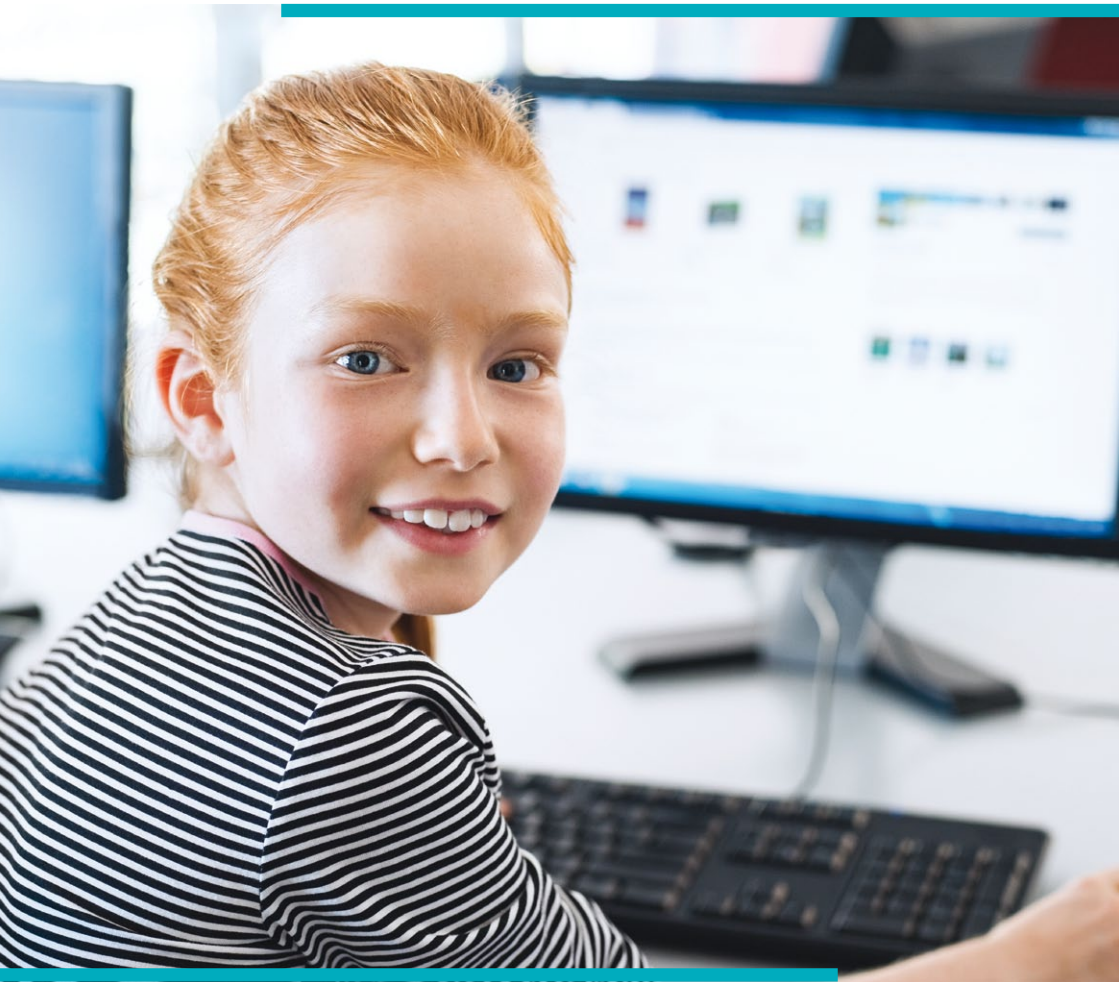


Bezpieczeństwo dzieci i młodzieży online

Kompendium dla rodziców i profesjonalistów

DAJEMY DZIECIOM SIŁĘ

NASK

saferinternet.pl

Współfinansowane przez Unię Europejską
Instrument "Łącząc Europę"

Główny Partner:

Fundacja orange

Bezpieczeństwo dzieci i młodzieży online

Kompendium dla rodziców i profesjonalistów

Bezpieczeństwo dzieci i młodzieży online. Kompendium dla rodziców i profesjonalistów

