamująca się do sieci i systemów komputerowych"[13], „osoba, która nielegalnie uzyskuje dostęp do informacji i czasami sabotuje informacje w systemie komputerowym"[14]. Dariusz Doroziński podkreśla, że zazwyczaj haker jest utożsamiany z „przestępcą, niebezpiecznym maniakiem komputerowym, którego dla dobra ludzkości należałoby zamknąć w więzieniu"[15]. Dla wielu osób to „komputerowy włamywacz i przestępca […], który korzystając ze zdalnych środków dostępu, do-

---

[11] S. Bratus, *Hacker curriculum: How hackers learn networking*, „IEEE Distributed Systems Online" 2007, 8(10), s. 1–7.

[12] K. Majewska, *The electronic register in Polish schools: Studies from the level of early school education*, w: D. Siemieniecka (ed.), *Virtuality and education: Future prospects*, Wydawnictwo Adam Marszałek, Toruń 2019, s. 93–111; taż, *Modern educational tools in the teacher's work*, „The New Educational Review" 2018, 51(1), s. 125–135.

[13] *Haker*, https://sjp.pwn.pl/slowniki/haker.html (dostęp: 24.07.2019).

[14] *Hacker*, https://www.merriam-webster.com/dictionary/hacker (dostęp: 24.07.2019).

[15] D. Doroziński, *Hakerzy. Technoanarchiści cyberprzestrzeni*, Helion, Gliwice 2001, s. 17.

konuje włamań do systemów informatycznych dla zabawy bądź w innym celu”[16]. Nie można jednak bagatelizować faktu, że hakerzy nie są podrzędnymi rzezimieszkami. To grupa inteligentnych, wyspecjalizowanych w konkretnej dziedzinie profesjonalistów, „ekspertów w programowaniu i rozwiązywaniu problemów z komputerem”[17]. Z tym terminem identyfikuje się również „entuzjastycznego użytkownika komputera”[18], co nadaje mu pozytywnego zabarwienia. W raporcie Hackerone 2016 grupie tej przypisuje się umiejętności techniczne oraz ciekawość umożliwiającą przekraczanie granic technologii. To zrzeszenie nastolatków, profesjonalistów oraz emerytów mieszkających w różnych zakątkach świata oraz będących przedstawicielami różnych zawodów[19]. Charakter terminu jest zatem niezmiernie pluralistyczny.

Mimo silnie odznaczającej się inkongruencji należy podkreślić, że każda z przytoczonych powyżej definicji jest właściwa. Środowisko hakerów można zatem podzielić na dwie heterogeniczne grupy. Pierwszą z nich – będącą idealnym przykładem dysharmonii zachodzącej między potęgą ludzkiego umysłu a siłą charakteru i wewnętrzną potrzebą bycia uczciwym człowiekiem. Powyższy tok myślenia oddają słowa ukazujące hakerstwo jako „poczucie kontroli, adrenalinę, wiedzę, posiadanie czegoś, czego nie powinieneś mieć”[20]. Druga grupa służy walce z niemoralnymi oszustami i złodziejami działającymi w przestrzeni Internetu, co odzwierciedla stwierdzenie: „Haker jest osobą, która poszła dalej niż korzystanie z komputera w celu przetrwania (»Zarabiam na życie, pisząc oprogramowanie«). W ten sposób powstaje coś takiego jak Linux. Nie martwisz się o wielki zarobek. Powód, dla którego hakerzy

---

[16] A. Makosz, *Haker*, „Gazeta Prawna”, https://www.gazetaprawna.pl/encyklopedia/prawo/hasla/332774,haker.html (dostęp: 24.07.2019).

[17] *Hacker*, https://www.merriam-webster.com/dictionary/hacker (dostęp: 24.07.2019).

[18] *Hacker*, https://www.lexico.com/en/definition/hacker (dostęp: 24.07.2019).

[19] Hackerone, *2016 Bug Bounty Hacker Report*, s. 3, https://www.hackerone.com/sites/default/files/2017-05/HackerOne%202016%20Bug%20Bounty%20Report.pdf (dostęp: 25.07.2019).

[20] J. Littman, *The fugitive game: Online with Kevin Mitnick*, Little, Brown and Co, New York 1996, s. 91.

od Linuxa coś robią, jest taki, że ich to interesuje"[21]. Starcie powyższych światopoglądów spowodowało, że w literaturze zwykło się przypisywać hakerom miano białych, szarych lub czarnych kapeluszy, zgodnie z pobudkami i efektem podejmowanych przez nich działań. Białe kapelusze, kojarzone z czystością, są utożsamiane z osobami wykorzystującymi swój potencjał w słusznych sprawach. Głównym celem ich działań jest weryfikowanie zabezpieczeń, odszukiwanie oraz wskazywanie luk w systemach komputerowych i w różnego typu aplikacjach[22]. Od pewnego czasu *white hats* mają również możliwość ukończenia szkolenia oraz uzyskania certyfikatu Certified Ethical Hacker, potwierdzającego umiejętność weryfikowania bezpieczeństwa systemów komputerowych[23]. Szare kapelusze dokonują włamań i kradzieży danych w celu wykazania się swoimi umiejętnościami. To środowisko funkcjonuje zazwyczaj w granicach prawa. Niekiedy szare kapelusze hakują w celu znalezienia luk w systemie, zabezpieczenia ich, a następnie uzyskania korzyści z odstąpienia wypracowanych zabezpieczeń administratorowi. Czarne kapelusze podejmują się głównie działań nieprawnych, w celu czerpania zysków[24]. Słownik synonimów określa hakera bliskoznacznymi pojęciami „kraker" (ang. *cracker*) lub „cyberprzestępca", „pirat komputerowy", „komputerowy przestępca"[25]. Nie jest to jednak całkowicie poprawne. Wielu autorów rozróżnia hakerów i krakerów, utożsamiając drugą z grup z negatywnymi i potępianymi pobudkami. Środowisko to często przypomina, że u podstaw hakerstwa leżały aktywności społecznie poprawne i nieszkodliwe dla otoczenia, odcinając się tym samym od nielegalnych i nieetycznych zachowań.

---

[21] L. Torvalds, *Prologue: What makes hackers tick? a.k.a. Unus's law*, za: R. Himanen, *The hacker ethic: A radical approach to the philosophy of business*, Random House, New York 2001, s. XV.

[22] T. Caldwell, *Ethical hackers: Putting on the white hat*, „Network Security" 2011, 7, s. 10–13.

[23] R. Messier, *CEH v10 certified ethical hacker study guid*e, John Wiley & Sons, New York 2019.

[24] W. Staszewski, *Brzytwa w czarnym kapeluszu*, https://www.newsweek.pl/polska/spoleczenstwo/biale-szare-i-czarne-kapelusze-wsrod-hakerow/z6b7t3g (dostęp: 2.08.2019).

[25] B. Wysocki, *Czy warto być hakerem?*, „EduAkcja. Magazyn Edukacji Elektronicznej" 2013, 1(5), s. 4.

Gdyby analizować definicję terminu pod kątem lotności umysłu i zdolności do samodzielnego tworzenia, należałoby zbiorowość hakerów podzielić na trzy, rozdzielne grupy:

- twórców, zajmujących wierzchołek piramidy;
- uczących się, ambitnych, młodych ludzi poznających tajniki świata hakerów;
- odtwórców, bezmyślnie kopiujących własność intelektualną innych osób.

Zaprezentowane powyżej podziały nie wyczerpują wszystkich możliwości. Analogicznych podgrup, w zależności od przyjętych kryteriów, można wyróżnić zdecydowanie więcej.

Aktywności podejmowane przez hakerów opisuje się jako hakerstwo, haking, cyberatak itd. Zgodnie z analizą historii dokonaną przez Stevena Levy'ego środowisko hakerskie kieruje się następującymi racjami:

- dostęp do komputera oraz sieci nie powinien być niczym ograniczany; to dzięki technologii pozyskuje się osobiste doświadczenie i wiedzę o świecie;
- wolność danych winna być niepodważalna;
- nie hierarchia, a decentralizacja świadczy o sile społeczeństwa;
- wartość hakera stanowi działanie, nie zaś płeć, rasa czy wyznanie;
- komputer pomaga tworzyć piękno i sztukę;
- komputery mogą zmienić życie na lepsze[26].

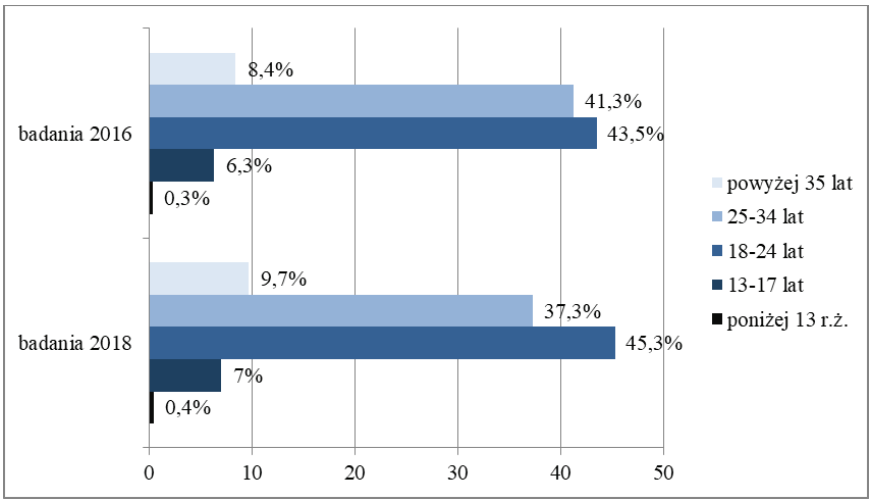
Kim jest typowy haker? Badania zrealizowane w 2018 r. na grupie 1698[27] respondentów wykazały, że ponad 90% hakerów ma mniej niż 35 lat[28].

---

[26] S. Levy, dz. cyt., s. 28.

[27] Badania miały charakter ankietowy. Grupa badawcza została wytypowana z ogółu hakerów zrzeszonych w organizacji The HackerOne, która dzieli się wiedzą, rozwiązuje problemy, ostrzega firmy przed potencjonalnymi zagrożeniami. W ramach swej działalności The HackerOne pomogła Departamentowi Obrony USA rozwiązać około 3 tys. luk w zabezpieczeniach, co znacznie poprawiło bezpieczeństwo pracy wielu departamentów w Stanach Zjednoczonych.

[28] Hackerone, *The 2018 Hacker Report*, 2018, s. 4, https://www.hackerone.com/sites/default/files/2018-01/2018_Hacker_Report_0.pdf (dostęp: 9.08.2019).



Wykres 1. Wiek hakerów, zestawienie wyników badań z 2016 i 2018 r.

Źródło: opracowanie własne na podstawie raportów *The 2018 Hacker Report* oraz *2016 Bug Bounty Hacker Report*.

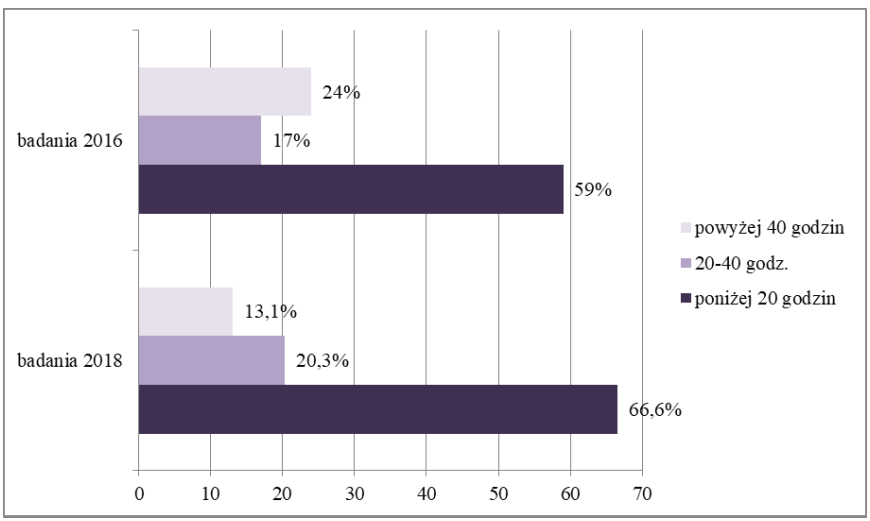
Przeprowadzone analizy wykazują, że 58% hakerów jest samoukami, a 44% to specjaliści z branży IT. Jednym z powodów, dla którego ludzie interesują się hakerstwem, jest chęć zarobkowania (13,1% badanych). Analiza danych ujawnia, że dobrzy specjaliści zarabiają średnio trzykrotnie więcej aniżeli inżynier oprogramowania w rodzimym kraju. Wyjątkiem są Indie, gdzie hakerzy mogą zarabiać nawet 16-krotnie więcej[29]. Dodatkowo działania hakerów są determinowane przez takie czynniki, jak: chęć nauki (14,7%) i sprostania wyzwaniom (14%), zabawa (14%), potrzeba udowodnienia swoich umiejętności, popisywanie się (3%), nadanie tempa rozwojowi kariery (12,2%), pomoc innym (8,5%), zmiana świata na lepsze (10%), ochrona i obrona (10,4%)[30]. Warto podkreślić, że w 2018 r. (w porównaniu z 2016 r.) główny czynnik, czyli chęć zysku, ustąpił pola potrzebie nauki[31].

[29] Tamże.

[30] Tamże, s. 24.

[31] Hackerone, *2016 Bug Bounty Hacker Report*, s. 10; *Kariera w cyberbezpieczeństwie*, „OUCH! Biuletyn Bezpieczeństwa Komputerowego", maj 2019, https://www.sans.org/sites/default/files/2019-04/201905-OUCH-May-Polish.pdf (dostęp: 23.08.2019).

Bez względu na osobiste pobudki najwięcej osób spędza na hakowaniu poniżej 20 godzin tygodniowo. Średnio co dziesiąta osoba poświęca tej pasji ponad 60 godzin tygodniowo[32].



Wykres 2. Liczba godzin poświęcona na hakowanie w ciągu tygodnia, zestawienie wyników badań z 2016 i 2018 r.

Źródło: opracowanie własne na podstawie raportów *The 2018 Hacker Report* oraz *2016 Bug Bounty Hacker Report*.

Najbardziej niebezpieczni, według 39% ankietowanych, są hakerzy, którzy mają dostęp do wewnętrznych informacji, np. na temat firmy; 20% specjalistów obawia się działań osób, które mają aktualną wiedzę oraz znają wcześniej niewykorzystywane luki; 17% lęka się działań grup wspieranych finansowo przez np. przestępczość zorganizowaną. Co dziesiąty specjalista z branży IT (11%) jako poważne zagrożenie wskazuje wysoce zaawansowane umiejętności ataku oraz działania sieci hakerów[33].

---

[32] Hackerone, *2016 Bug Bounty Hacker Report*, s. 10.

[33] Black Hat, *Portrait of an imminent cyberthreat*, 2017, s. 20, https://www.blackhat.com/docs/us-17/2017-Black-Hat-Attendee-Survey.pdf (dostęp: 29.07.2019).

Haker, kraker, phreaker

„Jeśli dana osoba hakuje w celach przestępczych, jest to przestępca, a nie haker”[34]. Gdyby te słowa nie były jedynie ideologią, a oddawały rzeczywisty stan rzeczy, wówczas charakterystyka poszczególnych podgrup związanych z hakerstwem byłaby o wiele prostsza i koncentrowałaby się jedynie na pozytywnych aspektach ich działania. Tymczasem wśród hakerów nietrudno znaleźć czarne charaktery, działające na niekorzyść pojedynczych jednostek, a nawet całego społeczeństwa.

Nie jest tajemnicą, że wraz z rozwojem technologii informacyjnych zaczęła zmieniać się specyfika i możliwości działań w Internecie. W konsekwencji słowo „haker” stało się zbyt ogólne, uniemożliwiając tym samym ukazanie odrębnych kierunków działania i filozofii leżącej u podstaw aktywności środowiska. W literaturze i w powszechnym użyciu obok białych, szarych i czarnych kapeluszy zaczęły pojawiać się zatem nowe formy hakerstwa i definicje je określające: kraker, haktywista, *script kiddie*, *green hat*, *red hat*, *blue hat*, cyberterrorysta, terrorysta informacyjny, haker rządowy, cyberżołnierz, haker „samobójca”, etyczny haker, phreaker (*phone freak* – z ang. dosłownie „telefoniczny maniak”).

Kraker (ang. *cracker* – „łamacz”) na podstawie słownika języka polskiego oznacza „osobę łamiącą zabezpieczenia aplikacji lub włamującą się do sieci komputerowych w celach niezgodnych z prawem”[35]. Swoją popularność termin ten zyskał w latach 90. ubiegłego stulecia i potocznie był utożsamiany z hakerstwem.

Haktywista (ang. *hactivist* – „haker aktywista”) zgodnie z literaturą uzyskuje nieautoryzowany dostęp do plików i sieci komputerowych w celach społecznych lub politycznych[36]. Wykorzystuje „cyberataki do promocji określonych postaw, wartości lub idei politycznych lub aby zwrócić uwagę opinii publicznej na określone problemy”[37]. Dorothy

---

[34] Hackerone, *2016 Bug Bounty Hacker Report*, s. 3.

[35] *Kraker*, https://sjp.pl/kraker (dostęp: 28.07.2019).

[36] T. Jordan, P. Taylor, *Hacktivism and cyberwars. Rebels with a cause?*, Routledge, London 2004.

[37] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.

Denning zaznacza, że „haktywizm obejmuje działania wykorzystujące techniki hakerskie przeciwko witrynie internetowej z zamiarem zakłócenia jej normalnego funkcjonowania, a nie spowodowania poważnych szkód”[38]. Najbardziej znaną i rozpoznawalną grupą haktywistów jest obecnie grupa Anonymous[39].

Script Kiddie (z ang. „skryptowy dzieciak, skryptowiec”) to niedoświadczony kraker, amator korzystający z gotowych programów lub skryptów, bez dogłębnego zrozumienia ich działania. Zajmuje najniższy szczebel w hierarchii hakerów[40]. Działania powyższej grupy często przyczyniają się do fali ataków społecznych wymierzonych w środowisko hakerów[41].

Green hat (z ang. „zielony kapelusz”) – haker nowicjusz, działający nad poprawieniem swoich umiejętności. *Od script kiddie* odróżnia go chęć poznawania, nauki oraz kontrolowania swoich działań. Ze względu na dużą liczbę zadawanych pytań jest krytykowany w środowisku hakerów[42].

Red hat (z ang. „czerwony kapelusz”) działa w słusznej sprawie, podobnie jak *white hat*. Od białych kapeluszy odróżnia go sposób działania – grupa ta nie buduje silnych zabezpieczeń, a w celu osłabienia czarnego kapelusza atakuje jego sprzęt. Z myślą o tym *red hats* używają wirusów, włamują się do komputerów itd. Aktywności są podyktowane chęcią sparaliżowania działań czarnych kapeluszy[43].

---

[38] D. Denning, *Activism, hacktivism and cyberterrorism. The internet as a tool for influencing*, w: J. Arquilla, D. Ronfeldt (eds.), *Networks and netwars. The future of terror, crime and militancy*, RAND Corporation, Santa Monica 2001, s. 241.

[39] G.E. Coleman, *Hacker, hoaxer, whistleblower, spy. The many faces of anonymous*, Verso, London–New York 2014.

[40] D. Melnichuk, *The hacker's underground. Handbook: Learn what it takes to crack even the most secure systems*, Createspace, Lexington 2008, s. 11.

[41] T. Jordan, *Hakerstwo*, tłum. T. Płudowski, Wydawnictwo Naukowe PWN, Warszawa 2011, s. 41–42.

[42] M. Hamza, N. College, *Cybercrime and security*, https://www.researchgate.net/publication/322086317_CyberCrime_and_Security (dostęp: 22.07.2019).

[43] Cybrary, *7 types of hackers you should know*, https://www.cybrary.it/0p3n/types-of-hackers/ (dostęp: 24.07.2019); Alpine Security, *Hacker hat colors: An inside look at the hacking ecosystem*, https://www.alpinesecurity.com/blog/hacker-hat-colors-an-inside-look-at-the-hacking-ecosystem (dostęp: 24.07.2019).

Blue hat (z ang. „niebieski kapelusz"), którego zaangażowanie podsyca pragnienie zemsty na firmie lub konkretnej osobie. „Ta grupa niekoniecznie jest znana z chęci uczenia się lub doskonalenia swoich umiejętności. Chcą tylko wiedzieć wystarczająco dużo, by zemścić się"[44].

Cyberterrorysta (ang. *cyberterrorist* – „cybernetyczny terroryzm") – termin ten narodził się w latach 80. XX w. w Institute for Security and Intelligence w Californii[45]. Cyberterroryzm identyfikuje się z pozyskiwaniem nielegalnego dostępu do sieci komputerowych firm, agencji rządowych itp. w celu niszczenia danych[46]. Poczynania cyberterrorystów są utożsamiane z sabotażem przez Internet[47] lub wykorzystaniem technologii komputerowych do ataków terrorystycznych[48]. Zgodnie ze wskazaniami Ministerstwa Spraw Zagranicznych najbardziej zagrożone ruchem cyberterrorystów są rządowe strony internetowe, bazy bankowe oraz infrastruktura krytyczna[49].

Terrorysta informacyjny (ang. *information terrorist*) – zgodnie z definicją zaproponowaną w 1997 r. przez Matthew G. Devosta, Briana K. Houghtona oraz Neala Allena Pollarda to osoba, która „umyślnie nadużywa cyfrowego systemu informacyjnego, sieci lub innych komponentów w celu osiągnięcia celu, który wspiera lub ułatwia kampanię lub akcję terrorystyczną"[50]. Na podstawie raportu NATO z 2001 r. terrorysta informacyjny jest utożsamiany z cyberterrorystą – „wyko-

---

[44] Alpine Security, dz. cyt.

[45] M. Conway, *Cyberterrorism: The story so far*, „Journal of Information Warfare" 2003, 2(2), s. 36.

[46] Tamże.

[47] H. Sher, *Cyberterror should be international crime – Israeli minister*, „Newsbytes" 2000, November 10.

[48] R. Westphal Jr (ed.), *War and virtual war. The challenges to communities*, Oxford, United Kingdom 2003.

[49] Rzeczpospolita Polska, Ministerstwo Spraw Zagranicznych, *Zapobieganie i zwalczanie terroryzmu*, https://www.msz.gov.pl/pl/polityka_zagraniczna/polityka_bezpieczenstwa/zwalczanie_terroryzmu_miedzynarodowego/zapobieganie_i_zwalczanie_terroryzmu/page_30058 (dostęp: 22.08.2019).

[50] M. Devost, B. Houghton, N. Pollard, *Information terrorism: Political violence in the information age*, „Terrorism and Political Violence" 1997, 9(1), s. 75.

rzystuje system informatyczny lub technologię komputerową jako broń lub cel”[51].

Haker rządowy (ang. *government hacker*), jego aktywność w Internecie, w tym kontrolowanie wiadomości oraz danych, a także zamierzone powodowanie szkód w konkretnych jednostkach, ma na celu ochronę interesów państwa. Często zaznacza się, że hakowanie przez rząd ma na celu inwigilację lub zebranie danych wywiadowczych oraz że zagraża prawom człowieka[52].

Cyberżołnierz (ang. *cyber soldier*) – wojskowy, który do walki z wrogiem wykorzystuje komputery lub Internet[53]. Zadaniem tej grupy jest obrona cyfrowych zasobów armii, a także zakłócanie łączności radiowej, satelitarnej itd. w razie potrzeby.

Haker „samobójca” (ang. *suicide hacker*) działa w celu zniszczenia konkretnych obiektów, podobnie jak zamachowiec samobójca.