Polskie Centrum Programu Safer Internet
Warszawa 2018

www.saferinternet.pl

NASK – Państwowy Instytut Badawczy
ul. Kolska 12
01-045 Warszawa
www.nask.pl

Fundacja Dajemy Dzieciom Siłę
ul. Walecznych 59
03–932 Warszawa
www.fdds.pl

Redakcja: Anna Rywczyńska, Szymon Wójcik

Opracowanie graficzne i skład: Ewa Brejnakowska-Jończyk, www.ewa-bj.pl

Publikacja dofinansowana ze środków
Unii Europejskiej, Instrument „Łącząc Europę”

Partnerem publikacji jest Fundacja Orange

ISBN 978-83-65448-13-2

Spis treści

Wstęp

/Anna Rywczyńska, Szymon Wójcik/

Każdego dnia, wychowując bądź ucząc dziecko, podejmujemy wiele decyzji. Mamy świadomość, że kształtujemy zachowania, które w przyszłości będą wpływać na jego życie. Nie jesteśmy w stanie uchronić dzieci przed wszystkimi potencjalnymi zagrożeniami. Możemy jednak przygotować je na trudne sytuacje i dać im wsparcie, tak aby mogły sobie z nimi radzić.

Jedną z aktywności, która od początku wymaga mądrego przewodnictwa, jest kontakt młodych ludzi z internetem. Kiedyś – nowe zjawisko, dziś – codzienność, niezmiennie jednak wyzwanie dla rodziców i nauczycieli.

Globalna sieć przynosi coraz większe możliwości rozwojowe, ale może też być źródłem sytuacji ryzykownych. Niepodważalnym faktem jest to, że rozwijanie kompetencji cyfrowych jest bardzo ważnym elementem funkcjonowania we współczesnym świecie, ale nawet temu towarzyszą dylematy: kiedy i jak rozpocząć przygodę dziecka z internetem? Jak długo pozwolić dziecku korzystać z urządzeń ekranowych? W jaki sposób uchronić młodych ludzi przed szkodliwymi i niebezpiecznymi treściami? Często potrzebujemy wskazówek, jak pomóc młodym świadomie budować swój „cyfrowy profil", jak bezpiecznie zarządzać relacjami w sieci czy też chronić swoją prywatność. Podejmowane wybory zawsze będą indywidualną decyzją dostosowaną do naszych doświadczeń, charakteru i zainteresowań dziecka, jego predyspozycji i pasji, ale część z nich może być też wsparta bardzo konkretną wiedzą dotyczącą istniejących rekomendacji, zidentyfikowanych zagrożeń oraz skutecznych działań profilaktycznych. Taka jest właśnie rola Polskiego Centrum Programu Safer Internet tworzonego przez NASK – Państwowy Instytut Badawczy oraz Fundację Dajemy Dzieciom Siłę, które od 2005 r., w ramach wspólnego projektu europejskiego, popularyzują wiedzę o świadomym uczestnictwie w świecie cyfrowym, przestrzegają przed zagrożeniami online oraz reagują na zagrożenia w sieci zgłaszane przez polskich internautów.

Oddajemy w Państwa ręce nową edycję Kompendium *Bezpieczeństwo dzieci i młodzieży online*, które ma na celu usystematyzowanie najnowszej wiedzy dotyczącej aktywności dzieci i młodzieży w internecie. Czytelnik znajdzie w nim diagnozę zjawisk społecznych zachodzących w sieci, analizę sytuacji ryzykownych, ze szczególnym uwzględnieniem ich przyczyn i sposobów zapobiegania zagrożeniom oraz dostanie bogatą gamę wskazówek profilaktycznych i edukacyjnych. Świat internetu zmienia się bardzo szybko. W stosunku do poprzedniej edycji nie tylko zmieniliśmy układ treści, ale też dodaliśmy rozdziały poświęcone wyzwaniom, które przed kilkoma laty w zasadzie nie istniały – np. zagrożeniom informacyjnym. Mamy nadzieję, że wszystko to pomoże rodzicom i nauczycielom mądrze wprowadzać dzieci w świat cyfrowego obywatelstwa.

Rozdział I

Cyfrowy świat dzieci i młodzieży

/Marcin Bochenek, Agnieszka Wrońska/

I.1. Dzieci i młodzież jako użytkownicy sieci w perspektywie badań

Od momentu powstania internet cieszy się wielkim powodzeniem. W ostatnich dziesięciu latach można zauważyć niezwykle dynamiczny wzrost zarówno dostępu do globalnej sieci, jak i wykorzystania sieci w sferze społecznej, kulturalnej i biznesowej. Na ów wzrost składa się wiele czynników, przede wszystkim łatwy dostęp do technologii, który jeszcze dwadzieścia kilka lat temu mieli nieliczni.

Podczas gdy w 2008 r. w Polsce nieco ponad połowa gospodarstw domowych z dziećmi miała dostęp do globalnej sieci, dzisiaj jest to 99,2 proc. (GUS, 2018).

Internet staje się popularnym narzędziem komunikacji nie tylko z powodu łatwej dostępności, ale również malejących kosztów ekonomicznych ponoszonych przez jego użytkowników. Na atrakcyjność sieci składają się też inne czynniki, np.: możliwość pozyskiwania aktualnych informacji, praktycznie nieograniczony dostęp do różnorodnych zasobów, możliwość komunikacji z internautami z całego świata, multimedialność, a także hipertekstualność.

Dlatego też dzieci i młodzież, dorastając w otoczeniu nowoczesnych technologii, traktują i postrzegają korzystanie z internetu, a także znajdujących się w nim serwisów informacyjnych, edukacyjnych, społecznościowych i rozrywkowych, komunikatorów i rozmaitych aplikacji jako nieodłączny element ich codzienności domowej, szkolnej i środowiskowej. Podejmują one wiele rozmaitych aktywności w sieci, która w ich opinii jest „od zawsze" i która stanowi naturalne otoczenie, towarzyszące im w domu, szkole, przestrzeni publicznej. Z raportu przygotowanego w 2016 r. (Orange Polska, 2016) wynika, że przeważająca większość najmłodszych użytkowników sieci (68 proc.) twierdzi, iż trudno im wyobrazić sobie codzienność bez internetu, a około 60 proc. badanych uważa, że bez dostępu do sieci życie nie byłoby takie ciekawe.

Nastolatki wykazują się szczególnie intensywną aktywnością w internecie. Korzystanie z sieci stało się dla nich naturalnym elementem zachowania. Dzięki technologii mobilnej młodzi mają stały dostęp do internetu. Wyniki analiz prowadzonych przez różne grupy badaczy potwierdzają, że niemal cała populacja współczesnych nastolatków korzysta z sieci.

Z publikacji *Raport z badania. Nastolatki 3.0* (Tanaś i in., 2017) wynika, że zdecydowana większość młodzieży (ponad 80 proc.) deklaruje, iż korzysta z internetu wielokrotnie w ciągu dnia. Ponad 30 proc. badanych przyznało, że jest stale online. Analizy zamieszczone w raporcie dowodzą, że zaledwie 0,7 proc. młodych ludzi w ogóle nie korzysta z sieci.

Podobne zestawienie zamieszczono w raporcie *Cybernauci – diagnoza wiedzy, umiejętności i kompetencji dzieci i młodzieży, rodziców i opiekunów oraz nauczycieli w zakresie bezpiecznego korzystania z internetu* (Baran, Cichocka, Maranowski, 2016). W tej publikacji dowiedziono, że prawie 80 proc. ankietowanych uczniów, pytanych o częstotliwość korzystania z internetu, odpowiedziało: „kilka razy dziennie oraz bardzo często" (łącznie).

Stała obecność młodych ludzi online jest oczywistym skutkiem rozpowszechnienia się urządzeń mobilnych. Raporty *Nastolatki 3.0* (Tanaś i in., 2017), *Cybernauci* (Baran i in., 2016) oraz *Rodzice i dzieci wobec zagrożeń dzieci w internecie* (Orange Polska, 2016) wskazują, że najbardziej popularnymi narzędziami wykorzystywanymi do łączenia się z siecią są: smartfon oraz laptop, dużo rzadziej wykorzystywany jest komputer stacjonarny. Wielu rodziców przyznało, że ich dziecko ma własny sprzęt komputerowy i/lub urządzenie mobilne wyposażone w taki limit transferu, że może dowolnie korzystać z internetu w wybranym przez siebie miejscu i czasie.

Z danych zamieszczonych w publikacji Eurostatu (Eurostat Statistics Explained, 2017) wynika, że liczba urządzeń mobilnych posiadanych przez dzieci zwiększa się z każdym rokiem, i jest zależna od wieku właściciela. Według raportu UKE (Raport UKE, 2017) aż 83 proc. dzieci w wieku 7–14 lat ma telefon komórkowy.

Analizy badań, które zamieszczono w tekście *Korzystanie z urządzeń mobilnych przez małe dzieci* (Bąk, 2015), pokazują, że aż 25 proc. dzieci w wieku przedszkolnym korzysta z urządzeń mobilnych codziennie. Rodzice dają dzieciom tablety lub smartfony zarówno do zabawy, jak i podczas jedzenia posiłków czy przy usypianiu.