Etyczny haker (ang. *ethical hacker*) – jego plany i filozofia funkcjonowania są oparte na dobrych intencjach[54]. Często do kategorii etycznych hakerów zalicza się białe kapelusze, które działają w imię wyższego dobra i w zgodzie z ideą niesienia pomocy. Etyczne hakowanie niesie ze sobą wiele korzyści, m.in. pomaga w ochronie kluczowych systemów, sieci i kont przed złodziejami danych, ułatwia utrzymanie kontroli nad informacjami, wspiera wykrywanie niedoskonałości i luk w systemie, przyczynia się do podniesienia bezpieczeństwa sprzętowego oraz zmniejsza ryzyko ataków w niego wymierzonych[55].

---

[51] M. Mates, *Technology and terrorism*, https://www.tbmm.gov.tr/ul_kom/natopa/raporlar/bilim%20ve%20teknoloji/AU%20121%20STC%20Terrorism.htm (dostęp: 22.08.2019).

[52] S. Herpig, *Government hacking, global challenge*, https://www.stiftung-nv.de/sites/default/files/government_hacking_akt.feb_.pdf (dostęp: 23.08.2019); *A human rights response to government hacking*, https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf (dostęp: 23.08.2019).

[53] *Cyber soldier*, https://dictionary.cambridge.org/dictionary/english/cyber-soldier (dostęp: 23.08.2019).

[54] A. Maurushat, *Ethical hacking*, University of Ottawa Press, Ottawa 2019.

[55] A. Ushmani, *Ethical hacking*, „International Journal of Information Technology” 2018, 4(6).

Phreaker – włamuje się do systemów telefonicznych w celu prowadzenia darmowych rozmów lub podejmowania zaplanowanych działań[56].

Wyróżnione grupy systematyzują środowisko hakerów, aczkolwiek należy mieć na uwadze to, że z czasem zaproponowany podział okaże się zbyt ogólny, a w konsekwencji nieaktualny.

Skutki działania hakerów

Hakerzy i ataki na szkołę

Oczywiście realia i oprogramowanie szkolne nie są głównym celem ataków hakerskich, co nie oznacza, że przestrzeń ta jest całkowicie wolna od zagrożeń. Ryzykowne zachowania nauczycieli oraz kadry administracyjnej mogą wywołać zamieszanie w klasie, w szkole, a nawet w całym środowisku związanym z placówką.

Nietrudno przewidzieć, ile problemów szkole mógłby stworzyć dostęp osoby nieuprawnionej do Systemu Informacji Oświatowej. Powyższe sprawozdanie w przestrzeni internetowej placówki są zobowiązane składać corocznie. Wysiłek związany z uzupełnieniem danych jest znaczny, co wynika z konieczności wprowadzenia do systemu informacji na temat szkoły, każdego ucznia oraz nauczyciela (m.in. imienia, nazwiska, daty urodzenia, numeru PESEL, informacji o niepełnosprawności). Dane zgromadzone w SIO stanowią podstawę do naliczenia części oświatowej subwencji ogólnej na dany rok. Istotne jest zatem dotrzymanie terminów oraz wprowadzenie danych zgodnych ze stanem faktycznym. Pominięcie lub niewykazanie pewnych faktów skutkuje obniżeniem dopłaty, zaś na podstawie ustawy o dochodach jednostek samorządu terytorialnego w przypadku źle uzupełnionego wniosku (Dz.U. z 2018 r., poz. 1530 z późn. zm.) szkole nie przysługuje prawo do zwiększenia części oświatowej subwencji ogólnej (art. 37 ust. 4). W sytuacji, gdy ustalona dla jednostki samorządu terytorialnego część oświatowa subwencji ogólnej jest wyższa od należnej, minister spraw finansów publicznych ma prawo zmniejszyć o odpowiednią

[56] D. Doroziński, dz. cyt., s. 20.

kwotę część oświatową subwencji ogólnej (art. 37 ust. 1)[57]. Włamanie się do systemu podyktowane złymi pobudkami umożliwiłoby zatem częściową lub całkowitą zmianę danych, a nawet usunięcie wniosku, co mogłoby zakończyć się poważnymi konsekwencjami. Innym równie istotnym zagrożeniem jest kradzież danych, do której może przyczynić się nienależyte zabezpieczenie różnego typu baz osobowych znajdujących się w szkole. Tymczasem art. 82 ust. 1 stanowi, iż „każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę"[58].

Włamanie do dziennika elektronicznego, obok kradzieży danych, może dodatkowo skutkować problemami dotyczącymi wystawienia niewłaściwej oceny. W historii kilkuletniej obecności dziennika elektronicznego w szkole niejednokrotnie odnotowywano włamania oraz nadużycia związane z nielegalnym dostępem do e-dziennika. Przykładem może być szkoła podstawowa w Złotowie, w której to trzech uczniów, niezgodnie z prawem, weszło w posiadanie hasła dostępowego do konta nauczyciela i zmieniło dane w systemie teleinformatycznym[59]. Włamania do systemu dokonał również 19-letni uczeń szkoły w Wyszogrodzie. „Po zebraniu materiału dowodowego okazało się, że chłopak logował się na stronę dziennika, wykorzystując serwery na terenie innych państw europejskich"[60]. Inny z uczniów „stworzył replikę strony internetowej szkoły, później wkleił odpowiedni skrypt, na końcu – wysłał odnośnik do linku do jeszcze innej strony internetowej. Kolej-

[57] Strona główna Sejmu Rzeczpospolitej Polskiej, *ISAP – Internetowy System Aktów Prawnych*, http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001530 (dostęp: 13.09.2019).

[58] Portal o unijnym rozporządzeniu o ochronie danych osobowych, Artykuł 82 – Prawo do odszkodowania i odpowiedzialność, https://gdpr.pl/baza-wiedzy/akty-prawne/interaktywny-tekst-gdpr/artykul-82-prawo-do-odszkodowania-i-odpowiedzialnosc (dostęp: 13.09.2019).

[59] M. Pieczyńska-Chamczyk, *Uczniowie sami sobie poprawili oceny w dzienniku*, https://www.asta24.pl/2017/06/20/uczniowie-poprawili-oceny-dzienniku (dostęp: 13.09.2019).

[60] INTERIA.PL/Policja, https://fakty.interia.pl/polska/news-wlamal-sie-do-elektronicznego-dziennika-i-poprawil-oceny,nId,2251580#utm_source=paste&utm_medium=paste&utm_campaign=firefox (dostęp: 14.09.2019).

ne zabiegi pozwoliły mu uzyskać dostęp do hasła jednego z nauczycieli. Wykorzystał je, by zmienić oceny w dzienniku internetowym"[61]. Powyższych historii, różniących się między sobą datą popełnionego przestępstwa, wiekiem dzieci czy miejscem zdarzenia, jest niezmiernie wiele. Niemniej jednak każda z nich świadczy o istniejącym już problemie i realnych zagrożeniach. Niebezpieczeństwo, które z jednej strony dotyczy szkoły, z drugiej nie jest obojętne dla uczniów, którzy być może nie w pełni świadomi konsekwencji podejmowanych działań mogą całkowicie przekreślić sobie szansę na dalsze kształcenie i uczciwe życie.

Na forach internetowych bez problemu można znaleźć dyskusje na temat kradzieży haseł, zawirusowania komputerów szkolnych, zdobycia danych do logowania itp. O wskazówki i porady pytają przede wszystkim osoby młode, np. (pisownia oryginalna):

> Witam
> Kilka miesięcy temu dowiedziałem sie ze moja szkoła założy dziennik elektroniczny […]
> Stad ode mnie do Was pytanie.
> – Co lub jakim sposobem narobić największych szkód?
> Myśleliśmy już żeby wysłać na email dyrektora plik autostart z formatem dysku c bez pytania albo żeby wysłać jakiś plik typu „praca na informatykę" w której będzie robak żeby zdobyć hasła.
> A teraz wyjaśnię trochę sprawę – W naszej szkole nauczycielem informatyki jest dyrektor (uczy nas w 2 klasie liceum jak otworzyć folder lub jak znaleźć ukryty plik na komputerze przez „uruchom") Gdy zadaje nam pracę domową sprawdza ją u siebie w gabinecie na najlepszym kompie w szkole (wnioskujemy z kolegą, że na tym komputerze będzie znajdowała się cała baza danych tego dziennika) otwiera wszystkie pliki bo się na nich nie zna.
> Proszę Was o pomoc napiszcie, jak możecie, czy to dobry pomysł wysyłać mu format czy może powinniśmy poświecić trochę czasu i wymyślić coś lepszego

[61] A. Smogulecka, K. Sklepik, *Poznań: młody haker zmieniał szkolne oceny*, https://gloswielkopolski.pl/poznan-mlody-haker-zmienial-szkolne-oceny/ar/376527 (dostęp: 14.09.2019).

P.S. Nie myślcie tylko, że jestem jakimś dzieckiem z gimnazjum, któremu zależy, żeby rodzice nie sprawdzili złych ocen. Bawię się z kumplem w takie drobne szperanie w nie swoim komputerze wiec mniej więcej wiem co jest 5. :P
pozdrawiam
Hate[r]

[…]

A czym lub jakim programem, wirusem mogę narobić największych szkód na komputerze?

[…]

Najprościej byłoby zainstalować keyloggera na komputerze nauczyciela, gdyż na każdej lekcji nauczyciel loguje się do dzienniczka, mając jego login i hasło możesz robić wszystko to co on, czyli np. zmieniać oceny. To jednak tworzy kolejny problem, w dzienniczkach elektronicznych istnieją w pewnym sensie prawa dostępu, niektórzy nauczyciele mogą się logować tylko z jednego komputera, inni z całej sieci wewnętrznej a jeszcze inni z dowolnego komputera na świecie, dlatego musisz wiedzieć komu kradniesz hasło to i będziesz wiedział czy możesz się zalogować z komputera w klasie, szkole (np. bibliotece) lub we własnym domu. Różni nauczyciele także mają różne prawa do działań w dzienniczku, wychowawca klasy np. ma prawo dostępu do wszystkich ocen swojej klasy, podczas, gdy zwykli nauczyciele mają dostęp tylko do ocen wystawionych przez samych siebie[62].

Biorąc pod uwagę, że dostęp do wysokiej jakości komputerów oraz Internetu jest coraz bardziej powszechny, a dzieci coraz mniej kontrolowane przez rodziców i nierzadko samotne w swoich aktywnościach, warto zaalarmować, że liczba epizodów o podobnym zabarwieniu może przybierać na sile.

Oczywiście zdarzeń z udziałem hakerów w przestrzeni szkolnej może być znacznie więcej. Szkoły dysponujące platformą e-learningową mogą zostać zaatakowane, a zamieszczone dane – podmienione,

[62] Hacker.com.pl, https://haker.com.pl/threads/21204-Dziennik-elektroniczny (dostęp: 14.09.2019).

usunięte, wykradzione itd. Uczniowie z konta pocztowego szkoły mogą zostać poinformowani o odwołaniu zajęć, zmianie planu lekcji, zaś rodzice zaproszeni na fikcyjną wywiadówkę. Źródłem nadużyć może stać się również nielegalnie pozyskany dostęp do systemu teleinformatycznego związanego z monitoringiem placówki.

W konsekwencji, w celu zabezpieczenia placówki przed najbardziej popularnymi atakami, rekomenduje się uwrażliwienie kadry na wiele zagrożeń związanych z Internetem oraz dokształcanie pozwalające na względnie bezpieczne korzystanie z sieci. Pożądana jest również instalacja oprogramowania antywirusowego.

Przestrzeń domowa wolna od hakerów?

Co może spotkać mnie ze strony hakera? Odpowiedź na to pytanie, zwłaszcza laikom, wydaje się niesłychanie prosta. Zaznacza się, że haker może włamać się do komputera, może wykraść dane i hasła do kont e-mailowych, bankowych itd. Poziom ogólności powyższych odpowiedzi sprawia, że trudno wyobrazić sobie realne zagrożenia, a tym bardziej ich następstwa. Scenariusze, jakie pisze życie, zaskakują nawet wytrawnych znawców tematu.

Hakerzy, jak wynika z policyjnych statystyk, łamią prawo, dopuszczając się ataków, szantażów, wyłudzeń, włamań, zniszczeń czy też czynów pedofilskich. Bardzo często zastraszają swoje ofiary, wykorzystują ich obawy i wstyd. Analiza działań komputerowych przestępców wykazuje, że statystyczny użytkownik sieci może stać się ofiarą masowych, nieukierunkowanych ataków mających na celu wyłudzenie okupu za uruchomienie zablokowanego uprzednio urządzenia. Firma Symantec, opisując oprogramowanie *ransomware* zaznacza, że „nigdy w historii ludzkości ludzie na całym świecie nie byli poddawani wymuszeniom na masową skalę w takim stopniu, jak dzieje się to dziś”[63]. Do zainfekowania *ransomware*'em cyberprzestępcy wykorzystu-

[63] K. Savage, P. Coogan, H. Lau, *The evolution of ransomware*, Version 1.0 – August 6, 2015, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf. (dostęp: 16.09.2019).

ją analogiczne działania, jak w przypadku innego złośliwego oprogramowania[64].

Obok wyłudzeń popularną formą działania hakerów są kradzieże. „W okresie od stycznia do listopada 2017 r. stwierdzono blisko 6 tys. przestępstw związanych z bankowością, z czego 1,8 tys. opisano jako ataki na e-bankowość i phishing"[65]. Poza tym odnotowano 433 przypadki skimmingu, czyli skopiowania paska magnetycznego karty płatniczej w celu jej podrobienia. Dodatkowe zabezpieczenia antyphishingowe wprowadzane przez banki, jak również stosowanie kodów SMS z hasłami przyczyniły się do znacznego ograniczenia tradycyjnych, przywołanych powyżej metod. Niestety przestrzeń bankowa w konsekwencji tych działań nie stała się wolna od zagrożeń ze strony hakerów. Analizowana grupa zmieniła jedynie obszar swojej aktywności i w sposób naturalny – zgodny z trendami – zaczęła wykorzystywać złośliwe oprogramowanie ukierunkowane na urządzenia mobilne (głównie smartfony). Celem podejmowanych wysiłków jest zawirusowanie, instalacja nakładek na bankowe aplikacje mobilne, a następnie wyłudzanie haseł służących do autoryzacji przelewów. Przestępstwa o powyższym charakterze dzieją się na naszych oczach już od kilku lat, stanowiąc tym samym realne zagrożenie statystycznego użytkownika sieci. Za przykład może posłużyć opisana w mediach historia młodej kobiety, która w czerwcu 2018 r. doświadczyła ataku hakera. W powyższym przypadku instalacja zawirusowanej aplikacji zakończyła się wyłudzeniem z konta bankowego znaczącej kwoty. Oszust w promocyjnej ofercie banku pieniądze „na klik" zaciągnął w imieniu kobiety kredyt na 13 tys. złotych, do których zwrotu bank zobowiązał ofiarę, bagatelizując fakt działania hakera i odrzucając składane przez nią odwołania oraz reklamacje[66].

---

[64] B. Mejssner, *Blokują komputer i żądają okupu*, https://pieniadze.rp.pl/finanse-domowe/12585-blokuja-komputer-zadaja-okupu (dostęp: 16.09.2019).

[65] W. Boczoń, *1,8 tys. stwierdzonych przestępstw dotyczących e-bankowości w 2017 r. Zobaczcie statystyki KGP*, https://prnews.pl/18-tys-stwierdzonych-przestepstw-dotyczacych-e-bankowosci-2017-r-zobaczcie-statystyki-kgp-432171 (dostęp: 16.09.2019).

[66] *Haker przejął kontrolę nad telefonem i ukradł 13 tys. zł z konta w banku*, https://www.polsatnews.pl/wiadomosc/2018-08-22/przejal-kontrole-nad-telefonem-i-ukradl-13-tys-zl-z-konta-w-banku/ (dostęp: 26.09.2019).

Firma AdaptiveMobile Security w opracowanej dokumentacji wykazała, że hakerzy zagrażają nie tylko naszym telefonom, ale również ich kartom SIM. Zagrożenie Simjacker to podatność na ataki, która jest niezależna od zainstalowanego na telefonie oprogramowania. W przypadku tej formy działania programy antywirusowe nie sprawdzają się, ponieważ atak zachodzi przez nawiązanie połączenia z kartą SIM. Zabezpieczenie w takiej sytuacji leży wyłącznie po stronie operatora sieci komórkowej[67]. Uzyskanie dostępu do kluczowych funkcji kart SIM umożliwia również exploit WIBattack, wykryty przez specjalistów do spraw bezpieczeństwa z Ginno Security Lab. Wspomniane powyżej zagrożenia umożliwiają hakerowi zlokalizowanie telefonu ofiary, wysyłanie SMS-ów, nawiązywanie połączeń – oczywiście bez wiedzy użytkownika. W następstwie podjętych działań haker ma także możliwość pozyskania prywatnych danych lub przekierowania ofiary na uprzednio przygotowaną stronę internetową, gdzie mogą znajdować się złośliwe kody[68].

Działania hakerów, oprócz strat finansowych, mogą narazić potencjalnego użytkownika sieci na utratę prywatności, straty moralne i emocjonalne. Powyższa forma prześladowania stała się udziałem rodziny ze Słupska, która przez dwa lata była podglądana, podsłuchiwana, zastraszana przy użyciu SMS-ów, narażana na treści pedofilskie, włamania do komputerów, telefonów i telewizorów. W artykule dla „Głosu Pomorza" ofiary hakerów zwierzają się:

> […] od dwóch lat żyjemy w piekle […]. Najpierw były głuche telefony – opowiada pani Anita. – To nas nie zaniepokoiło aż tak bardzo. Któregoś

---

[67] D. Długosz, *Simjacker to kolejne zagrożenie dla telefonów. Hakerzy mogą w ten sposób wykradać dane*, „Komputer Świat", https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/simjacker-to-kolejne-zagrozenie-dla-telefonow-hakerzy-moga-w-ten-sposob-wykradac-dane/8p54gd6?utm_source=www.komputerswiat.pl_viasg_komputerswiat&utm_medium=referal&utm_campaign=leo_automatic&srcc=ucs&utm_v=2 (dostęp: 22.09.2019).

[68] Tenże, *WIBattack to nowe zagrożenie dla kart SIM. Hakerzy mogą wysyłać wiadomości i lokalizować telefon*, „Komputer Świat", https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/wibattack-to-nowe-zagrozenie-dla-kart-sim-hakerzy-moga-wysylac-wiadomosci-i/tz4nt1p (dostęp: 23.09.2019).

dnia zadzwoniła do mnie zdenerwowana mama, twierdząc, że jej telefon komórkowy, leżący na stole, sam dzwoni na telefon stacjonarny. Od tego momentu wszystko poszło lawinowo. […] Nagle wszyscy zaczęliśmy dostawać esemesy, obrzydliwe, wulgarne, o treściach pedofilskich i z przerażającymi groźbami. Wiadomości wysyłane były z naszych własnych telefonów lub z numerów z egzotycznych miejsc, na przykład z Bali czy z Kanady. Próby zablokowania telefonu u operatora spełzły na niczym. […] Nasze rachunki drastycznie wzrosły. Zmieniałam startery – bezskutecznie. W ciągu kilku minut potrafił wysłać sto wiadomości. […] Prześladowca wie, co w danym momencie robią, w której części mieszkania się znajdują, w co są ubrani. Wiedział nawet, jaką córka ma bieliznę – opowiada dalej pani Anita. – Podglądał też moją mamę i babcię. Co bardziej przerażające – wie, w jakich ławkach w klasie siedzą dzieci, zna nauczycieli, imiona kolegów i koleżanek, zna intymne szczegóły z życia naszych znajomych. […] Jestem wyczerpana, ten człowiek zrujnował nam życie.

Ataki hakerskie, często trudne do wykrycia, stają się zmorą policji, która w przekonaniu ofiar nie robi nic lub też podejmuje nieudolne próby pomocy. Zgodnie z uwagami specjalistów opieszałość i nieudolność funkcjonariuszy nie wynika z ich złej woli, a głównie z niedofinansowania, a w konsekwencji z braku specjalistów z obszaru IT w szeregach policji. „Niestety, policjanci tkwią w statystykach i dokumentach, zamiast działać”[69].

Żyjemy w „smart czasach”, co m.in. oznacza, że łącząc się za pomocą specjalnej aplikacji oraz technologii *bluetooth*, możliwe staje się uruchomienie pralki, piekarnika z ulubionym daniem, nastawienie tosta lub ugotowanie wody na herbatę. Wszystko na odległość, bez konieczności bezpośredniego udziału człowieka. Otrzymanie SMS-a od lodówki ze zdjęciem zawartości to rzeczywistość. Ludzkość zewsząd jest otoczona technologią, która niepodważalnie pomaga w życiu codziennym. Nie wolno jednak bagatelizować faktu, że podłączone do

[69] K. Sowińska, *Haker zamienił życie czterech rodzin ze Słupska w koszmar*, https://gp24.pl/haker-zamienil-zycie-czterech-rodzin-ze-slupska-w-koszmar/ar/4788345 (dostęp: 28.09.2019).

sieci urządzenia mogą stać się przyczyną naszych zmartwień i celem ataków hakerskich. SANS Security Awareness ostrzega, że producenci „smart urządzeń" nie analizują kwestii bezpieczeństwa w wystarczającym stopniu, utożsamiając to z nieuzasadnionym wydatkiem. Sprzęty domowe często nie są zabezpieczone lub użyte hasło jest typowe i łatwe do odszyfrowania. Niejednokrotnie konsumenci nie mają nawet możliwości zmiany klucza. W konsekwencji hakerzy uzyskują łatwy dostęp do urządzeń, co niekiedy pozwala również na śledzenie aktywności użytkowników[70].

Mając na uwadze powyższe informacje, dane opublikowane przez firmę Akamai – mówiące, iż średnio 43% wszystkich prób uzyskania dostępu do różnego typu kont internetowych jest podejmowanych przez hakerów – pozornie nie wydają się przerażające[71]. Niemniej jednak należy mieć świadomość, że dostęp do osobistego konta, podobnie jak do sprzętu elektronicznego, może otwierać hakerowi drzwi do prywatności ofiary i dawać mu tym samym potężne narzędzie – wiedzę. Informacje na temat zainteresowań, rodziny, niekiedy związane z kompromitującymi faktami, bywają wykorzystywane w celu wyłudzenia okupu. Z taką sytuacją w 2018 r. policja spotykała się wielokrotnie. Zazwyczaj „szantażysta informuje, że kilka miesięcy temu wgrał wirusa do twojego komputera, przejął nad nim kontrolę i wszystko o Tobie wie. W mailu jest groźba ujawnienia informacji, które mogą Cię skompromitować. Na przykład, że haker ma zdjęcia i filmy pokazujące, jak odbiorca maila ogląda »strony dla dorosłych«. Za rezygnację z ujawnienia kompromitujących informacji szantażysta żąda okupu. Ma być wpłacone w bitcoinach. Sumy – około 900 dolarów […]"[72].

---

[70] *Inteligentne urządzenia w Twoim domu*, „OUCH! Biuletyn Bezpieczeństwa Komputerowego", sierpień 2018, https://www.sans.org/sites/default/files/2018-07/201808-OUCH-August-Polish_0.pdf (dostęp: 28.09.2019).

[71] PAP, *43 proc. wszystkich prób logowania do usług to działania hakerów*, https://businessinsider.com.pl/technologie/prawie-polowa-prob-logowan-do-uslug-to-dzialania-hakerow/p1hh11g (dostęp: 28.09.2019).

[72] M. Rybak, *Hakerzy atakują i szantażują. Żądają okupu płaconego w bitcoinach*, „Gazeta Wrocławska", https://gazetawroclawska.pl/hakerzy-atakuja-i-szantazuja-zadaja-okupu-placonego-w-bitcoinach/ar/13680536 (dostęp: 29.09.2019).