Cyfrowy świat już od najwcześniejszych lat towarzyszy dzieciom w ich aktywnościach poznawczych, rozrywkowych i interakcyjnych. A wiek, w którym najmłodsi internauci zaczynają samodzielnie korzystać z sieci, systematycznie się obniża. Jeszcze kilka lat temu twierdzono, że dzieci zaczynają swoją przygodę z siecią w wieku 9–10 lat. Obecnie wielu badaczy (Orange Polska, 2016; Eurostat Statistics Explained, 2017; Lange, Bochenek, Wrońska, 2018) uważa, że dzieci stają się użytkownikami internetu w wieku 6–7 lat i poniżej.

Dla młodych ludzi sieć stanowi źródło wiedzy, informacji, jest wsparciem w nauce szkolnej, miejscem rozrywki i realizacji zainteresowań, a także coraz częściej – przestrzenią do wyrażania emocji, nawiązywania i budowania relacji społecznych, kreowania swojego wizerunku, miejscem aktywności twórczej.

Wśród nastolatków niemal każdy jest członkiem jakiejś wirtualnej społeczności, z którą porozumiewa się za pomocą czatów, komunikatorów czy portali społecznościowych. Internet służy im głównie do celów komunikacyjnych i rozrywkowych, nieco rzadziej edukacyjnych. Głównymi przyczynami korzystania z sieci przez młodych ludzi są przede wszystkim interakcje pośrednie oraz cele rozrywkowe: dostęp do serwisów społecznościowych, kontakty ze znajomymi, słuchanie muzyki i oglądanie filmów (Konopczyński, Lange, Osiecki, 2014).

Dzieci i młodzież traktują nowoczesne technologie jako doskonałe narzędzie edukacyjne, które pozwala im zarówno na pogłębianie posiadanych już wiadomości, jak i poszukiwanie nowych informacji. W wielu badaniach zdiagnozowany został problem częstego braku wsparcia w rozwijaniu kompetencji cyfrowych ze strony rodziców i opiekunów. Młodzi ludzie bardzo często deklarują, że internet poznają na drodze samoedukacji. Przeprowadzone analizy ukazują, że choć rodzice przyznają, iż to oni są odpowiedzialni za bezpieczeństwo najmłodszych osób w sieci (Orange Polska, 2016), to jednak dzieci nie postrzegają ich jako przewodników w wirtualnym świecie (Tanaś i in., 2017).

Skala i sposoby wykorzystania internetu przez młodzież w kontekście rozwoju kompetencji cyfrowych – informatycznych, jak i informacyjnych (Batorski, Płoszaj, 2012), specjalistycznych czy społecznych, skłaniają do tego, aby mówić o nim w kategoriach szans i wyzwań, które przynosi użytkownikom. Internet może być postrzegany jako centrum zarządzania życiem osobistym, szkolnym, rekreacją, jako źródło wiedzy i informacji oraz medium prezentacji siebie i narzędzie do kreacji i wymiany myśli. Z jednej strony sieć daje ogromne możliwości edukacyjne i twórcze, z drugiej jednak nie należy zapominać, że korzystanie z internetu czasem wiąże się z zagrożeniami, które mogą mieć konsekwencje w różnych sferach życia.

Młodzi twórcy w sieci

W 2018 r. zespół badawczy z NASK wspólnie z prof. Jackiem Pyżalskim przeprowadzili badanie poświęcone aktywności młodych twórców internetowych: *Blogerzy, youtuberzy i inni – świat młodych twórców internetu*, analizując aktywność młodzieży w sieci.

Przebadanych zostało przeszło 100 młodych internautów w wieku 13–18 lat tworzących w internecie oryginalne treści. Badanie polegało na 60-minutowej swobodnej rozmowie z każdym z respondentów. Nowatorski charakter badania jest godny podkreślenia, ponieważ do tej pory europejscy badacze przeważnie skupiali się na analizie postaw i zachowań młodych internautów, a także zajmowali się zagadnieniami związanymi z bezpieczeństwem podczas korzystania z sieci. Badania nad oryginalną twórczością zamieszczaną w internecie, jako formą pozytywnej aktywności, należą do rzadkości. Ponadto warto zauważyć, że jeśli nawet naukowcy decydują się na obserwację takiej sfery działalności młodych użytkowników sieci, to jednak wówczas przeprowadzają badania w kilkunastoosobowych grupach.