Bardzo często wirusy pobieramy samodzielnie, wraz z aplikacją, filmem lub w ramach działań związanych z tzw. akcjami promocyjnymi znanych produktów. Przykładem może być chociażby kampania spamowa wykryta w 2019 r. przez firmę Eset. Jak opisują specjaliści, hakerzy podszywali się pod popularne firmy czy też aplikacje (np. WhatsApp) i obiecywali darmowe próbki, produkty lub usługi w zamian za rozesłanie spamu oraz wypełnienie ankiety dostępnej pod zamieszczonym linkiem. W rzeczywistości hakerzy zarabiali na każdorazowym wczytaniu konkretnego adresu. Na wskazanych przez hakerów stronach można odnaleźć chociażby złośliwe oprogramowanie[73]. Odnośnie do aplikacji i ich związku z wirusami warto zaznaczyć, że nie ma znaczenia, skąd zostaną pobrane. Nawet sklep Google Play, popularny i przez wielu użytkowników utożsamiany z bezpiecznym miejscem, zawierał zawirusowane zasoby. „Firma ESET poinformowała o dwóch kolejnych aplikacjach, które mogą generować nakładki na ekrany logowania do aplikacji mobilnych. Zagrożeni mogą być m.in. użytkownicy bankowości mobilnej BZ WBK, PKO BP, ING Banku czy mBanku"[74].

W obliczu opisanych sytuacji nasuwa się pytanie – co robić? Czy w przerażeniu zlikwidować pocztę internetową, przestać korzystać z laptopa oraz tabletu? A może wrócić do tradycyjnego telefonu umożliwiającego jedynie wykonywanie połączeń telefonicznych bez jakiejkolwiek opcji SMART? W dobie Internetu oraz coraz bardziej rozpowszechniającej się socjomanii sieciowej podjęcie powyższych kroków jest niezmiernie trudne, a przez większość społeczeństwa byłoby identyfikowane z dziwactwem. W dzisiejszych czasach brak dostępu do sieci wielu ludziom uniemożliwiłby normalne funkcjonowanie, sprowadzając ich na margines cywilizacyjnego wykluczenia. W zachowaniu bezpieczeństwa, obok wysokiej klasy oprogramowania antywirusowe-

---

[73] S. Palczewski, *Hakerzy wykorzystują WhatsApp do złośliwych celów. Element szerszej kampanii*, https://www.cyberdefence24.pl/hakerzy-wykorzystuja-whatsapp-do-zlosliwych-celow-element-szerszej-kampanii (dostęp: 29.09.2019).

[74] W. Boczoń, *Uważajcie! Te programy na Androida mogą generować nakładki na aplikacje mobilne polskich banków*, https://www.cyberdefence24.pl/hakerzy-wykorzystuja-whatsapp-do-zlosliwych-celow-element-szerszej-kampanii (dostęp: 29.09.2019).

go, pomocny może okazać się zatem zdrowy rozsądek i dalekowzroczność w podejmowanych działaniach. Analiza obecnej sytuacji oraz przestępstw zachodzących w sieci komputerowej świadczy na korzyść umiaru i powściągliwości. W rezultacie warto wystrzegać się pobierania z sieci niesprawdzonych uprzednio zasobów, zachować ostrożność przy przeglądaniu poczty elektronicznej – szczególnie załączników oraz podejrzanych wiadomości otrzymywanych od nieznajomych osób. Specjaliści z branży IT zalecają również przysłanianie kamer w sprzętach komputerowych, co utrudni internetowemu stalkerowi śledzenie działań ofiary.

Hakerzy w przestrzeni publicznej – bezlitosne statystyki

Ankieta przeprowadzona w sierpniu 2016 r. przez firmę Thycotic na grupie ponad 250 uczestników konferencji, w tym zidentyfikowanych *black hats*, wykazała, że ponad 77% hakerów uważa, że żadne hasło nie jest bezpieczne przed nimi oraz przed rządem[75]. Największe obawy specjalistów zajmujących się cyberbezpieczeństwem dotyczą jednak phishingu, inżynierii społecznej (50%) oraz wyrafinowanych ataków skierowanych bezpośrednio na różnego typu instytucje (45%)[76]. Wśród nich można wymienić organizacje, niezmiernie istotne z punktu widzenia społecznego, zajmujące się ochroną zdrowia. Jak donosi firma Semantec, w 2018 r. zaobserwowano aktywność grupy hakerów Orangeworm, której celem prawdopodobnie jest szpiegostwo handlowe. Za pomocą trojanów uzyskano dostęp do systemów będących częścią infrastruktury powiązanej z ochroną zdrowia. Zaczęto śledzić producentów sprzętu medycznego. Złośliwe oprogramowanie Symantec odnalazł m.in. na komputerach będących integralną częścią sprzętu medycznego (np. do badań rentgenowskich), urządzeniach zawierających bazy danych osobowych pacjentów (np. służących do rejestracji), a tak-

[75] *Black Hat 2016: Hacker. Survey Report*, https://www.scmagazine.com/wp-content/uploads/sites/2/2018/07/2016_blackhatreport_thycotic_63543.pdf (dostęp: 29.09.2019), s. 2.

[76] Badania zrealizowane na grupie 580 respondentów w 2017 r. oraz 250 respondentów w 2016 r.

że na sprzęcie pomocnym w wypełnianiu formularzy poprzedzających diagnostykę[77].

Kolejnym, równie niepokojącym, niebezpieczeństwem jest manipulacja opinią publiczną. Działania hakerskie mogą wpłynąć na nasz punkt widzenia i być zagrożeniem dla demokracji. Wystarczy wyobrazić sobie sytuację włamania do smartfona szefa partii i opublikowania w mediach treści SMS-ów czy zdjęć o dowolnym podłożu. Wzburzenie wyborców może wywołać wiele niekoniecznie kompromitujących informacji, które wraz z niewybrednymi komentarzami czy też socjotechnikami stosowanymi w środkach masowego przekazu mogą okazać się istotne dla wyniku wyborczego. Tym bardziej że media posiłkują się sensacjami, które są podsycane pikantnymi, niepotwierdzonymi szczegółami opisywanymi przy użyciu zwrotu „prawdopodobnie". Ataku hakerskiego doświadczył chociażby szef kampanii wyborczej Hillary Clinton, który otwierając spreparowany przez rosyjskich hakerów e-mail, ujawnił login i hasło do konta poczty. W rezultacie „na rosyjskim celowniku znalazło się ponad 100 adresów e-mail ludzi pracujących dla Hillary Clinton, w tym Podesta. Do czerwca 2016 r. aż 20 z nich dało się nabrać. Wśród nich były osoby odpowiedzialne za planowanie podróży kandydatki Demokratów, finanse jej kampanii oraz relacje z mediami"[78], co zgodnie z opiniami specjalistów wpłynęło na wyniki wyborów. Z atakami hakerów wielokrotnie zmagały się również organizacje polityczne Unii Europejskiej[79], jak również państwa znajdujące się w granicach Europy[80].

---

[77] PAP, *Hakerzy atakują infrastrukturę ochrony zdrowia w Europie i USA*, http://www.rynekzdrowia.pl/Technologie-informacyjne/Hakerzy-atakuja-infrastrukture-ochrony-zdrowia-w-Europie-i-USA,183924,7.html (dostęp: 29.09.2019).

[78] A. Leszczyński, *Rosyjscy hakerzy manipulują prezydenckimi wyborami w USA*, http://wyborcza.pl/7,75400,20928764,rosyjscy-hakerzy-manipuluja-prezydenckimi-wyborami-w-usa.html (dostęp: 30.09.2019).

[79] PAP, *Rosyjscy hakerzy nasilają ataki przed wyborami do PE*, „Gazeta Prawna", 28.02.2019, https://www.gazetaprawna.pl/artykuly/1400365,rosyjscy-hakerzy-nasilaja-ataki-przed-wyborami-do-pe.html (dostęp: 29.09.2019).

[80] PAP, *Zmasowany atak w całej Europie i USA. Hakerzy wzięli na celownik banki, firmy, instytucje rządowe*, https://businessinsider.com.pl/wiadomosci/atak-hakerski-w-europie-na-celowniku-banki-i-lotnisko/vlhd68n (dostęp: 30.09.2019); Polskie Radio, *Cyberatak na międzynarodową skalę. Świat walczy ze skutkami działania hakerów*,

Specjaliści od cyberbezpieczeństwa odnotowali również zainteresowanie hakerów organizacjami o charakterze wojskowym. „W okresie od marca do maja bieżącego roku przestępcy byli w stanie wykraść tajne dokumenty z ponad 50 zainfekowanych komputerów, spośród których ponad połowa należała do wenezuelskiego wojska. Kampania swoją skuteczność zawdzięcza sprytowi i wiedzy twórców samego zagrożenia, którzy nie tylko rozbudowywali i aktualizowali narzędzie ataku, ale także posługiwali się przy tym żargonem wojskowym”[81]. Nietrudno wyobrazić sobie, ile problemów oraz ofiar mogłoby przysporzyć ujawnienie tajnych planów obejmujących działania obronne lub ewakuacyjne ludności cywilnej.

Na ataki narażone są również różnego rodzaju przedsiębiorstwa, w tym korporacje przechowujące dane osobowe swoich klientów. Na podstawie cyklicznie realizowanych analiz wyszczególnione zostały główne zagrożenia, z którymi zmagają się informatycy obsługujący firmy.

Tabela 6. Zagrożenia obserwowane przez specjalistów ds. bezpieczeństwa cyfrowego USA

Rodzaj zagrożenia	2017	2016
Phishing lub wyłudzanie informacji z sieci społecznościowych, albo inne formy inżynierii społecznej	50%	46%
Zaawansowane ataki skierowane bezpośrednio na organizację	45%	43%
Przypadkowe wycieki danych spowodowane nieprzestrzeganiem zasad bezpieczeństwa przez użytkowników końcowych	21%	15%
Polimorficzny *malware*	20%	15%
Ransomware lub inne formy wymuszenia	17%	15%
Kradzież danych lub sabotaż złośliwych osób w firmie	16%	19%
Ataki na usługi w chmurze lub aplikacje używane przez firmę	15%	11%
Luki w zabezpieczeniach przeoczone przez programistów firmy	15%	20%
Luki w zabezpieczeniach spowodowane aplikacjami	11%	11%
Cyberataki na urządzenia i systemy inne niż komputerowe	12%	9%

https://www.polskieradio.pl/5/3/Artykul/1782434,Cyberatak-na-miedzynarodowa-skale-Swiat-walczy-ze-skutkami-dzialania-hakerow (dostęp: 30.09.2019).

[81] *Maczeta atakuje! Hakerzy wykradali dane wojsku*, Superbiznes, https://superbiz.se.pl/technologie/maczeta-atakuje-hakerzy-wykradali-dane-wojsku-aa-5rbh-4QZ7-uHud.html (dostęp: 30.09.2019).

Tabela 6 (cd.)

Rodzaj zagrożenia	2017	2016
Błędy wewnętrzne lub zewnętrzne ataki	12%	11%
Szpiegostwo lub nadzór obcych rządów lub konkurentów	11%	16%
Kradzież danych, sabotaż lub ujawnienie danych przez haktywistów	8%	9%
Ataki na partnerów biznesowych	7%	7%
Potrzeba zgodności z branżowymi i regulacyjnymi wytycznymi bezpieczeństwa	7%	9%
Ataki za pośrednictwem urządzeń mobilnych	6%	9%
Nadzór rządu	5%	10%

Źródło: Black Hat, *Portrait of an imminent cyberthreat*, 2017, s. 13, https://www.blackhat.com/docs/us-17/2017-Black-Hat-Attendee-Survey.pdf (dostęp: 29.07.2019).

Również polskie firmy zmagają się z cyberzagrożeniami. Analizy przeprowadzone w ramach piątej edycji Badania Stanu Bezpieczeństwa Informacji wykazały, że:

- 62% z nich w ciągu roku miało problemy z zakłóceniami, a nawet kilkugodzinnymi przestojami spowodowanymi nieprzyjaznym działaniem hakerów;
- 44% spółek wskutek ataków poniosło znaczące straty finansowe;
- 21% spotkało się z zagrożeniami typu *ransomware*;
- co piąta duża lub średnia firma nie ma specjalisty odpowiedzialnego za bezpieczeństwo informacji oraz sprzętu komputerowego;
- prawie połowa korporacji (46%) nie ma procedur postępowania w przypadku cybernapaści;
- wydatki na bezpieczeństwo sieciowe stanowią jedynie 3% budżetu IT;
- zaledwie 8% przedsiębiorstw podejmuje właściwe decyzje pod względem odpowiedzialności informatycznej;
- największe bezpieczeństwo informatyczne wykazują firmy z sektora finansowego, telekomunikacji, energetyki oraz produkcji przemysłowej;
- obecnie co dziesiąta spółka posiada polisę ubezpieczeniową od następstw cyberzagrożeń[82].

[82] PwC, *Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami li-*

Mimo wielu niebezpieczeństw „w opinii przeciętnej polskiej firmy, cyberbezpieczeństwo jest trendem, nie zaś realnym wyzwaniem, które powinno stać się jednym z priorytetów zarządu”[83]. Być może przyczyniają się do tego sami zatrudnieni, jak wykazują bowiem badania, średnio za 33% cyberincydentów odpowiedzialni są pracownicy firmy, tymczasem hakerzy są sprawcami 28% z nich[84].

Zespół CERT Polska, działający w strukturach NASK, podkreśla, że liczba zgłaszanych incydentów z roku na rok regularnie wzrasta. W 2018 r. liczba cyberprzestępstw wyniosła 3739 i była wyższa o prawie 18% od liczby zdarzeń z 2017 r., 75% z nich dotyczyło osób fizycznych lub podmiotów prywatnych. Obecnie wśród najczęściej występujących zdarzeń wymienia się:

- phishing;
- dystrybucję złośliwego oprogramowania;
- spam[85].

Zespół badawczy Thycotic w zrealizowanych analizach odniósł się również do zagrożeń dotyczących statystycznych konsumentów – 56% aktywnie działających hakerów wskazało, że ogół społeczeństwa nie ma podstawowej wiedzy na temat phishingu oraz innych ataków socjotechnicznych. Kolejnym możliwym do zrealizowania czarnym scenariuszem jest kradzież danych osobowych klientów firm, które nie przykładają należytej uwagi do przestrzegania podstawowych zasad bezpieczeństwa. Zagrożenie to dostrzega aż 36% ankietowanych. Sama wymiana i korzystanie z danych osobowych przez spółki handlowe jest klasyfikowane jako wysoce ryzykowne przez 20% badanych. Średnio co trzeci haker (29%) działa na podstawie braku odpowiedniego oprogramowania zabezpieczającego na urządzeniach konsumenckich. Co czwarty ma ułatwione zadanie ze względu na brak umiejętności two-

---

czą na szczęście, 2018, s. 2, 12, 31, https://www.pwc.pl/pl/pdf/publikacje/2018/cyber--ruletka-po-polsku-raport-pwc-gsiss-2018.pdf (dostęp: 30.09.2019).

[83] Tamże, s. 30.

[84] Tamże, s. 9.

[85] *Raport roczny 2018 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego Internetu*, s. 4, https://www.cert.pl/PDF/Raport_CP_2017.pdf (dostęp: 30.09.2019).

rzenia i utrzymywania silnych haseł do kont oraz urządzeń komputerowych. Drzwi do przestępstw i nielegalnych działań otwierają również awarie zabezpieczeń internetowych oraz luki w budowie przeglądarek, na co wskazuje 16% ankietowanych. Co dziesiąty haker wśród potencjalnych zagrożeń dostrzega nadzór, a w konsekwencji naruszanie prywatności przez agencje i podmioty rządowe. Na podstawie zgromadzonych danych można pokusić się o stwierdzenie, że w najbliższym czasie jednym z najpoważniejszych problemów związanych z cyberbezpieczeństwem będzie zwiększone wykorzystanie oprogramowania *ransomware* – ułatwiającego wyłudzanie okupów[86].

Ataki hakerskie wpływają na funkcjonowanie całego społeczeństwa. Tracą na nich obywatele, przedsiębiorstwa, organizacje, również gospodarka. „W rankingu Interpolu przestępczość internetowa wyprzedziła pod względem »dochodowości« handel narkotykami. Według danych Cisco 45% cyberataków w naszym kraju spowodowało straty wynoszące ponad 100 000 USD"[87]. Zyskują jedynie nieuczciwi użytkownicy sieci.

Przeciwdziałanie

Zainfekowany system

O tym, jak poważnym problemem jest zainfekowany system komputerowy, świadczy chociażby liczba wskazań wyświetlających się w wyszukiwarce po wpisaniu haseł: „wirus w telefonie" (3,73 mln), „czy mam wirusa w komputerze" (817 tys. wskazań), „zainfekowany komputer" (309 tys.), „jak sprawdzić, czy mam zainfekowany komputer" (113 tys.), „jak sprawdzić, czy mam zainfekowany telefon" (69,7 tys.). Często zdarza się, że nawet doświadczony użytkownik sprzętu ma problem ze zdiagnozowaniem infekcji, tym bardziej że programy antywirusowe niekiedy również nie wykrywają zagrożenia.

---

[86] Black Hat, *Portrait…*, s. 19.

[87] Fakt24, *Masz taki telefon? Jesteś na celowniku hakerów*, https://www.fakt.pl/facet/technologie/posiadacze-smartfonow-na-celowniku-hakerow/jdsqewr (dostęp: 30.09.2019).

Do zakażenia *malware*'em może dojść przez uruchomienie zainfekowanego programu, gry lub pliku w dowolnym formacie. Na złośliwy *software* możemy natrafić w załącznikach e-mail, w tym w spamie. Polska firma Opcja szacuje, że „aż 87% złośliwego oprogramowania trafia na komputery drogą mailową. Wirusy, robaki i konie trojańskie – niemal każdy rodzaj złośliwego oprogramowania – może być rozpowszechniany poprzez e-mail"[88].

Do zagrożeń związanych z usługą poczty elektronicznej klasyfikuje się również phishing. Głębsza analiza powyższego zjawiska wykazuje, że działania opierające się na poczcie elektronicznej często wykorzystują całą gamę narzędzi inżynierii społecznej i psychologicznej, za pomocą której nakłaniają użytkowników do podania szczegółowych danych osobowych lub do zainstalowania złośliwego oprogramowania – chociażby *ransomware*'u, konia trojańskiego o charakterze keyloggera itp. Przekazanie oprogramowania odbywa się za pomocą linku lub też załącznika. W minionych latach hakerzy podszywali się pod dostawców mediów, urząd skarbowy, policję, popularne sklepy itp. Z danych zawartych w raporcie Proofpoint o zagrożeniach cyberprzestrzeni wynika, że liczba ataków z użyciem poczty elektronicznej systematycznie wzrasta[89].

Inną przyczyną zainfekowania systemu może być trojan downloader, czyli program „pobierający inne programy za pośrednictwem Internetu i uruchamiający je na zaatakowanym komputerze bez wiedzy czy zgody użytkownika"[90]. Równie popularny w minionych latach był botnet, czyli twór będący siecią połączonych ze sobą komputerów, przejętych przez hakera przy użyciu złośliwego oprogramowania. Zainfekowane maszyny, będące częścią sieci, umożliwiają hakerowi zdalną kontrolę, w następstwie czego może on zacząć korzystać z konta

---

[88] Opcja.pl, *Przewodnik po bezpieczeństwie e-maili – przegląd popularnych zagrożeń*, https://www.opcja.pl/przewodnik-po-bezpieczenstwie-email-przeglad-popularnych-zagrozen/ (dostęp: 30.09.2019).

[89] Proofpoint, *Report. Understanding email fraud. A global survey of IT leaders in the US, The UK, Australia, France and Germany, 2017*, https://www.proofpoint.com/sites/default/files/pfpt-us-tr-survey-of-understanding-email-fraud-180315.pdf (dostęp: 30.09.2019).

[90] Encyklopedia wirusów, *Trojan-Downloader.Win32.Dila*, http://www.wiruspc.pl/encyclopedia/id,11921/trojan-downloader.win32.dila.html (dostęp: 30.09.2019).

ofiary, przejmować prywatne wiadomości lub przeprowadzać ataki DDoS[91].

Bezpieczeństwu danych i systemowi, jak podkreśla firma Kaspersky, zagrażają także exploity, czyli „podgrupa szkodliwych programów. Zawierają one dane lub kod wykonywalny, który może wykorzystać jedną lub wiele luk w oprogramowaniu działającym na komputerze lokalnym lub zdalnym"[92]. W sieci można napotkać również *malvertisement* lub *malvertising* – odmianę reklam internetowych służącą do rozprzestrzeniania szkodliwego *software*'u. W powyższym przypadku „kod ukryty pośrednio lub bezpośrednio w wyświetlanej reklamie prowadzi do infekcji urządzenia ofiary złośliwym lub potencjalnie szkodliwym oprogramowaniem"[93].

Statystycznego eksploatatora powinien niepokoić fakt, że część zagrożeń nie zawsze jest wykrywana przez aplikacje zabezpieczające. Zaatakowany system nie pozostaje jednak całkowicie niezmieniony, wykazując pewne symptomy, których obecność może świadczyć o istniejącym problemie. Niepokój mogą zatem wzbudzać:

- spowolnienie pracy komputera;
- problemy z uruchomieniem lub zamknięciem systemu operacyjnego;
- częste zawieszanie się sprzętu;
- wyświetlanie na ekranie urządzenia informacji o błędach;
- samoistne znikanie (np. folderów, plików) lub uruchamianie zawartości komputera (np. muzyki, filmów);
- niekontrolowane otwieranie lub zamykanie napędu CD-ROM;
- samoistne rozsyłanie spamu z konta e-mail;
- trudność w nawiązaniu połączenia z Internetem;
- niekontrolowane uruchamianie przeglądarki internetowej lub przekierowywanie użytkownika na inne strony w sieci;
- zniknięcie programu antywirusowego z urządzenia;
- problemy z działaniem hasła itp.

---

[91] Avast, *Botnet*, https://www.avast.com/pl-pl/c-botnet (dostęp: 30.09.2019).

[92] Kaspersky, *Co to są exploity i dlaczego są złe*, https://plblog.kaspersky.com/co-to-sa-exploity-i-dlaczego-sa-zle/3409/ (dostęp: 10.10.2019).

[93] CERT Orange Polska, *Malvertisment, czyli biznes pełną gębą*, https://www.cert.orange.pl/aktualnosci/malvertisment-czyli-biznes-pelna-geba (dostęp: 10.10.2019).

Oczywiście występowanie powyższych oznak nie jest jednoznaczne z zainfekowaniem systemu, jednak powinno zwrócić uwagę i wzmóc czujność użytkownika.

W przypadku podejrzenia infekcji zaleca się pełne skanowanie systemu. Warto, aby powyższe działanie przebiegało na podstawie aktualnej bazy danych. Brak programu antywirusowego winien być niezwłocznie uzupełniony. Właściwym posunięciem jest również odłączenie urządzenia od Internetu oraz sieci lokalnej (o ile jest jej częścią). Jest to istotne, gdyż zaatakowany system może ułatwić osobom trzecim dostęp do baz danych, zapisanych w pamięci urządzenia. Kolejnym ważnym przedsięwzięciem jest przekopiowanie istotnych zasobów na urządzenie zewnętrzne – *pendrive*, płytę DVD itd. W przypadku środowiska Windows, gdy komputer nie chce uruchomić się z dysku twardego, rekomenduje się włączenie systemu w trybie awaryjnym przy użyciu dysku startowego. Problem z rozpoznaniem nośnika może wynikać z tego, że wirus uszkodził tablicę partycji dysku. W tych okolicznościach pomocny może okazać się program ScanDisk będący integralną częścią systemu Windows.

Równolegle do powyższych działań należy zadbać o bezpieczeństwo kont internetowych. W konsekwencji, korzystając z komputera wolnego od wirusów, trzeba niezwłocznie zmienić wszystkie hasła, zarówno do banku, poczty elektronicznej, dziennika elektronicznego, jak i do serwisów społecznościowych.

Kiedy mimo naszych starań mamy problem ze złośliwym oprogramowaniem, warto skontaktować się z dostawcą posiadanego przez nas oprogramowania antywirusowego lub poprosić o pomoc informatyka. Pamiętajmy, że wszystkie cyberprzestępstwa należy zgłaszać w jednostce policji lub w prokuraturze.

Edukacja i działania profilaktyczne

Droga ku bezpieczeństwu sieciowemu winna pokrywać się ze ścieżką edukacji formalnej i towarzyszyć uczniom już od pierwszej klasy szkoły podstawowej. Edukacja medialna, a w szczególności „edukacja dla Internetu", jest jednym z głównych starań, jakie jesteśmy zobowiązani

inicjować, aby chronić nasze dzieci przed różnorodnymi zagrożeniami świata wirtualnego[94]. Działanie to jest niezmiernie ważne, jak podkreśla bowiem Józef Bednarek, Internet jest źródłem niewłaściwych wzorców, chociażby w kontekście kształtowania osobowości odbiorcy[95]. Wiele ryzykownych sytuacji stwarzają również aktywności podejmowane przez hakerów. W konsekwencji nauczyciele w ramach lekcji wychowawczych powinni uświadamiać oraz przygotowywać uczniów do właściwych zachowań w sieci. Wiele interesujących materiałów z tego zakresu można odnaleźć na stronie saferinternet.pl, będącej częścią działań Polskiego Centrum Programu Safer Internet. W skład PCPSI wchodzą: Państwowy Instytut Badawczy NASK oraz Fundacja Dajemy Dzieciom Siłę (dawniej Fundacja Dzieci Niczyje), co jest gwarancją wysokiej jakości omawianych zasobów. Wśród materiałów edukacyjnych znajdują się: pliki multimedialne, kursy e-learningowe, scenariusze zajęć, poradniki i broszury, zasoby opracowane na potrzebę kampanii społecznych, jak również raporty z badań[96]. Inną ciekawą bazę wiedzy stanowi strona Fundacji Orange, gdzie w zakładce dla nauczycieli i wolontariuszy pedagodzy odnajdą urozmaicone opracowania do kreowania: aktywności z udziałem dzieci od czwartego do szóstego roku życia, lekcji na różnych poziomach szkoły podstawowej (od I do VIII klasy) oraz ponadpodstawowej, jak też do rozmów w środowisku osób dorosłych[97]. Równie zachęcająco prezentuje się biblioteka materiałów na stronie cyfrowobezpieczni.pl, Bezpieczna Szkoła Cyfrowa[98], gdzie bezpośrednio poruszona została problematyka ochrony przed wirusami, doboru haseł oraz bezpiecznego logowania do różnego typu kont.

---

[94] W. Strykowski, *Kompetencje medialne: pojęcie, obszary, formy kształcenia*, w: W. Strykowski, W. Skrzydlewski (red.), *Kompetencje medialne społeczeństwa wiedzy*, wyd. eMPi2, Poznań 2004, s. 46.

[95] J. Bednarek, *Multimedia w kształceniu*, Wydawnictwo Naukowe PWN, Warszawa 2006, s. 268–279.

[96] Polskie Centrum Programu Safer Internet, saferinternet.pl (dostęp: 20.08.2019).

[97] Fundacja Orange, *Strefa wiedzy dla nauczycieli i wolontariuszy*, https://fundacja.orange.pl/strefa-wiedzy/dla-nauczycieli-i-wolontariuszy (dostęp: 20.08.2019).

[98] Cyfrowobezpieczni.pl, Bezpieczna Szkoła Cyfrowa, https://www.cyfrowobezpieczni.pl/biblioteka-materialow/scenariusze-lekcji (dostęp: 20.08.2019).

Powyższe zasoby zostały opracowane z funduszy Ministerstwa Edukacji Narodowej w ramach zadania „Poprawa kompetencji pracowników szkoły, uczniów i ich rodziców w zakresie bezpiecznego korzystania z cyberprzestrzeni oraz reagowania na zagrożenia". Równolegle do opisanych stron w sieci funkcjonuje wiele innych witryn poświęconych powyższej tematyce.

Profilaktyka zagrożeń internetowych winna stać się częścią wykładów, ale również codziennych działań pedagogów. W celu bezpieczniejszego użytkowania sprzętu warto trzymać się kilku podstawowych zasad:

- regularnie weryfikować stan instalacji oraz aktualizacji programu antywirusowego, zarówno w kontekście komputera, jak i innych urządzeń podłączonych do sieci;
- pamiętać o systematycznym wykonywaniu kopii bezpieczeństwa plików;
- chronić hasła dostępu do prywatnych kont w sieci[99];
- nie otwierać podejrzanych e-maili od nieznanych osób, poczty zawierającej błędy w tytule, wiadomości o niewiarygodnych zdarzeniach itp.;
- nie klikać w linki, nie otwierać załączników, nie instalować oprogramowania przekazanego w e-mailu od nieznanego nadawcy;
- nie odwiedzać witryn z nielegalnymi treściami;
- unikać dodawania swoich sprzętów do grupy urządzeń zaufanych, umożliwiając sobie dodatkowe uwierzytelnianie przy logowaniu np. do placówki banku;
- uważać na zasoby pobierane z sieci – nawet zaufane strony mogą zawierać złośliwe oprogramowanie;
- przed utylizacją sprzętu przywrócić go do ustawień fabrycznych[100];
- nie obawiać się pytań i prosić o pomoc w razie potrzeby.

---

[99] *Black Hat 2016*…, s. 3.

[100] *Utylizacja urządzenia mobilnego*, „OUCH! Biuletyn Bezpieczeństwa Komputerowego", marzec 2019, https://www.sans.org/sites/default/files/2019-03/201903--OUCH-March-Polish_0.pdf (dostęp: 26.08.2019).

W przypadku placówek, które w dużej mierze są oparte na pracy zdalnej, warto rozważyć korzystanie z sieci prywatnej – VPN[101].

W dzisiejszych czasach, zdominowanych przez nowe media, Internet oraz cyberdziałania, przed nauczycielami zaczynają pojawiać się nowe i trudne wyzwania. Istotne jest ustawiczne zdobywanie wiedzy przedmiotowej oraz umiejętności dydaktycznych wspieranych zmieniającymi się narzędziami komputerowymi. Dodatkowo należy podkreślić, że dynamiczne i intensywne tempo zmian, niespotykane wcześniej w szkolnictwie, wymaga reorientacji nastawienia, jak również wypracowania wewnętrznej potrzeby zdobywania dodatkowych kompetencji o charakterze społecznym, informatycznym, a także psychologicznym. Jedynie profesjonalne, wielokierunkowe przygotowanie daje szanse na prawidłową realizację procesu nauczania oraz wychowania podopiecznych. Przed współczesnymi pedagogami coraz silniej zaczyna zaznaczać się nowy obowiązek – znajomość zagrożeń przestrzeni internetowej oraz sposobów skutecznego ich unikania. Adepci zawodu winni pamiętać, że ich wiedza i przejawiane zachowania w ogromnym stopniu będą rzutować na sposób myślenia i działania powierzonych im pokoleń. Nauczyciele (bez względu na poziom nauczania czy wykładany przedmiot) stają się odpowiedzialni nie tylko za edukację przedmiotową, ale również za kształtowanie prawidłowych postaw związanych z obecnością w sieci, jak również przygotowanie do odpowiedzialnego korzystania z nowych mediów.

Stopniowe i świadome wprowadzanie dzieci do świata Internetu oraz regularne działania profilaktyczne mogą zminimalizować (a niekiedy nawet zlikwidować) zagrożenia z niego płynące.

Narzędzia stosowane przez hakerów oraz oprogramowanie zabezpieczające

Specjaliści od cyberbezpieczeństwa podkreślają, że formy hakerskich ataków są różnorodne i w dużej mierze zależą od środowiska, na które

[101] *Wirtualne Sieci Prywatne (VPN)*, „OUCH! Biuletyn Bezpieczeństwa Komputerowego", lipiec 2019, https://www.sans.org/sites/default/files/2019-06/201907--OUCH-July-Polish.pdf (dostęp: 26.08.2019).

są nakierowane. Do jednych z najbardziej popularnych sposobów ataku należą działania oparte na inżynierii społecznej. „Niedawne naruszenie danych ponad 10 000 pracowników Wydziału Sprawiedliwości i Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych oraz ponad 20 000 pracowników Federalnego Biura Śledczego (FBI) jest kolejnym przykładem na to, że »wniknięcie« do organizacji z pomocą metod socjotechnicznych jest dla hakerów o wiele łatwiejszym zadaniem niż pisanie exploitów zero-day – powiedział Zoltán Györkő, prezes firmy Balabit"[102].

Phishing jest działaniem, u którego podstaw leży wspomniana inżynieria społeczna. Oszustwo polega na nakłanianiu ofiary do podania różnorodnych danych i haseł lub podjęcia działań ułatwiających ich zdobycie. W konsekwencji haker inicjuje aktywności, które ułatwiają zdobycie zaufania ofiary. Niejednokrotnie e-maile phishingowe sugerują, że ich adresatem są instytucje lub firmy cieszące się społecznym zaufaniem. Wielokrotnie w temacie wiadomości można spotkać informacje o wygranej lub superpromocji, która kończy się za kilka minut. Sytuacje te są aranżowane w celu wymuszenia na użytkowniku sieci szybkich i nieprzemyślanych działań. W ramach stosowanych socjotechnik cyberprzestępcy często przenoszą swoje aktywności również poza formalną drogę e-mailową i starają się pozyskać zaufanie ofiary za pomocą mediów społecznościowych, np. Twittera, Facebooka, Instagrama lub komunikatorów Skype'a, WhatsAppa itp.[103]

Kolejną formą ofensywy jest włamanie się na konto, a niekiedy również do sieci lokalnej. W rankingach popularnych metod hakerskich wysoko lokują się również ataki webowe, np. SQL injection, polegające na wysłaniu do strony WWW fragmentu zapytania SQL. Powyższa forma umożliwia m.in. ominięcie mechanizmu uwierzytelniania, odczytanie wybranych plików, nieautoryzowany dostęp do bazy danych[104].

---

[102] eGospodarka, *10 ulubionych narzędzi cyberprzestępcy*, http://www.egospodarka.pl/130511,10-ulubionych-narzedzi-cyberprzestepcy,1,12,1.html (dostęp: 26.08.2019).

[103] *Oszustwa za pośrednictwem mediów społecznościowych*, „OUCH! Biuletyn Bezpieczeństwa Komputerowego", wrzesień 2019, https://www.sans.org/sites/default/files/2019-09/201909-OUCH-September-Polish.pdf (dostęp: 26.08.2019).

[104] Sekurak, *Czym jest SQL injection?*, https://sekurak.pl/czym-jest-sql-injection/ (dostęp: 26.08.2019).

Każdy nauczyciel w swojej codziennej pracy może spotkać się również z *malware*'em rozprzestrzeniającym się za pomocą poczty elektronicznej, dokumentów, instalatorów czy pamięci przenośnej. W ramach podstawowego podziału złośliwego oprogramowania wyróżnia się: wirusy, robaki i trojany. Bardziej zaawansowana klasyfikacja uwzględnia również: backdoory, trojany zdalnego dostępu, złodzieje informacji i *ransomware*[105]. Wirusy to zdolne do replikacji oraz zainfekowania kolejnych jednostek programy niszczące i wykradające informacje. Mogą one także zmienić działanie systemu. Wirusy mają charakter wykonywalny, co oznacza, że nie są czynne, dopóki użytkownik ich nie aktywuje przy okazji uruchamiania zainfekowanego elementu. Podobnym działaniem charakteryzują się robaki, które zagrażają nie tylko jednemu komputerowi, ale również całym sieciom internetowym. Robaki w przeciwieństwie do wirusów rozprzestrzeniają się samoistnie. Trojany, które nie mają zdolności replikowania, są nieświadomie instalowane przez użytkowników. Na obecność trojanów na komputerze mogą wskazywać m.in. nagle wyskakujące okna lub znikające pliki. To złośliwe oprogramowanie ułatwia także kradzież danych, zarażanie innymi rodzajami *malware*'u oraz dostęp do systemu osób trzecich.

W przypadku trojanów zdalnego dostępu mamy do czynienia z oprogramowaniem umożliwiającym czynności administracyjne, w tym: przechwytywanie wiadomości, haseł i danych, wgrywanie na komputer nowych plików, wykonywanie zrzutów ekranu, uruchamianie kamery i mikrofonu, podsłuchiwanie rozmów internetowych[106].

Dostęp do systemu operacyjnego osobom wtajemniczonym, a niekiedy również nieupoważnionym, ułatwiają także backdoory, czyli luki w budowie oprogramowania osłabiające mechanizm bezpieczeństwa. Wśród korporacji, które zdecydowały się na świadome zastosowanie backdoora, są znane wszystkim firmy Microsoft czy Samsung. Powyższe rozwiązanie, jak argumentują specjaliści, miało pomóc twórcom w przeprowadzeniu wewnętrznych testów, jak również być dodatkową

---

[105] Redakcja WebSecurity, *Wirusy, trojany, robaki… Co to jest malware?*, http://websecurity.pl/wirusy-trojany-robaki-co-to-jest-malware/ (dostęp: 26.08.2019).

[106] O. Pursche, *Tak szpiegują trojany R.A.T.*, „Komputer Świat", https://www.komputerswiat.pl/artykuly/redakcyjne/tak-szpieguja-trojany-rat/96er5v2 (dostęp: 26.08.2019).

ochroną przed hakerami. W rzeczywistości „tylne drzwi" dały sposobność do np. wykradania prywatnych danych, podsłuchiwania, szpiegowania lub wdrażania złośliwego oprogramowania[107].

Kolejnym narzędziem stosowanym przez hakerów są złodzieje informacji. Tym mianem określa się każde złośliwe oprogramowanie, które może wykradać prywatne zasoby, hasła i dane dostępowe do kont itp. W tej grupie wyróżnia się keyloggery (rejestrujące działania na klawiaturze), nagrywarki pulpitu (wykonujące regularne screeny ekranu) i oprogramowanie zrzucające z pamięci RAM niezaszyfrowane, łatwe do użycia dane.

Inną odmianą złośliwego oprogramowania jest *ransomware*, za pomocą którego cyberprzestępcy szyfrują całe dyski lub pojedyncze dane w celu wyłudzenia opłaty za ich odszyfrowanie.

Bardziej doświadczeni hakerzy mogą również przygotować exploity, czyli programy wykorzystujące dane lub kod wykonywalny, działające na podstawie luk w oprogramowaniu sprzętu[108].

Równie niebezpiecznym i realnym w obszarze szkolnictwa zagrożeniem jest wzrost popularności modelu Bring Your Own Device. „Tylko w Polsce, jak wynika z badań przeprowadzonych w 2015 roku, jest ponad 19 milionów smartfonów. Firma Citrix przewiduje, iż do 2020 roku 89% organizacji będzie oferować mobilny styl pracy. Już dziś ilości danych, jakie rocznie są przesyłane przez sieci komórkowe, jest gigantyczna, a prognoza na lata 2016–2021 wynosi 1600 ExaBytów"[109]. Oczywiście aktywność nauczycieli poza szkołą jest w dużej mierze ograniczona, nie da się jednak ukryć, że odgrywa znaczącą rolę w życiu pedagogów. Bezpieczeństwo danych jest zatem istotne chociażby ze względu na pracę z systemem Moodle, testami komputerowymi[110], e-dziennikiem[111] itp. Placówki edukacyjne powinny zatem zabezpieczyć

---

[107] J. Szczęsny, *Backdoor w telefonach z Androidem? Google potwierdza*, https://antyweb.pl/backdoor-android-google/ (dostęp: 26.08.2019).

[108] Kaspersky, dz. cyt.

[109] G. Podgórski, *Bezpieczeństwo informacji w modelu BYOD*, „Nierówności Społeczne a Wzrost Gospodarczy" 2018, 53(1/2018), s. 181.

[110] K. Majewska, *Komputerowy system egzaminowania*, „E-mentor" 2015, 1(58), s. 41–47.

[111] Taż, *The electronic register in Polish schools…*, s. 93–111.

finanse na odpowiednie wyposażenie, działania ochronne, wykupienie licencji niezbędnych programów. Ważna jest również przemyślana strategia wsparcia technicznego pracowników oraz uwrażliwienie na kwestie prawne.

Specjaliści od zabezpieczeń wyróżniają także zagrożenie określane jako *shadow* IT. Polega ono na samowolnej instalacji oprogramowania lub aplikacji przez pracownika szkoły, firmy itd. Forma ta może doprowadzić do wykradnięcia danych, jak również naraża jednostkę na karę finansową związaną z użytkowaniem oprogramowania niezgodnie z licencją[112].

W celu ochrony naszych urządzeń warto skorzystać z profesjonalnych programów antywirusowych lub firewalla. Gwarantują one szerokie zabezpieczenie od osłony plików systemowych i rejestru, po dostęp do stron internetowych. Wykrywają liczne zagrożenia, zapobiegają atakom i nieuprawnionemu dostępowi do systemu, neutralizują oraz usuwają szkodliwe aplikacje i programy. Głównym warunkiem prawidłowego ich funkcjonowania jest regularna aktualizacja.

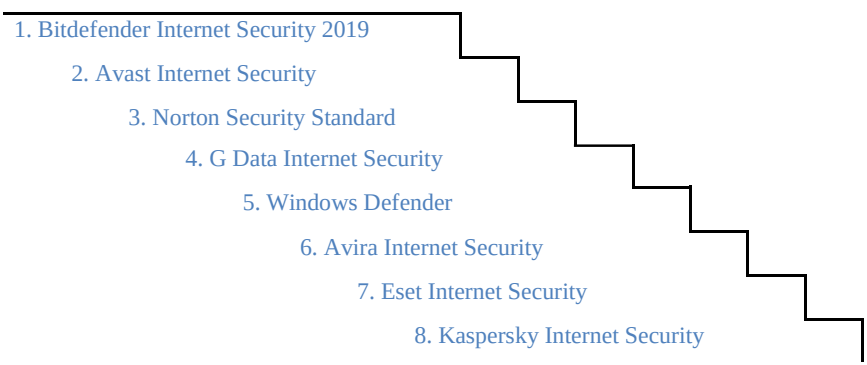
Należy mieć na uwadze, że programy antywirusowe i firewalle nie są wolne od wad. W ich przypadku brak aktualizacji jest równoważny z ich bezużytecznością, a nawet ze szkodliwością wynikającą ze złudnego poczucia bezpieczeństwa użytkownika oprogramowania. Dodatkowo firewall nie ma zabezpieczenia przed modyfikacjami m.in. „zaufanych" plików, rejestru i zapisów obejmujących „zaufane aplikacje". Odnośnie do programów zewnętrznych należy zaznaczyć, że najbardziej aktualne i niezawodne pliki instalacyjne nie są darmowe.

Badania przeprowadzone w 2018 r. przez laboratorium „Komputer Świat" oraz dwa renomowane instytuty: AV-Test i AV-Comparatives, wykazały, że „dla prywatnych użytkowników pecetów najpoważniejszym zagrożeniem pozostaje ransomware. Jeśli takiemu programowi uda się zaszyfrowanie prywatnych danych, to te na ogół należy spisać na straty, nawet jeśli użytkownik zapłaci duży okup (ransom). Tym waż-

---

[112] M. Silic, D. Silic, G. Oblakovic, *Influence of shadow IT on innovation in organizations*, „Complex Systems Informatics and Modeling Quarterly CSIMQ" 2016, 8 (September/October), s. 68–80.

niejsza jest skuteczna ochrona przed takim zagrożeniem. Ale tylko Bitdefender, Avast, G Data, Norton i Avira w tym ważnym kryterium testu okazały się bezbłędne. Eset i Kaspersky przepuściły po dziesięć procent testowych wirusów szantażujących, a Windows Defender wręcz połowę"[113]. Kaspersky zawiódł również pod kątem rozpoznawalności aktualnych zagrożeń. Na przetestowanych 4361 zagrażających naszemu sprzętowi programów zlekceważył aż 28. W następstwie licznych i długoterminowych testów uwzględniających m.in. skuteczność przeciwwirusową, wpływ na prędkość pracy urządzenia oraz cenę autorzy badania opracowali listę rankingową płatnych aplikacji antywirusowych.



Wykres 3. Lista rankingowa płatnego antywirusowego *software*'u
Źródło: opracowanie własne na podstawie „Komputer Świat".

Wśród darmowego oprogramowania antywirusowego przetestowanego w 2019 r. AVLab poleca:

- Comodo Internet Security Premium (ocena 5);
- SecureAPlus (ocena 5);
- VoodooShield (ocena 5);
- Kaspersky Free (ocena 4,5);
- Comodo Cloud Antivirus (ocena 4,5);

[113] *Najsurowszy test bezpieczeństwa wszech czasów. Który z programów antywirusowych okazał się najlepszy?*, „Komputer Świat", https://www.komputerswiat.pl/recenzje/programy/najsurowszy-test-bezpieczenstwa-wszech-czasow-ktory-z-programow-antywirusowych-okazal/p2wd4d7 (dostęp: 26.08.2019).

- Avast Free Antivirus (ocena 4);
- Avira Free Antivirus (ocena 4);
- Bitdefender Antivirus Free Edition (ocena 4);
- Panda Dome (dawniej Panda Free Antivirus) (ocena 4);
- Sophos HOME Free/Premium* (ocena 4);
- ZoneAlarm Free Antivirus + Firewall (ocena 4)[114] .

Zabezpieczenie sprzętu komputerowego jest konieczne. Szczególnie, że „co trzeci Polak ma obawy, że w ciągu ostatnich kilku miesięcy jego komputer został zawirusowany"[115]. Niestety, jak wykazały badania zrealizowane w 2016 r. przez ARC Rynek i Opinia[116], trzykrotnie więcej kobiet niż mężczyzn nie dysponuje wiedzą na temat oprogramowania oraz faktu jego posiadania na swoim komputerze[117]. Zestawiając te dane z sylwetką statystycznego, polskiego nauczyciela – kobiety w wieku średnim, rysuje się smutny obraz szkoły narażonej na ataki pochodzące z przestrzeni internetowej.

---

[114] Polecane darmowe antywirusy na 2019 r. od redakcji AVLab, https://avlab.pl/polecane-darmowe-antywirusy-na-rok-2019-od-redakcji-avlab (dostęp: 28.08.2019).

[115] km, *4/5 Polaków ma program antywirusowy w prywatnym pececie. Avast najpopularniejszy*, https://www.wirtualnemedia.pl/artykul/4-5-polakow-ma-program-antywirusowy-w-prywatnym-pececie-avast-najpopularniejszy (dostęp: 28.08.2019).

[116] Badania zrealizowane na grupie 900 osób.

[117] *Polacy a komputerowe wirusy*, https://arc.com.pl/Polacy-a-komputerowe-wirusy-blog-pol-1534962147.html (dostęp: 28.08.2019).