Badanie *Blogerzy, youtuberzy i inni – świat młodych twórców internetu* miało charakter jakościowy i pozwoliło nakreślić obraz młodego, twórczego polskiego internauty. Ważną informacją uzyskaną przez badaczy jest ta, że aktywność online nie musi oznaczać zerwania ze światem offline. Wprost przeciwnie. Poniżej zamieszczono kilka danych, które doskonale ilustrują to stwierdzenie.

- Aż 40 proc. badanych blogerów prowadziło również tradycyjny pamiętnik.
- Aż 22 proc. regularnych graczy online spotyka się też na gry offline, m.in. aby grać w klasyczne planszówki.
- Aż 48 proc. administratorów w sieci pełni też role liderów offline.

Czy światy online i offline to jedno? Tu zdania odpowiadających były podzielone. Poszczególni respondenci w odmienny sposób opisywali, jak widzą zależność między tymi dwoma światami. „Przepływanie" pomiędzy tymi rzeczywistościami jest dla nich zupełnie naturalne, tak jak naturalnie czują się w każdej z nich.

Dlaczego podjęli ten trud, dlaczego poświęcają swój czas na tworzenie? To z jednej strony chęć sprawdzenia się, ale z drugiej – potrzeba zaprezentowania swoich umiejętności i wiedzy. Starają się to robić profesjonalnie, wielu z pytanych ciągle doskonali swoje umiejętności. Wszystko to prowadzi do sytuacji, w której całkiem spora grupa zarabia na swojej działalności. Czy wiążą więc przyszłość zawodową i prywatną ze swoją obecną aktywnością w sieci? Taką deklarację składają tylko niektórzy respondenci. Warto jednak zauważyć, że duża grupa takiej możliwości nie wyklucza.

Dla młodych twórców internetowych ważna jest współpraca, ale także dzielenie się pasją z innymi („Największą satysfakcję daje mi to, że mogę dzielić się z innymi tym, co kocham robić"). Podkreślają, że konieczny jest szacunek dla odbiorców. Uznanie, którego doświadczają, stanowi motywację do działania. Internet ich zmienia. Choć bycie aktywnym i rozpoznawalnym ma swoje ciemne strony – hejt, czasami niechęć ze strony innych użytkowników – to jednak przeważają dobre strony aktywności w sieci. Młodzi twórcy są przekonani, że kontakty z ludźmi są ważne oraz że warto i należy być sobą.

Twórcza aktywność młodych ludzi w sieci to nowe zjawisko, bo i możliwość takiej ekspresji swoich umiejętności jest nowa. Warto tę możliwość spożytkować także w procesie edukacji szkolnej. Oczywiście nie każdy młody internauta, a dziś znaczy to w praktyce, że nie każdy młody człowiek, będzie internetowym twórcą. Warto jednak zauważyć, iż upowszechnianie, pokazywanie innego, bardziej twórczego korzystania z sieci daje szansę na podniesienie poziomu cyfrowej świadomości. To niezwykle istotne w dobie zalewu tzw. fake newsów i niskiej jakości treści znajdujących się w sieci. Nauczyciele, wychowawcy i rodzice stają dziś więc z jednej strony przed wyzwaniem, z drugiej przed szansą. Przed wyzwaniem, bo praca z młodymi twórcami, pokazywanie takich przykładów nie są łatwym procesem. Przed szansą, bo dla wielu innych młodych ludzi właśnie przykład rówieśników będzie tym, na którym będą chcieli się wzorować.

W praktyce uzyskane wnioski i rekomendacje, które opracowano na bazie różnorodnych i wielopłaszczyznowych badań, mogą stać się podstawą do projektowania i modelowania skutecznych działań w zakresie przygotowania najmłodszych użytkowników do twórczego i bezpiecznego wykorzystania możliwości świata cyfrowego.