Zakończenie

Świat technologii oraz wirtualnych konstrukcji otaczających nas z każdej strony zaczyna swym rozmiarem oraz charakterem przypominać ten realny. Coraz więcej osób niekoniecznie uzależnionych od nowych mediów czy różnorodnych form aktywności sieciowych zatraca poczucie granicy między tymi przestrzeniami, balansując na pograniczu rzeczywistości i jej iluzji. Zjawisko to wymaga refleksji oraz analizy korzyści oraz zagrożeń wynikających z tego stanu rzeczy. Nie jesteśmy w stanie przewidzieć kierunków zachodzących zmian oraz pojawiających się w ich kontekście zagrożeń. Jeszcze pół wieku temu dostęp do komputerów miała niewielka grupa ludzi. Trzydzieści lat temu nikt nie słyszał o cyberprzemocy, cyberstalkingu czy cyberseksie. Regularnie, co kilka tygodni, pojawiają się nowe wirusy, robaki oraz trojany. Atakują one komputery oraz urządzenia mobilne. Algorytmy sztucznej inteligencji projektowane przez profesjonalnych informatyków umożliwiają: gromadzenie danych, śledzenie aktywności w sieci, inwigilację rozmów internetowych i telefonicznych. Należy być świadomym, że tempo zmian technologicznych zgodnie z prawem Moore'a będzie przybierać na sile. Już dziś, jak donoszą uciekinierzy z Korei Północnej, kształci się tam elitę hakerów. Dziesięciolatki przejawiające zdolności informatyczne poznają języki programowania i tajniki związane z konstruowaniem narzędzi do cyberataków.

Człowiek, nawiązując kontakty przez medium, nie może być pewien istnienia swojego rozmówcy ani jego intencji. Dziś rozmawia się z systemami pomocy, automatami na infoliniach. Strony internetowe firm mają wirtualnych doradców. Dzisiejsze programy uczą się ludzi, których wybory i preferencje są analizowane przez systemy inteligentne, by służyć później profilowaniu. Niepewność istnienia drugiego człowieka,

a także konstruowanie robotów, humanoidów podobnych do zwierząt i ludzi sprawia, że technologie traktuje się jak żywe stworzenia. Przedmioty te mogą symulować ludzkie emocje (przez gesty, mimikę). Coraz częściej systemy te korzystają z asocjacji językowych. Powstają roboty do towarzystwa spełniające oczekiwania ich właścicieli. Celem działań dzisiejszych naukowców jest połączenie chipa z funkcjami mózgu. Otworzy to zupełnie nowe możliwości, np. łączące się z rozwojem medycyny. Osiągnięcia te będą zmierzały ku przeniesieniu świadomości człowieka w ciało maszyny. Jeśli tak się stanie, spełni się największe marzenie człowieka o nieśmiertelności. Trudno więc jest przewidzieć kierunki tych zmian. Człowiek stanie przed nowymi wyzwaniami związanymi z jego relacją z technologią (światami wirtualnymi, nadrealnością, hologramami), mając swoją naturę stworzoną przez geny i społeczeństwo. Przyszłość ta jest niepewna. Geny będą modyfikowane, społeczeństwo będzie miało charakter sieciowy. Jak będzie przebiegać proces uczenia się i nabywania wartości? Skąd młodzi ludzie będą czerpali wzorce? Zmiany, którym podlega dzisiejszy świat pod wpływem technologii, są czymś zupełnie nieznanym w skali istnienia człowieka jako gatunku.

Czy pedagog jest zatem w stanie w pełni przygotować nowe pokolenie do tak szybkich zmian? Czy wykłady uniwersyteckie mogą okazać się pomocne i znaleźć zastosowanie chociaż w jednej sytuacji problemowej zaistniałej w życiu dziecka i nastolatka, a związanej z przestrzenią wirtualną? Odpowiedź na powyższe pytania jest niezmiernie trudna i wymaga wielu analiz, badań oraz wnioskowania o charakterze wizjonerskim. W literaturze pedagogicznej są obecne głosy, że technologie edukacyjne mogą zastąpić nauczyciela.

Oczywiście technologie rozpatrywane w kontekście narzędzi są społecznie neutralne, nie stanowią zagrożeń oraz nie dają szans na lepsze życie. Ich afordancja wynika głównie z zamysłu oraz charakteru ich twórców oraz samych użytkowników, którzy niejednokrotnie gubią się w wolności wyborów.

Autorki prezentowanej książki mają jednak nadzieję, że jej lektura choć w niewielkim stopniu przyczyni się do kształtowania postawy odpowiedzialnego i bezpiecznego korzystania z narzędzi współczesnej kultury, jaką jest Internet oraz media społecznościowe.

Bibliografia

A human rights response to government hacking, https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf (dostęp: 23.08.2019).

Aftab P., *Internet a dzieci. Uzależnienia i inne niebezpieczeństwa*, tłum. B. Nicewicz, Prószyński i S-ka, Warszawa 2003.

Akera A., *Calculating a natural world. Scientists, engineers, and computers during the rise of U.S. cold war research*, MA: MIT Press (Inside technology), Cambridge 2007.

Alpine Security, *Hacker hat colors: An inside look at the hacking ecosystem*, https://www.alpinesecurity.com/blog/hacker-hat-colors-an-inside-look-at-the-hacking-ecosystem (dostęp: 24.07.2019).

Álvarez-García D. i in., *Risk factors associated with cybervictimization in adolescence*, „International Journal of Clinical and Health Psychology" 2015, 15(3).

Avast, *Botnet*, https://www.avast.com/pl-pl/c-botnet (dostęp: 30.09.2019).

Barlińska J., *Cyberprzemoc u adolescentów – o roli medium, własnych doświadczeń i empatii w zachowaniach świadków rówieśniczej przemocy elektronicznej*, praca doktorska napisana pod kier. dr hab. Anny Szuster-Kowalewicz, prof. UW, Warszawa 20013, http://depotuw.ceon.pl/bitstream/handle/item/265/doktorat.pdf?sequence=1 (dostęp: 3.05.2020).

Barlińska J., Lalak D., Szuster A., *Jak skutecznie ograniczyć cyberprzemoc rówieśniczą? – o efektywności metod aktywizujących kompetencje społeczne ze szczególnym uwzględnieniem empatii*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2018, 17(1), http://dzieckokrzywdzone.fdds.pl/index.php/DK/article/view/659/516 (dostęp: 3.05.2020).

Barlińska J., Szuster A., *Cyberprzemoc. O zagrożeniach i szansach na ograniczenie zjawiska wśród adolescentów*, Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 2014.

Bartmiński J., *Styl potoczny*, w: J. Anusiewicz, Fr. Nieckula (red.), *Język a Kultura*, t. 5: *Potoczność w języku i kulturze*, Wiedza o Kulturze, Wrocław 1992.

Bednarek J., *Multimedia w kształceniu*, Wydawnictwo Naukowe PWN, Warszawa 2006.

Belsey B., *Always on? Always aware!*, strona internetowa poświęcona problemowi cyberprzemocy, http://www.cyberbullying.ca/ (dostęp: 22.08.2019).

Beran T., Li Q., *The relationship between cyberbullying and school bullying*, „Journal of Student Wellbeing" 2007, 1(2).

Bezpieczna Szkoła. Procedury reagowania w przypadku wystąpienia wewnętrznych i zewnętrznych zagrożeń fizycznych w szkole, https://www.cyfrowa-szkola.info/wp-content/uploads/2017/10/Procedury-reagowania-w_2.pdf (dostęp: 3.05.2020).

Black Hat, *Portrait of an imminent cyberthreat*, 2017, https://www.blackhat.com/docs/us-17/2017-Black-Hat-Attendee-Survey.pdf (dostęp: 29.07.2019).

Bochenek M., Lange R. (eds.), *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów*, Państwowy Instytut Badawczy NASK, Warszawa 2019, https://www.nask.pl/download/30/2601/RAPORTNASTOLATKI2019.pdf (dostęp: 10.04.2019).

Bocij P., *The dark side of the Internet*, Praeger Publishers, London 2006.

Boczoń W., *1,8 tys. stwierdzonych przestępstw dotyczących e-bankowości w 2017 r. Zobaczcie statystyki KGP*, https://prnews.pl/18-tys-stwierdzonych-przestepstw-dotyczacych-e-bankowosci-2017-r-zobaczcie-statystyki-kgp-432171 (dostęp: 16.09.2019).

Boczoń W., *Uważajcie! Te programy na Androida mogą generować nakładki na aplikacje mobilne polskich banków*, https://www.cyberdefence24.pl/hakerzy-wykorzystuja-whatsapp-do-zlosliwych-celow-element-szerszej-kampanii (dostęp: 29.09.2019).

Borkowska A., *Cyberprzemoc – włącz blokadę na nękanie*, Państwowy Instytut Badawczy NASK, Warszawa 2019, https://www.gov.pl/attachment/6d56e2fc-abfb-4983-b5ac-578064342c6a (dostęp: 17.08.2019).

Bratus S., *Hacker curriculum: How hackers learn networking*, „IEEE Distributed Systems Online" 2007, 8(10).

Brenner S.W., Rehberg M., "*Kiddie Crime?" The utility of criminal law in controlling cyberbullying*, „First Amendment Law Review" 2010, 8.

Brewer G., Kerslake J., *Cyberbullying, self-esteem, empathy and loneliness*, „Computers in Human Behavior" 2015, 48.

Bulandra A., Kościołek J., *Przeciwdziałanie mowie nienawiści. Podręcznik dla środowiska politycznego*, https://www.google.com/url?sa=t&rct=j&q=-&esrc=s&source=web&cd=11&cad=rja&uact=8&ved=2ahUKEwjBnKDOgKXpAhXPy6YKHQmVBsI4ChAWMAB6BAgBEAE&url=http%3A%2F%2Finterkulturalni.pl%2Fplik.php%3Fid%3D148&usg=AOvVaw2u-SqLzbu9svAT2iV19FDi4 (dostęp: 3.05.2020).

Caldwell T., *Ethical hackers: Putting on the white hat*, „Network Security" 2011, 7.

Cattaneo L., Cho S., Botuck S., *Describing intimate partner stalking over time: An effort to inform victim-centered service provision*, „Journal of Interpersonal Violence" 2011, 26(17).

Centers for Disease Control and Prevention, *What are the consequences?*, https://www.cdc.gov/violenceprevention/youthviolence/bullyingresearch/fastfact.html (dostęp: 5.10.2019).

CERT Orange Polska, *Malvertisment, czyli biznes pełną gębą*, https://www.cert.orange.pl/aktualnosci/malvertisment-czyli-biznes-pelna-geba (dostęp: 10.10.2019).

Coleman G.E., *Coding freedom. The ethics and aesthetics of hacking*, Princeton University Press, Princeton–New York 2013.

Coleman G.E., *Hacker, hoaxer, whistleblower, spy. The many faces of anonymous*, Verso, London–New York 2014.

Coloroso B., *The bully, the bullied and the bystander*, Quill. Harper Collins, New York 2002.

Conway M., *Cyberterrorism: The story so far*, „Journal of Information Warfare" 2003, 2(2).

Cox L., Speziale B., *Survivors of stalking: Their voices and lived experiences*, „Affilia" 2009, 24(1).

Cupach W.R., Spitzberg B.H., *The dark side of relationship pursuit*, Lawrence Erlbaum Associates, Inc., Mahway 2004.

Cybrary, *7 types of hackers you should know*, https://www.cybrary.it/0p3n/types-of-hackers (dostęp: 24.07.2019).

Cyfrowobezpieczni.pl, Bezpieczna Szkoła Cyfrowa, https://www.cyfrowobezpieczni.pl/biblioteka-materialow/scenariusze-lekcji (dostęp: 20.08.2019).

Czaplicka M., *Hejt w internecie. Raport ilościowy*, https://prowly-uploads.s3.amazonaws.com/uploads/landing_page_image/image/11744/raport--o-hejcie-w-sieci.pdf (dostęp: 3.05.2020).

d'Haenens L., Vandoninck S., Donoso V., *How to cope and build online resilience?*, United Kingdom, Europe: EU Kids Online, 2013, http://eprints.lse.ac.uk/48115/1/How%20to%20cope%20and%20build%20online%20resilience%20%28lsero%29.pdf (dostęp: 5.10.2019).

Denning D., *Activism, hacktivism and cyberterrorism. The Internet as a tool for influencing*, w: J. Arquilla, D. Ronfeldt (eds.), *Networks and netwars. The future of terror, crime and militancy*, RAND Corporation, Santa Monica 2001.

Devost M., Houghton B., Pollard N., *Information terrorism: Political violence in the information age*, „Terrorism and Political Violence" 1997, 9(1).

Długosz D., *Simjacker to kolejne zagrożenie dla telefonów. Hakerzy mogą w ten sposób wykradać dane*, „Komputer Świat", https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/simjacker-to-kolejne-zagrozenie-dla-telefonow-hakerzy-moga-w-ten-sposob-wykradac-dane/8p54gd6?utm_source=www.komputerswiat.pl_viasg_komputerswiat&utm_medium=referal&utm_campaign=leo_automatic&srcc=ucs&utm_v=2 (dostęp: 22.09.2019).

Długosz D., *WIBattack to nowe zagrożenie dla kart SIM. Hakerzy mogą wysyłać wiadomości i lokalizować telefon*, „Komputer Świat", https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/wibattack-to-nowe-zagrozenie-dla-kart-sim-hakerzy-moga-wysylac-wiadomosci-i/tz4nt1p (dostęp: 23.09.2019).

Doroziński D., *Hakerzy. Technoanarchiści cyberprzestrzeni*, Helion, Gliwice 2001.

Douglas K.S., Dutton D.G., *Assessing the link between stalking and domestic violence*, „Aggression and Violent Behavior" 2002, 6.

eGospodarka, *10 ulubionych narzędzi cyberprzestępcy*, http://www.egospodarka.pl/130511,10-ulubionych-narzedzi-cyberprzestepcy,1,12,1.html (dostęp: 26.08.2019).

Encyklopedia wirusów, *Trojan-Downloader.Win32.Dila*, http://www.wiruspc.pl/encyclopedia/id,11921/trojan-downloader.win32.dila.html (dostęp: 30.09.2019).

Ericson J., *Hacking. Sztuka penetracji*, tłum. M. Rogóż, Helion, Gliwice 2008.

Facebook z dwoma miliardami użytkowników miesięcznie, https://www.wirtualnemedia.pl/artykul/ilu-uzytkownikow-ma-facebook-dwa-miliardy# (dostęp: 3.05.2020).

Fakt24, *Masz taki telefon? Jesteś na celowniku hakerów*, https://www.fakt.pl/facet/technologie/posiadacze-smartfonow-na-celowniku-hakerow/jdsqewr (dostęp: 30.09.2019).

Farnham F.R., James D.J., Cantrell P., *Association between violence, psychosis, and relationship to victim in stalkers*, „The Lancet" 2000, 355(15).

Farnicka M., Liberska H., Niewiedział D., *Psychologia agresji: wybrane problemy*, Wydawnictwo Naukowe PWN, Warszawa 2016.

Fletcher A. i in., *Brief report: Cyberbullying perpetration and its associations with socio-demographics, aggressive behaviour at school, and mental health outcomes*, „Journal of Adolescence" 2014, 37(8).

Fliciński P., Wojtowicz S., *Hip-hop słownik*, Wydawnictwo Naukowe PWN, Warszawa 2007.

Forward S., Buck C., *Toksyczne namiętności*, tłum. K. Drozdowski, Jacek Santorski & CO, Warszawa 1997.

Frączek A., *Czynności agresywne jako przedmiot studiów eksperymentalnej psychologii społecznej*, w: A. Frączek (red.), *Studia nad psychologicznymi mechanizmami czynności agresywnych*, Ossolineum, Wrocław 1979.

Fundacja Orange, *Strefa wiedzy dla nauczycieli i wolontariuszy*, https://fundacja.orange.pl/strefa-wiedzy/dla-nauczycieli-i-wolontariuszy (20.08.2019).

Gajda J., *Agresja językowa w stosunkach międzyludzkich*, w: W. Gruszczyński (red.), *Język narzędziem myślenia i działania*, Dom Wydawniczy ELIPSA, Warszawa 2002.

Gilbert P., *The Relationship of shame, social anxiety and depression: The role of the evaluation of social rank*, „Clinical Psychology and Psychotherapy" 2000, 7(3).

Goban-Klas T., *Komunikowanie i media*, s. 3, http://users.uj.edu.pl/~usgoban/files/socjologia_mediow_zarys.pdf (dostęp: 12.12.2019).

Gradinger P., Strohmeier D., Spiel C., *Definition and measurement of cyberbullying. Cyberpsychology*, „Journal of Psychosocial Research on Cyberspace" 2010, 4(2), https://cyberpsychology.eu/article/view/4235/3280 (dostęp: 5.10.2019).

Gromnicka D., *Asertywność w przykładach. Jak się zachowywać w typowych sytuacjach*, „Samo Sedno", Edgard, Warszawa 2015.

Groth J., *Cyberstalking – perspektywa psychologiczna*, „Forum Oświatowe" 2010, 2(43).

Grzesiak M., *8 sposobów na uwolnienie się od opinii innych*, https://mateuszgrzesiak.pl/8-sposobow-uwolnienie-sie-opinii-innych/ (dostęp: 3.05.2020).

Hacker.com.pl, https://haker.com.pl/threads/21204-Dziennik-elektroniczny (dostęp: 14.09.2019).

Hackerone, *2016 Bug Bounty Hacker Report*, https://www.hackerone.com/sites/default/files/2017-05/HackerOne%202016%20Bug%20Bounty%20Report.pdf (dostęp: 25.07.2019).

Hackerone, *The 2018 Hacker Report*, https://www.hackerone.com/sites/default/files/2018-01/2018_Hacker_Report_0.pdf (dostęp: 9.08.2019).

Haker przejął kontrolę nad telefonem i ukradł 13 tys. zł z konta w banku, https://www.polsatnews.pl/wiadomosc/2018-08-22/przejal-kontrole-nad-telefonem-i-ukradl-13-tys-zl-z-konta-w-banku/ (dostęp: 26.09.2019).

Hamza M., College N., *Cybercrime and security*, https://www.researchgate.net/publication/322086317_CyberCrime_and_Security (dostęp: 22.07.2019).

Hare R.D., *Psychopathy: A clinical construct whose time has come*, „Criminal Justice Behavior" 1996, 23.

Herpig S., *Government hacking, global challenge*, https://www.stiftung-nv.de/sites/default/files/government_hacking_akt.feb_.pdf (dostęp: 23.08.2019).

Hinduja S., Patchin J.W., *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*, Corwin Press, Thousand Oaks 2015.

Hołyst B., *Kryminologia*, Lexis Nexis, Warszawa 2004.

Informacja o wynikach kontroli. Zapobieganie i przeciwdziałanie cyberprzemocy wśród dzieci i młodzieży, NIK, Warszawa 2017, s. 19, https://www.nik.gov.pl/plik/id,15249,vp,17730.pdf (dostęp: 25.10.2019).

Inteligentne urządzenia w Twoim domu, „OUCH! Biuletyn Bezpieczeństwa Komputerowego", sierpień 2018, Web:https://www.sans.org/sites/default/files/2018-07/201808-OUCH-August-Polish_0.pdf (dostęp: 28.09.2019).

INTERIA.PL/Policja, https://fakty.interia.pl/polska/news-wlamal-sie-do-elektronicznego-dziennika-i-poprawil-oceny,nId,2251580#utm_source=paste&utm_medium=paste&utm_campaign=firefox (dostęp: 14.09.2019).

ISAP – Internetowy System Aktów Prawnych, strona główna Sejmu Rzeczpospolitej Polskiej, http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001530 (dostęp: 13.09.2019).

Jasik A., *Wyzwiska, obelgi, pogróżki w gwarze uczniowskiej (próba typologii gatunku)*, w: A. Dąbrowska, A. Nowakowska (red.), *Język a Kultura*, t. 17: *Życzliwość i agresja w języku i kulturze*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2005.

Joinson A., *Disinhibition and the Internet*, w: Gackenbach J. (ed.), *Psychology and the Internet: Intrapersonal, interpersonal, and transpersonal implications*, Academic Press, Amsterdam 2007.

Jonak Ł., *Dlaczego boimy się jednego procenta? O braku agresji w Internecie*, w: K. Krejtz (red.), *Internetowa kultura obrażania?*, Interactive Advertising Bureau Polska, Szkoła Wyższa Psychologii Społecznej oraz Ośrodek Przetwarzania Informacji, s. 57–66, http://komentuj-nie-obrazaj.pl/media/KOraport.pdf (dostęp: 3.05.2020).

Jordan T., Taylor P., *Hacktivism and cyberwars. Rebels with a cause?*, Routledge, London 2004.

Kariera w cyberbezpieczeństwie, „OUCH! Biuletyn Bezpieczeństwa Kompu terowego", maj 2019, https://www.sans.org/sites/default/files/2019-04/201905-OUCH-May-Polish.pdf (dostęp: 23.08.2019).

Kim S. i in., *Cyberbullying victimization and adolescent mental health: Evidence of differential effects by sex and mental health problem type*, „Journal of Youth and Adolescence" 2018, 47(3).

km, *4/5 Polaków ma program antywirusowy w prywatnym pececie. Avast najpopularniejszy*, https://www.wirtualnemedia.pl/artykul/4-5-polakow-ma-program-antywirusowy-w-prywatnym-pececie-avast-najpopularniejszy (dostęp: 28.08.2019).

Kosińska J., *Prawnokarna problematyka stalkingu*, „Prokuratura i Prawo" 2008, 10.

Kowalski R.M. i in., *Bullying in the digital age. A critical review and meta-analysis of cyberbullying research among youth*, „Psychological Bulletin" 2014, 140.

Kowalski R.M., Limber S.P., *Psychological, physical and academic correlates of cyberbullying and traditional bullying*, „Journal of Adolescent Health" 2013, 53(1).

Kowalski R.M., Limber S.P., McCord A., *A developmental approach to cyberbullying: Prevalence and protective factors*, „Aggression and Violent Behavior" 2019, 45.

Raport roczny 2018 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego Internetu, https://www.cert.pl/PDF/Raport_CP_2017.pdf (dostęp: 30.09.2019).

Krejtz K., Kolenda P., *W jaki sposób badać kulturę wypowiedzi w internecie?*, w: K. Krejtz (red.), *Internetowa kultura obrażania?*, Interactive Advertising Bureau Polska, Szkoła Wyższa Psychologii Społecznej oraz Ośrodek Przetwarzania Informacji, 2012, s. 17–24, http://komentuj-nieobrazaj.pl/media/KOraport.pdf (dostęp: 3.05.2020).

Kupczyk K., *Stalking w Polsce jest coraz częstszy. Czym jest cyberstalking i jak mu zapobiegać?*, Spy Shop blog, 2016, https://www.spyshop.pl/blog/infografiki-stalking-w-polsce-jest-coraz-czestszy-czym-jest-cyberstalking-i-jak-mu-zapobiegac/ (dostęp: 3.05.2020).

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.

Leszczyński A., *Rosyjscy hakerzy manipulują prezydenckimi wyborami w USA*, http://wyborcza.pl/7,75400,20928764,rosyjscy-hakerzy-manipuluja-prezydenckimi-wyborami-w-usa.html (dostęp: 30.09.2019).

Levy S., *Hackers. Heroes of the computer revolution. 1st (25th anniversary edition)*, O'Reilly, Beijing–Cambridge, UK–Farnham–Koeln–Sebastopol––Tokyo 2010.

Liberska H., *Perspektywy temporalne młodzieży. Wybrane uwarunkowania*, Wydawnictwo Naukowe UAM, Poznań 2004

Lindberg D., *Prevention of cyberstalking: A review of the literature*, Criminology and Criminal Justice Senior Capstone Project, Portland State University 2012.

Littman J., *The fugitive game: Online with Kevin Mitnick*, Little, Brown and Co, New York 1996.

Maczeta atakuje! Hakerzy wykradali dane wojsku, Superbiznes, https://superbiz.se.pl/technologie/maczeta-atakuje-hakerzy-wykradali-dane-wojsku-aa-5rbh-4QZ7-uHud.html (dostęp: 30.09.2019).

Majewska K., *Modern educational tools in the teacher's work*, „The New Educational Review" 2018, 51(1).

Majewska K., *The electronic register in Polish schools: Studies from the level of*

early school education, w: D. Siemieniecka (red.), *Virtuality and education: future prospects*, Wydawnictwo Adam Marszałek, Toruń 2019.

Markowska B., *Jacy „my" i jacy „oni"? Analiza semantyczna nazw i etykiet*, w: X. Bukowska, B. Markowska (red.), *To oni są wszystkiemu winni… Język wrogości w polskim dyskursie publicznym*, Trio, Warszawa 2013.

Mates M., *Technology and terrorism*, https://www.tbmm.gov.tr/ul_kom/natopa/raporlar/bilim%20ve%20teknoloji/AU%20121%20STC%20Terrorism.htm (dostęp: 22.08.2019).

Maurushat A., *Ethical hacking*, University of Ottawa Press, Ottawa 2019.

McCoy C., Potate M., McKinney C., *Cyberbullying*, w: P. Triggs, *Handbook on bullying: Prevalence, psychological impacts and intervention strategies*, Nova Science Publishers, Inc., New York 2014.

McKenna K.Y.A., Bargh J.A., *Plan 9 from cyberspace: The implications of the Internet for personality and social psychology*, „Personality and Social Psychology Review" 2000, 4(1).

Mead M., *Kultura i tożsamość. Studium dystansu międzypokoleniowego*, tłum. J. Hołówka, Wydawnictwo Naukowe PWN, Warszawa 1978.

Mejssner B., *Blokują komputer i żądają okupu*, https://pieniadze.rp.pl/finanse-domowe/12585-blokuja-komputer-zadaja-okupu (dostęp: 16.09.2019).

Melnichuk D., *The hacker's underground. Handbook: Learn what it takes to crack even the most secure systems*, Createspace, Lexington 2008.

Melosik Z., *Edukacja, młodzież i kultura współczesna: kilka uwag o teorii i praktyce pedagogicznej*, „Chowanna" 2003, 1.

Meloy J.R. (ed.), *Forensic perspectives*, Academic Press, London 1998.

Meloy J.R., *The psychology of stalking*, w: J.R. Meloy (ed.), *The psychology of stalking: Clinical and forensic perspectives*, Academic Press, London 2010.

Meloy J.R., Gothard S., *A demographic and clinical comparison of obsessional followers and offenders with mental disorders*, „American Journal of Psychiatry" 1995, 152.

Messier R., *CEH v10 certified ethical hacker study guid*e, John Wiley & Sons, New York 2019.

Miller S.L., Smolter N.L., *"Paper abuse": When all else fails, batterers use procedural stalking*, „Violence Against Women" 2011, 17(5).

Mullen P. i in., *A study of stalkers*, „The American Journal of Psychiatry" 1999, 156.

Mullen P.E., Pathé M., Purcell R., *Stalkers and their victims*, Cambridge University Press, Cambridge 2009.

Myers D.G., *Psychologia społeczna*, tłum. A. Bezwińska-Walerjan, Zysk i S-ka, Poznań 2003.

Naruszewicz-Duchlińska A., *Nienawiść w czasach Internetu*, Novae Res, Gdynia 2015.

National Institute of Justice Research Report 1998, *Domestic violence and stalking: The third annual report to Congress under the Violence against Women Act*, US Department of Justice, Office of Justice Programs, https://babel.hathitrust.org/cgi/pt?id=osu.32437121067694;view=1up;seq=12 (dostęp: 3.05.2020).

Nixon Ch.L., *Current perspectives: The impact of cyberbullying on adolescent health*, „Adolescent Health, Medicine and Therapeutics" 2014, 5, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4126576/ (dostęp: 28.11.2019).

Nöllke M., *Asertywność i sztuka celnej riposty*, tłum. A. Komin, Wydawnictwo BCedu, Warszawa 2010.

Notar Ch.E., Padgett S., Roden J., *Cyberbullying: A review of the literature*, „Universal Journal of Educational Research" 2013, 1(1).

Nowicka I., *Zjawisko stalkingu w kontekście resocjalizacji penitencjarnej kilka uwag,* „Humanistyczne Zeszyty Naukowe – Prawa Człowieka" 2017, 1(20), http://www.humanrights.com.pl/pdf/Tom20/10.%20Izabela%20NOWICKA%20-%20Zjawisko%20stalkingu%20w%20kontek%C5%9Bcie%20resocjalizacji%20penitencjarnej.%20Kilka%20uwag.pdf (dostęp: 3.05.2020).

Nowicka M., *Dyskurs o dyskursie, czyli o mowie wrogości przy pomocy mowy wrogości*, w: X. Bukowska, B. Markowska (red.), *To oni są wszystkiemu winni… Język wrogości w polskim dyskursie publicznym*, Trio, Warszawa 2013.

Obuchowska I., *Drogi dorastania. Psychologia rozwojowa okresu dorastania dla rodziców i wychowawców*, WSiP, Warszawa 1996.

Olweus D., *A profile of bullying at school*, „Educational Leadership" 2003, 60(6).

Olweus D., *Mobbing – fala przemocy w szkole. Jak ją powstrzymać?*, tłum. D. Jastrun, Jacek Santorski & Co Agencja Wydawnicza, Warszawa 2007.

Oszustwa za pośrednictwem mediów społecznościowych, „OUCH! Biuletyn Bezpieczeństwa Komputerowego", wrzesień 2019, https://www.sans.org/

sites/default/files/2019-09/201909-OUCH-September-Polish.pdf (dostęp: 26.08.2019).

Palczewski S., *Hakerzy wykorzystują WhatsApp do złośliwych celów. Element szerszej kampanii*, https://www.cyberdefence24.pl/hakerzy-wykorzystuja-whatsapp-do-zlosliwych-celow-element-szerszej-kampanii (dostęp: 29.09.2019).

PAP, *43 proc. wszystkich prób logowania do usług to działania hakerów*, https://businessinsider.com.pl/technologie/prawie-polowa-prob-logowan-do-uslug-to-dzialania-hakerow/p1hh11g (dostęp: 28.09.2019).

PAP, *Hakerzy atakują infrastrukturę ochrony zdrowia w Europie i USA*, http://www.rynekzdrowia.pl/Technologie-informacyjne/Hakerzy-atakuja-infrastrukture-ochrony-zdrowia-w-Europie-i-USA,183924,7.html (dostęp: 29.09.2019).

PAP, *Rosyjscy hakerzy nasilają ataki przed wyborami do PE*, „Gazeta Prawna" 28.02.2019, https://www.gazetaprawna.pl/artykuly/1400365,rosyjscy-hakerzy-nasilaja-ataki-przed-wyborami-do-pe.html (dostęp: 29.09.2019).

PAP, *Zmasowany atak w całej Europie i USA. Hakerzy wzięli na celownik banki, firmy, instytucje rządowe*, https://businessinsider.com.pl/wiadomosci/atak-hakerski-w-europie-na-celowniku-banki-i-lotnisko/vlhd68n (dostęp: 30.09.2019).

Parents can prevent cyberbullying, oficjalna strona internetowa National Parent Teacher Association, https://www.pta.org/home/family-resources/safety/Digital-Safety/Parents-Can-Prevent-Cyberbullying (dostęp: 6.11.2019).

Peisert M., *Formy i funkcje agresji werbalnej. Próba typologii*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2004.

Pieczyńska-Chamczyk M., *Uczniowie sami sobie poprawili oceny w dzienniku*, https://www.asta24.pl/2017/06/20/uczniowie-poprawili-oceny-dzienniku (dostęp: 13.09.2019).

Pielichowski J., *Kompendium prawno-psychologiczne z zakresu stalkingu*, „Wiedza Prawnicza" 2013, 6/201, http://www.wiedzaprawnicza.pl/teksty/6-2013/6-2013.pdf (dostęp: 3.05.2020).

Polska – reagowanie na mowę nienawiści, 2018, https://www.article19.org/wp-content/uploads/2018/04/Poland-Hate-Speech-report%E2%80%94-Polish.pdf (dostęp: 3.05.2020).

Polskie Centrum Programu Safer Internet, saferinternet.pl (dostęp: 20.08.2019).

Polskie Radio, *Cyberatak na międzynarodową skalę. Świat walczy ze skutkami działania hakerów*, https://www.polskieradio.pl/5/3/Artykul/178243-4,Cyberatak-na-miedzynarodowa-skale-Swiat-walczy-ze-skutkami-dzialania-hakerow (dostęp: 30.09.2019).

Portal o unijnym rozporządzeniu o ochronie danych osobowych, Artykuł 82 – Prawo do odszkodowania i odpowiedzialność, https://gdpr.pl/baza-wiedzy/akty-prawne/interaktywny-tekst- gdpr/artykul-82-prawo-do-odszkodowania-i-odpowiedzialnosc (dostęp: 13.09.2019).

Prevent cyberbullying, stopbullying.gov, oficjalna strona internetowa rządu Stanów Zjednoczonych, https://www.stopbullying.gov/cyberbullying/prevention (dostęp: 11.11.2019).

Proofpoint, *Report. Understanding email fraud. A global survey of IT leaders in the US, The UK, Australia, France and Germany, 2017*, https://www.proofpoint.com/sites/default/files/pfpt-us-tr-survey-of-understanding-email-fraud-180315.pdf (dostęp: 30.09.2019).

Przemoc wobec kobiet. Badanie na poziomie Unii Europejskiej, Urząd Publikacji Unii Europejskiej, Luksemburg 2014, http://europe-direct.kolobrzeg.eu/wp-content/uploads/2010/12/Przemoc-wobec-kobiet.pdf (dostęp: 3.05.2020).

Puzynina J., *Słowo – wartość – kultura*, Towarzystwo Naukowe Katolickiego Uniwersytetu Lubelskiego, Lublin 1997.

PwC, *Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście*, https://www.pwc.pl/pl/pdf/publikacje/2018/cyber-ruletka-po-polsku-raport-pwc-gsiss-2018.pdf (dostęp: 30.09.2019).

Pyżalski J., *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Oficyna Wydawnicza Impuls, Kraków 2012.

Pyżalski J., *Agresja elektroniczna wśród dzieci i młodzieży*, GWP, Sopot 2011.

Pyżalski J., *Polscy nauczyciele i uczniowie a agresja elektroniczna – zarys teoretyczny i najnowsze wyniki badań*, w: M. Jędrzejko, D. Sarzała (red.), *Człowiek i uzależnienia*, Akademia Humanistyczna im. Aleksandra Gieysztora, OficynaWydawnicza ASPRA-JR, Pułtusk–Warszawa 2010.

Pyżalski J. i in., *Polskie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski*, Wydawnictwo Naukowe UAM, Poznań 2019, https://fundacja.orange.pl/files/user_files/EU_Kids_Online_2019_v2.pdf (dostęp: 22.07.2019).

Raport „Nastolatki 3.0". Wybrane wyniki ogólnopolskiego badania uczniów w szkołach, Państwowy Instytut Badawczy NASK, 2016, https://akademia.nask.pl/badania/RAPORT%20-%20Nastolatki%203.0%20-%20wybrane%20wyniki%20bada%C5%84%20og%C3%B3lnopolskich.pdf (dostęp: 10.04.2019).

Reber A.S., *Słownik psychologii*, red. nauk. I. Kurcz, K. Skarżyńska, Scholar, Warszawa 2000.

Redakcja WebSecurity, *Wirusy, trojany, robaki… Co to jest malware?*, http://websecurity.pl/wirusy-trojany-robaki-co-to-jest-malware/ (dostęp: 26.08.2019).

Rekomendacja nr R (97) 20 Komitetu Ministrów Rady Europy nt. mowy nienawiści (Recommendation No. R (97) 20 of The Committee of Ministers to Member States on „Hate Speech"), https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680505d5b (dostęp: 10.10.2019).

Reykowski J., *Autorytaryzm a agresja wobec swoich i obcych*, w: Ł. Jurasz-Dudzik (red.), *Człowiek i agresja. Głosy o nienawiści przemocy. Ujęcie interdyscyplinarne*, Sic!, Warszawa 2002.

Różyło A., *Agresja werbalna. Próba klasyfikacji o inspiracji kognitywnej*, http://pedkat.pl/images/czasopisma/pk8/art19.pdf (dostęp: 3.05.2020).

Rudy-Murza M., *Internetowe lustro autoprezentacji*, Wydawnictwo Adam Marszałek, Toruń 2011.

Rybak M., *Hakerzy atakują i szantażują. Żądają okupu płaconego w bitcoinach*, „Gazeta Wrocławska", https://gazetawroclawska.pl/hakerzy-atakuja-i-szantazuja-zadaja-okupu-placonego-w-bitcoinach/ar/13680536 (dostęp: 29.09.2019).

Rzeczpospolita Polska, Ministerstwo Spraw Zagranicznych, *Zapobieganie i zwalczanie terroryzmu*, https://www.msz.gov.pl/pl/polityka_zagraniczna/polityka_bezpieczenstwa/zwalczanie_terroryzmu_miedzynarodowego/zapobieganie_i_zwalczanie_terroryzmu/page_3005 (dostęp: 29.09.2019).

Salmivalli C., *Participant role approach to school bullying: Implications for interventions*, „Journal of Adolescence" 1999, 22(4).

Salmivalli C., Voeten M., Poskiparta E., *Bystanders matter: Associations between reinforcing, defending, and the frequency of bullying behavior in classrooms*, „Journal of Clinical Child & Adolescent Psychology" 2011, 40(5).

Savage K., Coogan P., Lau H., *The evolution of ransomware*, Version 1.0 – August 6, 2015, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf (dostęp: 16.09.2019).

Sekurak, *Czym jest SQL injection?*, https://sekurak.pl/czym-jest-sql-injection/ (dostęp: 26.08.2019).

Sher H., *Cyberterror should be international crime – Israeli minister*, „Newsbytes" 2000, November 10.

Sheridan L., Boon J., *Stalkers typologies: Implications for law enforcement*, w: L. Sheridan, J. Boon (eds.), *Stalking and psychosexual obsession. Psychological perspectives for prevention, policing and treatment*, John Wiley & & Sons, Chichester 2002.

Siemieniecka D., Skibińska M., *Stalking and cyberstalking as a form of violence*, „Society, Integration, Education" 2019, 3.

Siemieniecki B., Wiśniewska-Nogaj L., Kwiatkowska W., *Agresja – zjawisko, skutki, zapobieganie. Perspektywa pedagogiki kognitywistycznej, psychoprofilaktyki oraz edukacji moralnej*, Wydawnictwo Naukowe UMK, Toruń 2020.

Silic M., Silic D., Oblakovic G., *Influence of shadow IT on innovation in organizations*, „Complex Systems Informatics and Modeling Quarterly CSIMQ" 2016, 8 (September/October).

Skarżyńska-Sernaglia J., *Ciemna strona relacji interpersonalnych*, www.stalking.it (dostęp: 3.01.2019).

Skarżyńska-Sernaglia J., *Stalking w Polsce – występowanie i charakterystyka zjawiska*, http://psychologia.net.pl/artykul.php?level=415 (dostęp: 3.05.2020).

Skarżyńska-Sernaglia J., *Stalking: od miłości do zbrodni – nowe wyzwanie dla psychologii, kryminologii i zespołów interdyscyplinarnych przeciwdziałających przemocy*, Львівського державного університету внутрішніх справ НАУКОВИЙ ВІСНИК 1/2009 (Lviv State University of Internal Affairs, Collection of scientific works), http://www2.lvduvs.edu.ua/documents_pdf/visnyky/nvsp/01_2009/09ssjipp.pdf (dostęp: 3.05.2020).

Smahel D. i in., *EU Kids Online 2020: Survey results from 19 countries*, EU Kids Online, 2020, https://doi.org/10.21953/lse.47fdeqj01ofo (dostęp: 10.03.2020)

Smith P.K. i in., *Cyberbullying: Its nature and impact in secondary school pupils*, „The Journal of Child Psychology and Psychiatry", 2008, 49(4).

Smogulecka A., Sklepik K., *Poznań: młody haker zmieniał szkolne oceny*, https://gloswielkopolski.pl/poznan-mlody-haker-zmienial-szkolne-oceny/ar/376527 (dostęp: 14.09.2019).

Sobolewski S., *Stalking: uporczywe nękanie – opis przestępstwa*, 2017, http://adwokat-sobolewski.pl/stalking-uporczywe-nekanie/ (dostęp: 3.05.2020).

Social media (media społecznościowe), blog marketingwsieci.pl, https://marketingwsieci.pl/slownik-e-marketingu/social-media/ (dostęp: 22.07.2019).

Southworth C. i in., *Intimate partner violence, technology, and stalking*, „Violence Against Women" 2007, 13(8).

Sowińska K., *Haker zamienił życie czterech rodzin ze Słupska w koszmar*, https://gp24.pl/haker-zamienil-zycie-czterech-rodzin-ze-slupska-w-koszmar/ar/4788345 (dostęp: 28.09.2019).

Stalking risk profile, https://www.stalkingriskprofile.com/victim-support (dostęp: 3.05.2020).

Staszewski W., *Brzytwa w czarnym kapeluszu*, https://www.newsweek.pl/polska/spoleczenstwo/biale-szare-i-czarne-kapelusze-wsrod-hakerow/z6b7t3g (dostęp: 2.08.2019).

Stopbullying.gov, oficjalna strona internetowa rządu Stanów Zjednoczonych, https://www.stopbullying.gov/cyberbullying/what-is-it/index.html (dostęp: 11.11.2019).

Strykowski W., *Kompetencje medialne: pojęcie, obszary, formy kształcenia*, w: W. Strykowski, W. Skrzydlewski (red.), *Kompetencje medialne społeczeństwa wiedzy*, wyd. eMPi2, Poznań 2004.

Sutton B.B., *Cyberbullying: An interview with Parry Aftab*, „A Journal for Educational Technology & Change" 2011, https://etcjournal.com/2011/02/17/7299/ (dostęp: 28.11.2019).

Szopa B., *Nękanie w Internecie*, 2016, https://stalking.com.pl/2016/01/11/nekanie-w-internecie/ (dostęp: 3.05.2020).

Szopa B., *Nowelizacja przepisów dot. nękania? Surowsze kary dla stalkerów?*, 2018, https://stalking.com.pl/2018/10/15/nowelizacja-przepisow-dot-nekania-surowsze-kary-dla-stalkerow/ (dostęp: 3.05.2020).

Szopa B., *Stalking w Polsce – trochę statystyki*, 2015, https://stalking.com.pl/2015/09/29/stalking-w-polsce-statystyka/ (dostęp: 3.05.2020).

Szopa B., *Uporczywe nękanie – gdzie zgłosić?*, 2015, https://stalking.com.pl/2015/07/10/uporczywe-nekanie-gdzie-zglosic/ (dostęp: 3.05.2020).

Szulc M., *Sposoby radzenia sobie ze stresem i umiejscowienie poczucia kontroli u ofiar cyberprzemocy*, „Pomeranian Journal of Life Sciences" 2018, 3(64), http://ojs.pum.edu.pl/pomjlifesci/article/view/449 (dostęp: 3.05.2020).

The Homebrew Computer Club, *Computer History Museum*, https://www.computerhistory.org/revolution/personal-computers/17/312 (dostęp: 20.05.2019).

Tjaden P., Thoennes N., *Stalking in America: Findings from the national violence against women survey*, Department of Justice, National Institute of Justice, Washington 1998.

Tokunaga R.S., *Following you home from school: A critical review and synthesis of research on cyberbullying victimization*, „Computers in Human Behavior" 2010, 26(3).

Tomaszek K., *Stalker – psychologiczna charakterystyka sprawców przestępstw „uporczywego nękania"*, „Studia z Psychologii w KUL" 2012, 18, https://www.kul.pl/files/55/Stud_psych_18-2012_Tomaszek.pdf (dostęp: 3.05.2020).

Tomczyk Ł., Srokowski Ł., *Kompetencje w zakresie bezpieczeństwa cyfrowego w polskiej szkole*, raport z badań, Stowarzyszenie Miast w Internecie, Tarnów 2016, https://www.mwi.pl/uploads/filemanager/publikacje/Raport%20z%20badan_wersja%20finalna.pdf (dostęp: 14.09.2019).

Turne F., *From counterculture to cyberculture. Stewart brand, the Whole Earth Network, and the rise of digital utopianism*, University of Chicago Press, Chicago 2006.

Ushmani A., *Ethical hacking*, „International Journal of Information Technology" 2018, 4(6).

Utylizacja urządzenia mobilnego, „OUCH! Biuletyn Bezpieczeństwa Komputerowego", marzec 2019, https://www.sans.org/sites/default/files/2019-03/201903-OUCH-March-Polish_0.pdf (dostęp: 26.08.2019).

Völlink T., *Coping with cyberbullying: Differences between victims, bully-victims and children not involved in bullying*, „Journal of Community & Applied Social Psychology" 2013, 23(1).

Walby S., Allen J., *Domestic violence, sexual assault and stalking: Findings from the British Crime Survey*, Home Office Research, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.477.2558&rep=rep1&type=pdf (dostęp: 3.05.2020).

Wallace P., *Psychologia Internetu*, tłum. T. Hornowski, Rebis, Poznań 2004.

Walrave M., Heirman W., *Skutki „cyberbullyingu" – oskarżenie czy obrona technologii?*, tłum. A. Nowak, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2009, 8(1).

Westphal R. Jr (ed.), *War and virtual war. The challenges to communities*, Oxford, United Kingdom 2003.

Wawrzyniak M., *Hejtoholik, czyli jak zaszczepić się na hejt, nie wpaść w pułapkę obgadywania oraz nauczyć się zarabiać na tych, którzy Cię oczerniają*, Helion, Warszawa 2015.

Węgrzynowska J., *Dzieci doświadczające przemocy rówieśniczej*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2016, 15(1).

What methods work with the different kinds of cyberbullies?, http://www.stopcyberbullying.org/pdf/howdoyouhandleacyberbully.pdf (dostęp: 2019.11.28).

Whitty M.T., Carr A.N., *Wszystko o romansie w sieci. Psychologia związków internetowych*, tłum. T. Kościuszuk, GWP, Gdańsk 2009.

Why don't kids ask for help?, stopbullying.gov, oficjalna strona internetowa rządu Stanów Zjednoczonych, https://www.stopbullying.gov/cyberbullying/what-is-it/index.html (dostęp: 11.11.2019).

Wingate V.S., Minney J.A., *Cyberbullying requires more than a virtual response*, w: M.F. Wright (ed.), *A social-ecological approach to cyberbullying*, Nova Science Publishers, Inc., New York 2016.

Wirtualne Sieci Prywatne (VPN), „OUCH! Biuletyn Bezpieczeństwa Komputerowego", lipiec 2019, https://www.sans.org/sites/default/files/2019-06/201907-OUCH-July-Polish.pdf (dostęp: 26.08.2019).

Witosz B., *O dyskursie wykluczenia i dyskursach wykluczonych z perspektywy lingwistycznej*, „Tekst i Dyskurs – Text und Diskurs" 2010, 3.

Włodarczyk J., *Mowa nienawiści w internecie w doświadczeniu polskiej młodzieży*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2014, 13(2).

Wojtasik Ł., *Cyberprzemoc – charakterystyka zjawiska*, w: Ł. Wojtasik (red.), *Jak reagować na cyberprzemoc? Poradnik dla szkół*, wydanie II poprawione, Fundacja Dajemy Dzieciom Siłę, https://www.ore.edu.pl/wp-content/plugins/download-attachments/includes/download.php?id=3167 (dostęp: 11.11.2019).

Woźniakowska-Fajst D., *Nękanie emocjonalne (stalking) w doświadczeniu studentów Uniwersytetu Warszawskiego*, http://cejsh.icm.edu.pl/cejsh/ele

ment/bwmeta1.element.desklight-6c12e957-42fc-4884-8eb0-382a78532e77 (dostęp: 3.05.2020).

Woźniakowska-Fajst D., *Prawne możliwości walki ze zjawiskiem stalkingu*, 2009, http://iws.gov.pl/wp-content/uploads/2018/08/Prawne-mo%C5%BCliwo%C5%9Bci-zjawisko-stalkingu-IWS-po-korekcie-2-D-Wo%C5%BAniakowska.pdf (dostęp: 3.05.2020).

Woźniakowska-Fajst D., *Prawne możliwości walki ze zjawiskiem stalkingu – czy w prawie polskim potrzebna jest penalizacja prześladowania?*, 2009, https://www.inp.pan.pl/wp-content/uploads/2017/09/AK31-Wozniakowska.pdf (dostęp: 3.05.2020).

Woźniakowska-Fajst D., *Stalking i inne formy przemocy emocjonalnej. Studium kryminologiczne*, Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 2019.

Wright M.F., *Predictors of anonymous cyber aggression: The role of adolescents' beliefs about anonymity, aggression, and the permanency of digital content*, „Cyberpsychology, Behavior And Social Networking" 2014, 177.

Wright M.F., Li Y., *Normative beliefs about aggression and cyber aggression among young adults: A longitudinal investigation*, „Aggressive Behavior" 2013, 39(3).

Wysocki B., *Czy warto być hakerem?*, „EduAkcja. Magazyn Edukacji Elektronicznej" 2013, 1(5).

Znaniecki F., *Socjologia wychowania*, Wydawnictwo Naukowe PWN, Warszawa 2001.

Zona M.A., Sharma K.K., Lane J., *A comparative study of erotomanic and obsessional subjects in a forensic sample*, „Journal of Forensic Sciences" 1993, 38(4), July.

Zych I., Ortega-Ruiz R., DelRey R., *Systematic review of theoretical studies on bullying and cyberbullying: Facts, knowledge, prevention and intervention*, „Aggressive Violent Behaviour" 2015, 23.

Aneks

Tabela 1. Zagrożenia bezpieczeństwa cyfrowego w środowisku szkolnym i sposoby reagowania

Procedura 1	**Dostęp do treści szkodliwych, niepożądanych i nielegalnych**
Podstawy prawne uruchomienia procedury	Kodeks karny, regulamin szkoły
Rodzaj zagrożenia objętego procedurą	Zagrożenie łatwym dostępem do treści szkodliwych, niedozwolonych, nielegalnych i niebezpiecznych dla zdrowia (pornografia, treści obrazujące przemoc i promujące działania szkodliwe dla zdrowia i życia dzieci, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawoływanie do samookaleczeń i samobójstw, korzystania z narkotyków; niebezpieczeństwo werbunku dzieci i młodzieży do organizacji nielegalnych i terrorystycznych).
Telefony/kontakty alarmowe krajowe	dyzurnet@dyzurnet.pl, **tel. 801 615 005, policja 997**
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Opis okoliczności, analiza, zabezpieczenie dowodów	Reakcja szkoły w przypadku pozyskania wiedzy o wystąpieniu zagrożenia będzie zależna od tego, czy: (1) treści te można bezpośrednio powiązać z uczniami danej szkoły, czy też (2) treści nielegalne lub szkodliwe nie mają związku z uczniami danej szkoły, lecz wymagają kontaktu szkoły z odpowiednimi służbami. W pierwszej kolejności należy zabezpieczyć dowody w formie elektronicznej (pliki z treściami niedozwolonymi, zapisy rozmów w komunikatorach, e-maile, zrzuty ekranu), znalezione w Internecie lub w komputerze dziecka. Zabezpieczenie dowodów jest zadaniem rodziców lub opiekunów prawnych dziecka, w czynnościach tych może wspomagać ich przedstawiciel szkoły posiadający odpowiednie kompetencje techniczne. W przypadku sytuacji (1) rozwiązanie leży po stronie szkoły, zaś (2) należy rozważyć zgłoszenie incydentu na policję oraz zgłosić go do serwisu Dyżurnet.
Identyfikacja sprawcy(-ów)	W identyfikacji sprawców kluczowe znaczenie będą miały zgromadzone dowody. W procesie udostępniania nielegalnych i szkodliwych treści małoletnim występują na ogół: twórca treści (np. pornografii) oraz osoba, która udostępniłaby je dziecku. Często osobami tymi są rówieśnicy – uczniowie tej samej szkoły czy klasy, dzieci sąsiadów. Konieczne jest poinformowanie wszystkich rodziców lub opiekunów dzieci uczestniczących w zdarzeniu o sytuacji i roli ich dzieci.

Tabela 1 (cd.)

Działania wobec sprawców zdarzenia ze szkoły/spoza szkoły	W przypadku udostępniania („szerowania", dzielenia się) treści opisanych wcześniej jako szkodliwe/niedozwolone/nielegalne i niebezpieczne dla zdrowia przez ucznia należy przeprowadzić z nim rozmowę na temat jego postępowania i w jej trakcie uzmysłowić mu szkodliwość prowadzonych przez niego działań. Działania szkoły powinny koncentrować się jednak na aktywnościach wychowawczych. W przypadku upowszechniania przez sprawców treści nielegalnych (np. pornografii dziecięcej) należy złożyć zawiadomienie o zdarzeniu na policję.
Aktywności wobec ofiar zdarzenia	Dzieci – ofiary i świadków zdarzenia – należy od pierwszego etapu interwencji otoczyć opieką psychologiczno-pedagogiczną. Rozmowa z dzieckiem powinna się odbywać w warunkach jego komfortu psychicznego, z poszanowaniem poufności i podmiotowości ucznia ze względu na fakt, iż kontakt z treściami nielegalnymi może mieć bardzo szkodliwy wpływ na jego psychikę. W jej trakcie należy ustalić okoliczności uzyskania przez ofiarę dostępu do ww. treści. Należy koniecznie powiadomić ich rodziców lub opiekunów prawnych o zdarzeniu i uzgodnić z nimi podejmowane działania i formy wsparcia dziecka. Działania szkoły w takich przypadkach powinna cechować poufność i empatia w kontaktach z wszystkimi uczestnikami zdarzenia oraz udzielającymi wsparcia. W przypadku kontaktu dziecka z treściami szkodliwymi należy dokładnie zbadać sposób, w jaki nastąpił kontakt dziecka z nimi. Poszukiwanie przez dziecko tego typu treści w sieci lub podsuwanie ich dziecku przez innych może być oznaką niepokojących incydentów ze świata rzeczywistego. Na przykład kontakty z osobami handlującymi narkotykami czy proces rekrutacji do sekty lub innej niebezpiecznej grupy.
Aktywności wobec świadków	W przypadku, gdy informacja na temat zdarzenia dotrze do środowiska rówieśniczego ofiary – w klasie czy szkole, wskazane jest podjęcie działań edukacyjnych i wychowawczych.
Współpraca z policją i sądami rodzinnymi	W przypadku naruszenia prawa, np. rozpowszechniania materiałów pornograficznych z udziałem nieletniego lub prób uwiedzenia małoletniego w wieku do 15 lat przez osobę dorosłą, należy – w porozumieniu z rodzicami dziecka – niezwłocznie powiadomić policję
Współpraca ze służbami i placówkami specjalistycznymi	Kontakt z treściami szkodliwymi lub niebezpiecznymi może wywołać potrzebę skorzystania przez ofiarę ze specjalistycznej opieki psychologicznej. Decyzja o takim kontakcie i skierowaniu na terapię musi zostać podjęta w porozumieniu z rodzicami/opiekunami prawnymi dziecka.

Procedura 2	**Cyberprzemoc**
Podstawy prawne uruchomienia procedury	Kodeks karny, regulamin szkoły

Tabela 1 (cd.)

Rodzaj zagrożenia objętego procedurą	Cyberprzemoc – przemoc z użyciem technologii informacyjnych i komunikacyjnych, głównie Internetu oraz telefonów komórkowych. Podstawowe formy zjawiska to nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów z użyciem sieci oraz podszywanie się w sieci pod kogoś wbrew jego woli. Do działań określanych mianem cyberprzemocy wykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, serwisy społecznościowe, grupy dyskusyjne, serwisy SMS i MMS.
Telefony alarmowe krajowe i lokalne	Telefon Zaufania dla Dzieci i Młodzieży – **116 111,** Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – **800 100 100,** dyzurnet@dyzurnet.pl.
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Przypadek cyberprzemocy może zostać ujawniony przez ofiarę, świadka (np. innego ucznia, nauczyciela, rodzica) lub osobę bliską ofierze (np. rodzice, rodzeństwo, przyjaciele). W każdym przypadku należy ze spokojem wysłuchać osoby zgłaszającej i okazać jej wsparcie. Podziękować za zaufanie i zgłoszenie tej sprawy. • Jeśli zgłaszającym jest ofiara cyberprzemocy, podejmując działania, przede wszystkim należy okazać wsparcie, z zachowaniem jej podmiotowości i poszanowaniem jej uczuć. Potwierdzić, że ujawnienie przemocy jest dobrą decyzją. Taką rozmowę należy przeprowadzić w miejscu bezpiecznym, zapewniającym ofierze intymność. Nie należy podejmować kroków, które mogłyby prowadzić do powtórnej wiktymizacji czy wzbudzić podejrzenia sprawcy (np. wywoływać ucznia z lekcji do dyrekcji). • Jeśli osobą zgłaszającą nie jest ofiara, na początku prosimy o opis sytuacji, także z zachowaniem podmiotowości i poszanowaniem uczuć osoby zgłaszającej (np. strach przed byciem „kapusiem", obawa o własne bezpieczeństwo). W każdej sytuacji w trakcie ustalania okoliczności trzeba ustalić charakter zdarzenia (rozmiar i rangę szkody, jednorazowość/powtarzalność). Realizując procedurę, należy unikać działań, które mogłyby wtórnie stygmatyzować ofiarę lub sprawcę, np.: wywoływanie uczniów z lekcji, konfrontowanie ofiary i sprawcy, niewspółmierna kara, wytykanie palcami itd. Trzeba dokonać oceny, czy zdarzenie wyczerpuje znamiona cyberprzemocy, czy jest np. niezbyt udanym żartem (wtedy trzeba podjąć działania profilaktyczne mające na celu niedopuszczenie do eskalacji tego typu zachowań w stronę cyberprzemocy).
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zabezpieczyć wszystkie dowody związane z aktem cyberprzemocy (np. zrobić kopię materiałów, zanotować datę i czas otrzymania materiałów, dane nadawcy, adresy stron WWW, historię połączeń itd.). W trakcie zbierania materiałów należy zadbać o bezpieczeństwo osób zaangażowanych w problem.

Tabela 1 (cd.)

Identyfikacja sprawcy(-ów)	Identyfikacja sprawcy(ów) często jest możliwa dzięki zebranym materiałom – wynikom rozmów z osobą zgłaszającą, z ofiarą, analizie zebranych materiałów. Ofiara często domyśla się, kto stosuje wobec niej cyberprzemoc. Jeśli ustalenie sprawcy nie jest możliwe, a w ocenie kadry pedagogicznej jest to konieczne, należy skontaktować się z policją. Bezwzględnie należy zgłosić rozpowszechnianie nagich zdjęć osób poniżej 18. roku życia (art. 202 par. 3 kk).
Aktywności wobec sprawców zdarzenia ze szkoły/spoza szkoły	Gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog szkolny powinien przeprowadzić z nim rozmowę o jego zachowaniu. Rozmowa taka ma służyć ustaleniu okoliczności zdarzenia, jego wspólnej analizie (w tym np. przyjrzeniu się przyczynom), a także próbie rozwiązania sytuacji konfliktowej (w tym sposobów zadośćuczynienia ofiarom cyberprzemocy). Cyberprzemoc powinna podlegać sankcjom określonym w wewnętrznych przepisach szkoły (kontrakt, regulamin). Szkoła może tu stosować konsekwencje przewidziane dla sytuacji „tradycyjnej" przemocy. Warto jednak rozszerzyć repertuar dostępnych środków, np. o czasowy zakaz korzystania ze szkolnej pracowni komputerowej w czasie wolnym i przynoszenia do szkoły akcesoriów elektronicznych (PSP, mp3) itp.
Aktywności wobec ofiar zdarzenia	W pierwszej kolejności należy udzielić wsparcia ofierze. Musi się ona czuć bezpieczna i otoczona opieką przez dorosłych. Na poczucie bezpieczeństwa dziecka wpływa fakt, że wie ono, iż szkoła podejmuje kroki w celu rozwiązania problemu. Podczas rozmowy z uczniem – ofiarą cyberprzemocy – należy zapewnić go, że nie jest winny zaistniałej sytuacji oraz że nikt nie ma prawa zachowywać się w ten sposób wobec niego, a także podkreślić, że dobrze zrobił, ujawniając sytuację. Należy okazać zrozumienie dla jego uczuć, w tym trudności z ujawnieniem okoliczności wydarzenia, strachu, wstydu. Trzeba podkreślić, że szkoła nie toleruje przemocy i że zostaną podjęte odpowiednie procedury interwencyjne. Należy poinformować ucznia o krokach, jakie może podjąć szkoła, i sposobach, w jakich może zapewnić mu bezpieczeństwo. Należy pomóc ofierze (rodzicom ofiary) w zabezpieczeniu dowodów (to może być dla niej zadanie trudne zarówno ze względów technicznych, jak i emocjonalnych), zerwaniu kontaktu ze sprawcą, zadbaniu o podstawowe zasady bezpieczeństwa online (np. nieudostępnianie swoich danych kontaktowych, kształtowanie swojego wizerunku itd.). Pomoc ofierze nie może kończyć się w momencie zakończenia procedury. Warto monitorować sytuację, „czuwać" nad jej bezpieczeństwem, np. zwracać uwagę, czy nie są podejmowane wobec niej dalsze działania przemocowe, obserwować, jak sobie radzi w grupie po ujawnionym incydencie cyberprzemocy. W działania wobec ofiary należy także włączyć rodziców/opiekunów ofiary – trzeba na bieżąco ich informować o sytuacji, pamiętając przy tym o podmiotowym traktowaniu dziecka – mówiąc mu o tym i starając się uzyskać jego akceptację dla udziału rodziców. Jeśli dziecko

Tabela 1 (cd.)

Aktywności wobec ofiar zdarzenia	nie wyraża zgody, należy omówić z nim jego obawy, a jeśli to nie pomaga, powołać się na obowiązujące nas zasady i przekazać informację rodzicom. W trakcie rozmowy z dzieckiem i/lub jego rodzicami/opiekunami, jeśli jest to wskazane, można zaproponować pomoc specjalisty (np. psycholog szkolny, poradnia psychologiczno-pedagogiczna) oraz przekazać informację o możliwości zgłoszenia sprawy policji.
Aktywności wobec świadków	Należy zadbać o bezpieczeństwo świadków zdarzenia, zwłaszcza jeśli byli oni osobami ujawniającymi cyberprzemoc. W trakcie rozmowy ze świadkami należy okazać zrozumienie i empatię dla ich uczuć – obawy przed przypięciem łatki „donosiciela", strachu przed staniem się kolejną ofiarą sprawcy itp.
Współpraca z policją i sądami rodzinnymi	Samo wystąpienie zjawiska cyberprzemocy nie jest jednoznaczne z koniecznością zaangażowania policji i sądu rodzinnego – procedura powinna umożliwiać rozwiązanie sytuacji problemowej na poziomie pracy wychowawczej szkoły. Szkoła powinna powiadomić odpowiednie służby (np. sąd rodzinny), gdy wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje regulaminowe wobec ucznia) i interwencje pedagogiczne, a ich zastosowanie nie przynosi pożądanych rezultatów (np. nie ma zmian postawy ucznia). Kontaktu z policją wymagają wszelkie sytuacje, w których zostało naruszone prawo (np. groźby karalne, świadome publikowanie nielegalnych treści, rozpowszechnianie nagich zdjęć z udziałem małoletnich). Za zgłoszenie powinien odpowiadać dyrektor szkoły.
Współpraca z dostawcami Internetu i operatorami telekomunikacyjnymi	Kontakt z dostawcą usługi może być wskazany w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów. Do podjęcia takiego działania stymuluje administratora serwisu art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

Procedura 3	**Zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu**
Podstawy prawne uruchomienia procedury	Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe
Rodzaj zagrożenia objętego procedurą (opis)	Infoholizm (siecioholizm) – nadmierne, obejmujące niekiedy niemal całą dobę korzystanie z zasobów Internetu i gier komputerowych (najczęściej sieciowych) i portali społecznościowych przez dzieci. Jego negatywne efekty polegają na pogarszaniu się stanu zdrowia fizycznego (np. choroby oczu, padaczka ekranowa, choroby kręgosłupa) i psychicznego (irytacja, rozdrażnienie, spadek sprawności psychofizycznej, a nawet depresja), zaniedbywaniu codziennych czynności oraz osłabianiu relacji rodzinnych i społecznych.

Tabela 1 (cd.)

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Infoholizm stwierdza najczęściej rodzic lub opiekun prawny dziecka. W przypadku konieczności podejmowania dalszych działań pomocowych można skierować ucznia, za zgodą i we współpracy z rodzicami, do placówki specjalistycznej, np. terapeutycznej. Kluczowe są tutaj pozostałe objawy wskazane wyżej. Nauczyciele w szkole także powinni zainteresować się przypadkami dzieci nieangażujących się w życie klasy, a poświęcającymi wolne chwile na kontakt online lub przychodzącymi do szkoły po nieprzespanej nocy. Rzadziej zgłoszeń można się spodziewać od rówieśników dziecka nadmiernie korzystającego z sieci.
Opis okoliczności, analiza, zabezpieczenie dowodów	Reakcja szkoły powinna polegać w pierwszych krokach na ustaleniu skutków zdrowotnych i psychicznych, jakie nadmierne korzystanie z zasobów Internetu wywołało u dziecka (np. gorsze oceny w nauce, niedosypianie, niedojadanie, rezygnacja z dawnych zainteresowań, załamanie się relacji z rodziną czy rówieśnikami). Celem tych ustaleń jest wybór odpowiedniej ścieżki rozwiązywania problemu – z udziałem specjalistów (lekarzy, terapeutów) lub bez – wyłącznie w szkole. W początkowej fazie popadania w uzależnienie do Internetu należy koncentrować się na wsparciu udzielonym w rodzinie i w szkole (psycholog/pedagog szkolny, wychowawca).
Aktywności wobec ofiar zdarzenia	Osoba, której problem dotyczy, powinna zostać otoczona zindywidualizowaną opieką przez pedagoga/psychologa szkolnego. Pierwszym jej etapem będzie rozmowa (rozmowy) ze specjalistą, która pozwoli zdiagnozować poziom zagrożenia, określić przyczyny popadnięcia w nałóg (np. sytuacja domowa, brak sukcesów edukacyjnych w szkole, izolacja w środowisku rówieśniczym) i ukazać specyfikę przypadku. Każde dziecko, u którego podejrzewa się nałóg korzystania z Internetu, powinno zostać profesjonalnie zdiagnozowane przez psychologa szkolnego. Czasem warto w tym zakresie skorzystać z pomocy poradni psychologiczno-pedagogicznej. Dziecku w trakcie wsparcia należy zapewnić komfort psychiczny – o jego sytuacji i specyfice uwarunkowań osobistych muszą zostać powiadomieni wszyscy uczący go i oceniający nauczyciele. O ile nie wiedzą o problemie swojego dziecka, niezbędne jest powiadomienie rodziców lub opiekunów prawnych dziecka i omówienie z nimi wspólnych rozwiązań. Tylko synergiczne współdziałanie rodziców i szkoły może zagwarantować powodzenie podejmowanych działań wspierających dziecko.
Aktywności wobec świadków	Jeśli świadkami problemu są rówieśnicy dziecka, należy im w rozmowie zwrócić uwagę na negatywne aspekty nadmiernego korzystania z zasobów Internetu oraz zaapelować o codzienne wsparcie dla dziecka dotkniętego problemem, a także o informowanie wychowawcy w przypadku wystąpienia kolejnych przypadków u innych dzieci.
Współpraca ze służbami i placówkami specjalistycznymi	W przypadku zdiagnozowania przez psychologa zaawansowanego uzależnienia od korzystania z zasobów Internetu dziecko powinno zostać skierowane przez szkołę, w bliskiej współpracy z rodzicami, do placówki specjalistycznej oferującej program terapeutyczny z zakresu przeciwdziałania uzależnieniom. W części przypadków może okazać się konieczna diagnoza i terapia lekarska.

Tabela 1 (cd.)

Procedura 4	**Nawiązywanie niebezpiecznych kontaktów w Internecie – uwodzenie, zagrożenie pedofilią**
Podstawy prawne uruchomienia procedury	Kodeks karny, art. 200, 200a § 1 i 2, art. 286 § 1
Rodzaj zagrożenia objętego procedurą (opis)	Zagrożenie obejmuje kontakty osób dorosłych z małoletnimi w celu zainicjowania znajomości prowadzących do wyłudzenia poufnych informacji, nawiązania kontaktów seksualnych, skłonienia dziecka do zachowań niebezpiecznych dla jego zdrowia i życia lub wyłudzenia własności (np. danych, pieniędzy, cennych przedmiotów rodzinnych).
Telefony alarmowe krajowe	**Tel. 116 111** **dyzurnet@dyzurnet.pl**
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Osobami najczęściej zgłaszającymi omawiany problem są rodzice/ /opiekunowie prawni dziecka lub osoby zajmujące się „poszukiwaniem pedofili". W pierwszym przypadku informacja trafia najpierw do szkół, w drugim – na policję. Zdarza się, że informacja jest uzyskiwana ze środowiska rówieśników ofiary. Kluczowe znaczenie w działaniach szkoły ma czas reakcji – szybkość przeciwdziałania zagrożeniu ze względu na niezwykle szkodliwe konsekwencje realizacji kontaktu online, przeradzającego się w zachowania w świecie rzeczywistym: uwiedzenie i wykorzystanie seksualne, kidnaping, a także wyłudzenie pieniędzy czy przedmiotów dużej wartości. W przypadkach niebezpiecznych kontaktów inicjowanych w Internecie może dochodzić do zagrożenia życia i zdrowia dziecka, szantażu i przymusu realizacji czynności seksualnych.
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zidentyfikować i zabezpieczyć w szkole, w formie elektronicznej dowody działania dorosłego sprawcy uwiedzenia (zapisy rozmów w komunikatorach, na portalach społecznościowych; zrzuty ekranowe, zdjęcia, wiadomości e-mail). Jednocześnie – bezzwłocznie – należy dokonać zawiadomienia na policji o wystąpieniu zdarzenia.
Identyfikacja sprawcy(-ów)	Ze względu na bezpieczeństwo nie należy podejmować samodzielnych działań w celu dotarcia do sprawcy, lecz udzielać wszelkiego możliwego wsparcia organom ścigania, m.in. zabezpieczyć i przekazać zebrane dowody. Identyfikacja sprawcy wykracza poza kompetencje i możliwości szkoły w większości przypadków uwodzenia przez Internet.
Aktywności wobec sprawców ze szkoły/spoza szkoły	Nie należy podejmować aktywności zmierzających bezpośrednio do kontaktu ze sprawcą. Zadaniem szkoły jest zebranie dowodów i opieka nad ofiarą i ewentualnymi świadkami.

Tabela 1 (cd.)

Aktywności wobec ofiar zdarzenia	W każdym przypadku próby nawiązania niebezpiecznego kontaktu – np. w celu werbunku do sekty lub grupy promującej niebezpieczne zachowania, a także werbunku do grupy terrorystycznej – należy przed wszystkim zapewnić ofierze opiekę psychologiczną i poczucie bezpieczeństwa. Podobne wsparcie winno być udzielone w przypadku zaobserwowania antyzdrowotnych i zagrażających życiu zachowań uczniów (samookaleczenia, zażywanie substancji psychoaktywnych), zachowania te mogą być bowiem inicjowane i wzmacniane poprzez kontakty w Internecie. O możliwym związku takich zachowań dzieci z inspiracją w Internecie należy powiadomić rodziców. Pierwszą czynnością w ramach reakcji na zagrożenie jest otoczenie ofiary pomocą psychologiczno-pedagogiczną we współpracy szkoły z rodzicami/opiekunami prawnymi. W trakcie rozmowy z dzieckiem prowadzonej w warunkach komfortu psychicznego przez wychowawcę/pedagoga/psychologa/osobę ze szkoły, do której dziecko ma szczególne zaufanie, należy uzyskać wszelkie możliwe informacje o sprawcy i przekazać je policji. Należy upewnić się, że kontakt ofiary ze sprawcą został przerwany, a dziecko odzyskało poczucie bezpieczeństwa. Towarzyszyć temu powinna analiza sytuacji domowej (rodzinnej) dziecka, w której może tkwić źródło poszukiwania kontaktów w Internecie. Dziecku należy udzielić profesjonalnej opieki terapeutycznej i/lub lekarskiej. Wszelkie działania szkoły wobec dziecka winny być uzgadniane z rodzicami/opiekunami prawnymi i inicjowane za ich zgodą.
Aktywności wobec świadków	Jeżeli zgłaszającym zagrożenie był rówieśnik ofiary, należy również objąć go opieką psychologiczną, pozytywnie wzmacniając jego reakcję na zdarzenie.
Współpraca z policją i sądami rodzinnymi	W przypadkach naruszenia prawa – szczególnie w przypadku uwiedzenia dziecka do lat 15 – obowiązkiem szkoły jest powiadomienie policji lub sądu rodzinnego.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	W przypadkach uwiedzenia nieletnich przez osoby dorosłe rekomenduje się – w porozumieniu z rodzicami/opiekunami prawnymi – skierowanie ofiary na terapię do placówki specjalistycznej opieki psychologicznej.

Procedura 5	**Seksting, prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich**
Podstawy prawne uruchomienia procedury	Kodeks karny (art. 191a i 202)
Rodzaj zagrożenia objętego procedurą	Seksting to przesyłanie drogą elektroniczną w formie wiadomości MMS lub publikowanie w portalach (społecznościowych) prywatnych treści, głównie zdjęć, o kontekście seksualnym, erotycznym i intymnym.

Tabela 1 (cd.)

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Zgłoszeń przypadków sekstingu dokonują głównie rodzice lub opiekunowie prawni dziecka – ofiary. Czasami informacja dociera do szkoły bezpośrednio od niej samej lub z grona bliskich znajomych dziecka. W rzadkich wypadkach nauczyciele i inni pracownicy szkoły sami identyfikują takie zdarzenia w sieci. Delikatny charakter sprawy, a także potencjalna penalizacja sprawcy, wymagają zachowania daleko posuniętej dyskrecji i profesjonalnej reakcji. Czasami zgłoszenia dokonują ofiary lub osoby je znające.
Opis okoliczności, analiza, zabezpieczenie dowodów	Wyróżniamy trzy podstawowe rodzaje sekstingu, które skutkują koniecznością realizacji zmodyfikowanych procedur reagowania. **Rodzaj 1.** Wymiana materiałów o charakterze seksualnym następuje tylko w ramach związku między dwojgiem rówieśników. Materiały nie uległy rozprzestrzenieniu dalej. **Rodzaj 2.** Materiały o charakterze seksualnym zostały rozesłane większej liczbie osób, jednak nie dochodzi do cyberprzemocy na tym tle. Młodzież traktuje materiał jako formę wyrażenia siebie. **Rodzaj 3.** Materiały zostały rozesłane większej liczbie osób w celu upokorzenia osoby na nich zaprezentowanej – lub zostają rozpowszechnione omyłkowo, jednak są zastosowane jako narzędzie cyberprzemocy.
Identyfikacja sprawcy(-ów)	Identyfikacja sprawcy będzie możliwa przede wszystkim dzięki zabezpieczeniu dowodów – przesyłanych zdjęć czy zrzutów ekranów portali, w których opublikowano zdjęcie(-a). Jako że sexting jest karalny, skrupulatność i wiarygodność dokumentacji ma duże znaczenie. Należy przy tym przestrzegać zasad dyskrecji, szczególnie w środowisku rówieśniczym ofiary.
Aktywności wobec sprawców zdarzenia ze szkoły/spoza szkoły	Zidentyfikowani małoletni sprawcy sekstingu winni zostać wezwani do dyrekcji szkoły, gdzie zostaną im przedstawione dowody ich aktywności. Niezależnie od zakresu negatywnych zachowań i działań wszyscy sprawcy powinni otrzymać wsparcie pedagogiczne i psychologiczne. Konieczne są także rozmowy ze sprawcami w obecności ich rodziców zaproszonych do szkoły. **Rodzaj 1.** Dalsze działania poza zapewnieniem wsparcia i opieki psychologiczno-pedagogicznej nie są konieczne, jednak istotne jest pouczenie sprawców zdarzenia, że dalsze rozpowszechnianie materiałów może być nielegalne i będzie miało ostrzejsze konsekwencje, w tym prawne.
Aktywności wobec sprawców zdarzenia ze szkoły/spoza szkoły	**Rodzaj 2.** Niektóre z tego typu materiałów mogą zostać uznane za pornograficzne, w takim wypadku na dyrektorze placówki ciąży obowiązek zgłoszenia incydentu na policję. Rozpowszechnianie materiałów pornograficznych z udziałem nieletnich jest przestępstwem ściganym z urzędu (§ 2020 Kodeksu karnego), dlatego też dyrektor placówki jest zobowiązany do zgłoszenia incydentu na policję i/lub do sądu rodzinnego. Wszelkie działania wobec sprawców incydentu powinny być podejmowane w porozumieniu z ich rodzicami lub opiekunami prawnymi.

Tabela 1 (cd.)

Aktywności wobec sprawców zdarzenia ze szkoły/spoza szkoły	**Rodzaj 3.** Niektóre z tego typu materiałów mogą zostać uznane za pornograficzne – konieczne jest zgłoszenie takiego przypadku na policję. W sytuacji zaistnienia znamion cyberprzemocy należy dodatkowo zastosować procedurę: Cyberprzemoc. Decyzja o ewentualnym poinformowaniu opiekunów powinna być podejmowana przez pedagoga/psychologa, biorącego pod uwagę dobro małoletnich, w zależności od charakteru sytuacji.
Aktywności wobec ofiar zdarzenia	Pierwszą reakcją szkoły i rodziców, obok dokumentacji dowodów, winno być otoczenie wszechstronną, dyskretną opieką psychologiczno-pedagogiczną ofiary oraz zaproponowanie odpowiednich działań wychowawczych, w przypadku upublicznienia przypadku sekstingu w środowisku rówieśniczym. Rozmowa na temat identyfikacji potencjalnego sprawcy powinna być realizowana w warunkach komfortu psychicznego dla dziecka – ofiary sekstingu, z szacunkiem dla jego indywidualności i przeżytego stresu.
Aktywności wobec świadków	Jeśli przypadek sekstingu zostanie upowszechniony w środowisku rówieśniczym – np. poprzez przesłanie MMS-ów do uczniów tej samej szkoły lub klasy lub publikacje w portalu społecznościowym, należy podjąć działania wychowawcze uświadamiające negatywne aspekty moralne sekstingu oraz narażanie się na dotkliwe kary.
Współpraca z policją i sądami rodzinnymi	W przypadku publikacji lub upowszechniania zdjęć o charakterze pornografii dziecięcej (co jest wykroczeniem ściganym z urzędu) kierownictwo szkoły jest zobowiązane do powiadomienia o tym zdarzeniu policji lub sądu rodzinnego.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	Kontakt ofiar z placówkami specjalistycznymi może okazać się konieczny w indywidualnych przypadkach. O skierowaniu do nich decyzję powinien podjąć psycholog/pedagog szkolny wspólnie z rodzicami/opiekunami prawnymi ofiary.

Procedura 6	**Bezkrytyczna wiara w treści zamieszczone w Internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, szkodliwość reklam**
Podstawy prawne uruchomienia procedury	Ustawa z 11 stycznia 2017r. – prawo oświatowe
Rodzaj zagrożenia objętego procedurą (opis)	Brak umiejętności odróżniania informacji prawdziwych od nieprawdziwych publikowanych w Internecie, bezkrytyczne uznawanie za prawdę tez publikowanych w forach internetowych, kierowanie się informacjami zawartymi w reklamach. Taka postawa dzieci może prowadzić do zagrożeń życia i zdrowia (np. stosowania wyniszczającej diety, samookaleczeń), skutkować rozczarowaniami i porażkami życiowymi (w efekcie korzystania z fałszywych informacji), utrudniać lub uniemożliwiać osiąganie dobrych wyników w edukacji (korzystanie z upraszczających i zawężających temat „ściąg" i „bryków"), a także utrwalenia się u ucznia ambiwalentnych postaw moralnych.

Tabela 1 (cd.)

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Uczniowie nie umiejący odróżniać prawdy od fałszu publikowanych w Internecie winni być identyfikowani przez nauczycieli i wychowawców w trakcie lekcji wszystkich przedmiotów. Często taka postawa ujawnia się podczas przygotowania prac domowych i jest stosunkowo łatwa do zidentyfikowania przez oceniającego je nauczyciela.
Opis okoliczności, analiza, zabezpieczenie dowodów	Posługiwanie się nieprawdziwymi informacjami zaczerpniętymi z Internetu w procesie dydaktycznym – podczas lekcji lub w zadaniach domowych – każdorazowo winno być zauważone przez nauczyciela, przeanalizowane i sprostowane. Przypadki spektakularne powinny być archiwizowane przez nauczycieli i wykorzystywane podczas zajęć z edukacji medialnej (informacyjnej).
Aktywności wobec sprawców zdarzenia ze szko-ły/spoza szkoły	Wystarczającą reakcją jest opublikowanie sprostowania nieprawdziwych informacji i – w miarę możliwości – rozpowszechnienie ich w Internecie, w portalach o zbliżonej tematyce.
Aktywności wobec ofiar zdarzenia i świadków	Szkoła powinna prowadzić działania profilaktyczne – edukację medialną (informacyjną) oraz filozoficzną (elementy epistemologii z uwzględnieniem realizmu poznawczego), zarówno w formie zajęć pozalekcyjnych, jak i w trakcie lekcji przedmiotów nieinformatycznych (np. języka polskiego, WDŻ) przez wszystkie lata nauki ucznia w szkole. Zajęcia w szkole mogą mieć charakter kilkuminutowych elementów edukacji medialnej lub filozoficznej wplecionej w lekcje o innej tematyce i/lub lekcji ukierunkowanych na zdobywanie przez dzieci i młodzież kompetencji medialnych

Procedura 7	**Łamanie prawa autorskiego**
Podstawy prawne uruchomienia procedury	Kodeks karny
Rodzaj zagrożenia objętego procedurą (opis)	Ryzyko poniesienia odpowiedzialności cywilnej lub karnej z tytułu naruszenia prawa autorskiego albo negatywnych skutków pochopnego spełnienia nieuzasadnionych roszczeń (tzw. *copyright trolling*).
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	W zależności od okoliczności oraz zaawansowania problemu, w którym doszło do ujawnienia sprawy, zdarzenie może zostać zgłoszone w sposób nieformalny (ustnie, telefonicznie, pocztą elektroniczną, na zamkniętym lub publicznym forum internetowym, na piśmie w postaci wezwania podpisanego przez domniemanego uprawnionego lub jego pełnomocnika) lub formalny (w postaci doręczenia odpisu pozwu lub innego pisma urzędowego, np. wezwania z policji lub prokuratury). Przyjęcie zgłoszenia dokonanego w sposób nieformalny powinno zaowocować powstaniem bardziej formalnego śladu, w postaci np. notatki służbowej, zakomunikowania przełożonemu itd., w zależności od wagi sprawy.

Tabela 1 (cd.)

Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Na wstępnym etapie należy przede wszystkim unikać wdawania się w argumentację, pochopnego przyznawania roszczeń lub spełniania żądań, piętnowania domniemanych sprawców itd. bez ustalenia wszystkich okoliczności sprawy, w razie potrzeby w konsultacji z prawnikiem. Prawo autorskie jest regulacją skomplikowaną, a sądy decydują w sprawach o naruszenie praw autorskich często w bardzo odmienny sposób, dlatego w większości przypadków uzyskanie fachowej pomocy prawnej jest wysoce wskazane. Najczęstszym przypadkiem, w którym szkoła może zetknąć się z problemem naruszenia praw autorskich, jest użycie materiałów prawnie chronionych na stronach internetowych szkoły, poza zakresem dozwolonego użytku, przez jej pracowników bądź uczniów. W przypadku naruszeń dokonanych przez uczniówów szkoła nie może występować w roli sędziego – dochodzenie roszczeń należy pozostawić osobom uprawnionym. Szkoła powinna na każdym etapie skupić się na swojej roli edukacyjno-wychowawczej poprzez organizację lekcji na temat praw autorskich, zwracając przy tym uwagę, że powinny one rzeczowo i konkretnie informować, jakie czyny są dozwolone, a jakie zabronione prawem.
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zebrać informacje przede wszystkim o: • osobie dokonującej zgłoszenia, czy jest do tego uprawniona (czy faktycznie przysługują jej prawa autorskie do danego utworu, czy posiada ważne pełnomocnictwo itd.); • wykorzystanym utworze (czy faktycznie jest chroniony przez prawo autorskie, w jakim zakresie został wykorzystany i czy zakres ten mieści się w zakresie posiadanych licencji lub dozwolonego użytku). Należy zweryfikować wszystkie informacje podawane przez zgłaszającego lub inne osoby. Jeżeli np. powołuje się on na toczące się w sprawie postępowanie karne, należy podjąć kontakt z odpowiednimi służbami w celu ustalenia, czy takie postępowanie faktycznie się toczy, czego dokładnie dotyczy i jaka jest w nim rola poszczególnych osób. Taki kontakt najlepiej przeprowadzać za pośrednictwem adwokata lub radcy prawnego. Należy sprawdzić, czy okoliczności podane w zgłoszeniu faktycznie nastąpiły i czy powoływane tam dowody nie zostały zmanipulowane.
Identyfikacja sprawcy(-ów)	Dochodzenie naruszeń praw autorskich realizowane jest, co do zasady, z inicjatywy samego uprawnionego przed sądami, a w przypadku naruszeń stanowiących przestępstwo dodatkowo zaangażowane mogą być policja i prokuratura. Szkoła nie powinna wyręczać tych organów w ich rolach ani też wkraczać w ich kompetencje. Szkoła powinna skupić się na swojej roli wychowawczej i edukacyjnej, wykorzystując otrzymanie zgłoszenia rzekomego naruszenia do przekazania zaangażowanym osobom (a być może i wszystkim uczniom, nauczycielom i opiekunom) wiedzy na temat tego, jak faktycznie prawo reguluje tę konkretną sytuację.

Tabela 1 (cd.)

Aktywności wobec sprawców zdarzenia ze szkoły/spoza szkoły	Zasadniczo o dochodzeniu roszczeń wobec sprawcy decyduje sam uprawniony (tzn. autor lub inna osoba, której przysługują prawa autorskie). Szkoła powinna natomiast podjąć działania o charakterze edukacyjno-wychowawczym, polegające na obszernym wyjaśnieniu, na czym polegało naruszenie, oraz przekazaniu wiedzy, jak do naruszeń nie dopuścić w przyszłości.
Aktywności wobec ofiar zdarzenia	Jeżeli osobą, której prawa autorskie naruszono, jest uczeń, należy rozważyć możliwość wystąpienia w roli mediatora, aby stosownie do okoliczności ułatwić stronom ugodowe lub inne kompromisowe zakończenie powstałego sporu. Na przykład w przypadku, gdy ofiarą jest osoba ze szkoły, autorytet szkoły może pomóc w skłonieniu sprawcy do zaprzestania naruszeń. Z kolei w przypadku, gdy ofiarą jest osoba spoza szkoły, szkoła może pomóc sprawcy w doprowadzeniu do zaniechania naruszeń i naprawienia ich skutków bez niepotrzebnej eskalacji sporu.
Aktywności wobec świadków	Stosownie do okoliczności należy samodzielnie zebrać ich zeznania lub zadbać, aby zostały one zebrane przez uprawnione organy.
Współpraca z policją i sądami rodzinnymi	Ponieważ, co do zasady, dochodzenie roszczeń z tytułu naruszeń zależy od decyzji uprawnionego, to uprawniony musi samodzielnie zdecydować, czy zawiadamiać policję lub składać powództwo. Stosownie do wskazanej wyżej roli mediatora szkoła powinna zaangażować się natomiast przede wszystkim w ułatwianie zakończenia sporu bez takiej eskalacji.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	Warto rozważyć zorganizowanie szkoleń lub warsztatów z zakresu prawa autorskiego w internecie dla wszystkich zainteresowanych osób w szkole. Materiały edukacyjne (scenariusze zajęć, podręczniki) dostępne są m.in. na stronach http://prawokultury.pl/, http://edukacjamedialna.edu.pl oraz http://www.legalnakultura.pl/pl. Fundacja Nowoczesna Polska prowadzi nieodpłatną linię pomocy w sprawach prawno-autorskich – pod numerem tel. +48 739 231 233 oraz przez Internet: https://prawokultury.pl/pierwsza-pomoc/pytanie/.
Współpraca z dostawcami Internetu i operatorami telekomunikacyjnymi	Zależnie od okoliczności, może być wskazana asysta sprawcy bądź ofiary przy kontakcie z tego typu podmiotami, np. w celu zablokowania dostępu do utworu umieszczonego w Internecie z naruszeniem prawa. Ponadto, stosownie do przepisów prawa, tego typu usługodawcy mogą zostać zobowiązani do przekazania szczegółów dotyczących naruszenia dokonanego z użyciem ich usług (do czego jednak może być potrzebne postanowienie sądowe).

Źródło: *Bezpieczna Szkoła. Procedury reagowania w przypadku wystąpienia wewnętrznych i zewnętrznych zagrożeń fizycznych w szkole*, https://www.cyfrowa-szkola.info/wp-content/uploads/2017/10/Procedury-reagowania-w_2.pdf, s. 38–54.

Informacje o autorach

Dorota Siemieniecka
Autorka jest kierownikiem Katedry Dydaktyki i Mediów, doktorem habilitowanym i pracuje w Instytucie Nauk Pedagogicznych UMK na stanowisku profesora UMK. Jest członkinią Polskiego Towarzystwa Pedagogicznego, przez wiele lat była członkinią zarządu Polskiego Towarzystwa Kognitywistycznego. Redaktor naczelna międzynarodowego czasopisma naukowego „Cognitive Science – New Media – Education" (http://apcz.umk.pl/czasopisma/index.php/CSNME/index).

Jej zainteresowania naukowe, działalność badawcza i dydaktyczna koncentrują się na zagadnieniach dydaktyki, twórczości w pedagogice, twórczym nauczaniu, na zastosowaniu nowoczesnych mediów w procesie edukacji, a także na kognitywistycznych aspektach mediów w edukacji. Od wielu lat współpracuje z uczelniami w Norwegii, USA, we Włoszech, w Rumunii, Federacji Rosyjskiej, Bośni i Hercegowinie, na Litwie i Łotwie. Wielokrotnie przebywała na stypendiach m.in. w USA i Niemczech. W 2018 r. weszła w skład Zespołu Pedagogiki Medialnej przy Komitecie Badań Pedagogicznych PAN. Jest również przewodniczącą komitetu naukowego i organizacyjnego cyklu międzynarodowych konferencji poświęconych problematyce kształcenia z wykorzystaniem mediów.

Małgorzata Skibińska
Autorka jest adiunktem w Katedrze Dydaktyki i Mediów Wydziału Filozofii i Nauk Społecznych Uniwersytetu Mikołaja Kopernika w Toruniu. Doktor nauk humanistycznych z zakresu pedagogiki. Jej zainteresowania naukowe i badawcze koncentrują się wokół problematyki umiejętności informacyjnych uczniów, metodyki nauczania technologii informacyjnej, wykorzystania oprogramowania *open source* w kształce-

niu szkolnym i akademickim. Jest członkiem Polskiego Towarzystwa Pedagogicznego i Polskiego Towarzystwa Kognitywistycznego. Autorka monografii pt. *Umiejętności informacyjne gimnazjalistów* (2011), współautorka książki pt. *Aktywność uczących się w przestrzeni Internetu* (2014); autorka i współautorka wielu publikacji naukowych poświęconych zastosowaniu mediów w edukacji.

Kamila Majewska
Adiunkt w Katedrze Dydaktyki i Mediów Wydziału Filozofii i Nauk Społecznych Uniwersytetu Mikołaja Kopernika w Toruniu. Doktor nauk społecznych z zakresu pedagogiki. Doświadczony nauczyciel matematyki i informatyki. Certyfikowana specjalistka z zakresu e-nauczania. Wykładowca związany z obszarem zastosowania nowych mediów w pracy pedagogów specjalnych oraz nauczycieli różnych szczebli, w szczególności edukacji wczesnoszkolnej. Aktywnie współpracuje z firmami edukacyjnymi w zakresie opracowywania oraz testowania innowacyjnych rozwiązań dydaktycznych. Stypendystka Bawarskiej Kancelarii Państwowej. W 2019 r. otrzymała stypendium ministra nauki i szkolnictwa wyższego dla wybitnych młodych naukowców.

Jest współautorką pozycji *Aktywność uczących się w przestrzeni Internetu* (2014) oraz autorką książki *Tablica interaktywna w procesie nauczania wczesnoszkolnego* (2015), jak również licznych prac naukowych ukazujących się w wydaniach zbiorowych „Multimedialnej Biblioteki Pedagogicznej", „The New Educational Review", „E-mentor".

Książka stanowi kompendium wiedzy z zakresu przeciwdziałania zachowaniom przemocowym w przestrzeni wirtualnej. Pewne osoby lub grupy, sięgając po możliwości nowych technologii, wykorzystują naiwność, brak wiedzy swoich ofiar do uzyskania emocjonalnych lub finansowych korzyści. Zachowania te są ukierunkowane na sprawowanie kontroli nad inną osobą lub zdobycie cudzej własności. Szczególną grupą zagrożoną cyberprzemocą jest młode pokolenie użytkowników Internetu – dzieci i młodzież. Przeniesienie zachowań agresywnych z przestrzeni realnej do środowiska cyfrowego przynosi nie tylko wiele szkód wszystkim jego uczestnikom, tj. cyberofiarom, cyberświadkom i cybersprawcom, lecz także stawia wyzwania dla pokolenia dorosłych, tj. rodziców, wychowawców, nauczycieli i terapeutów w zakresie zapobiegania i rozpoznawania zjawiska cyberprzemocy oraz pomocy w niwelowaniu jej negatywnych skutków.

W oddanej czytelnikowi publikacji opisano wybrane zagrożenia związane z aktywnością w Internecie, tj. szeroko rozumianą cyberprzemoc oraz szczególne jej odmiany, takie jak: stalking, cyberstalking, hejt i hakerstwo. Książka ta jest przeznaczona dla wszystkich użytkowników Internetu, którzy są zainteresowani tematyką zagrożeń płynących z sieci i sposobami radzenia sobie z nimi. Autorki mają świadomość, że narzędzia cyfrowe wykorzystywane przez przestępców komputerowych zmieniają się i stają się coraz bardziej doskonałe, jednak zalecenia postępowania w sytuacji określonego agresywnego zjawiska oraz sprawców mają charakter uniwersalny. Książka zawiera przegląd aktualnej literatury poświęconej omawianej problematyce oraz propozycje zapobiegania wybranym aspektom przemocy internetowej.

www.wydawnictwo.umk.pl

ISBN 978-83-231-4384-0
9 788323 143840