Bibliografia

1. Baran M., Cichocka E., Maranowski P., Pander W., (2016), *Cybernauci – diagnoza wiedzy, umiejętności i kompetencji dzieci i młodzieży, rodziców i opiekunów oraz nauczycieli w zakresie bezpiecznego korzystania z internetu. Raport podsumowujący badanie ex-ante*, Warszawa: Fundacja Nowoczesna Polska, Collegium Civitas, zob. bit.ly/cyberna (dostęp: 02.01.2019).
2. Batorski D., Płoszaj A., (2012), *Diagnoza i rekomendacje w obszarze kompetencji cyfrowych społeczeństwa i przeciwdziałania wykluczeniu cyfrowemu w kontekście zaprogramowania wsparcia w latach 2014–2020*, Warszawa: Ministerstwo Rozwoju Regionalnego, zob. bit.ly/cyfrwyk (dostęp: 02.01.2019).
3. Bąk A., (2015), *Korzystanie z urządzeń mobilnych przez małe dzieci. Wyniki badania ilościowego*, Warszawa: Fundacja Dzieci Niczyje, zob. bit.ly/mobdzie (dostęp: 02.01.2019).
4. Eurostat Statistics Explained, (2017), *Digital economy and society statistics – households and individuals*, zob. bit.ly/eurostt (dostęp: 02.01.2019).
5. Główny Urząd Statystyczny (GUS) (2017), *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2013–2017*, Warszawa: Zakład Wydawnictw Statystycznych, zob. bit.ly/spinf17 (dostęp: 02.01.2019).
6. Główny Urząd Statystyczny (GUS) (2018), *Społeczeństwo informacyjne w Polsce w 2018 roku*, zob. bit.ly/spinf2018 (dostęp: 02.01.2019).
7. Konopczyński M., Lange, R., Osiecki J. i in., (2014), *Ogólnopolskie badanie. Nastolatki wobec internetu*. Raport opracowany na zlecenie Rzecznika Praw Dziecka i NASK przez Pedagogium WSNS w okresie maj – czerwiec 2014, Warszawa: NASK – Państwowy Instytut Badawczy, zob. bit.ly/naswint (dostęp: 02.01.2019).
8. Lange R., Bochenek M., Wrońska, A., Niedzielska-Barczyk D., (2018), *Raport. Dziecko w świecie smartfonów*, Warszawa: NASK – Państwowy Instytut Badawczy, zob. bit.ly/dzsmart (dostęp: 02.01.2019).
9. Orange Polska (2016), *Rodzice i dzieci wobec zagrożeń dzieci w internecie.* Raport z badania przygotowany przez TNS Polska S.A. na zlecenie Orange Polska, we współpracy z Fundacją Orange i Fundacją Dajemy Dzieciom Siłę, zob. bit.ly/rdwzagr (dostęp: 02.01.2019).
10. Tanaś M., Kamieniecki W., Bochenek M., Wrońska A., Lange R., Fila M., Loba B., Konopczyński F., (2017), *Raport z badania. Nastolatki 3.0*, Warszawa: NASK – Państwowy Instytut Badawczy, zob. bit.ly/rapnas3 (dostęp: 02.01.2019).
11. Urząd Komunikacji Elektronicznej (UKE), (2017), *Badanie opinii publicznej w zakresie funkcjonowania rynku usług telekomunikacyjnych oraz preferencji konsumentów. Raport z badania dzieci i rodziców*, Warszawa/Gdańsk: Urząd Komunikacji Elektronicznej.
12. Wrońska A., Lange R., (2016), *Nastolatek jako użytkownik internetu – społeczny wzorzec konsumpcji*, w: Tanaś M. (red.), *Nastolatki wobec internetu*, Warszawa: NASK – Państwowy Instytut Badawczy, s. 15–26, zob. bit.ly/naswint (dostęp: 02.01.2019).

I.2. Bezpieczny start. Internet w życiu małych dzieci i rodziny

/Ewa Dziemidowicz/

Internet dzięki urządzeniom mobilnym stał się integralną częścią naszego życia. Udostępniamy go coraz młodszym dzieciom, sami również jesteśmy jego intensywnymi użytkownikami. W perspektywie rozwoju dziecka internet wykorzystywany w przemyślany i zrównoważony sposób może nieść za sobą wiele korzyści i być wartościowym narzędziem edukacji i rozrywki. Jednak zbyt wczesne i niekontrolowane udostępnianie mediów elektronicznych najmłodszym dzieciom może doprowadzić do szeregu zaburzeń i mieć negatywny wpływ na ich rozwój. Badania pokazują, że ponad 40 proc. rocznych i dwuletnich dzieci korzysta z tabletów lub smartfonów. Godne zauważenia jest to, że niemal co trzecie dziecko w tym wieku korzysta z urządzeń mobilnych codziennie lub prawie codziennie. Ponad 13 proc. rocznych i dwuletnich dzieci ma własny tablet lub smartfon. Co ciekawe, 60 proc. rodziców, których zapytano o powody udostępniania najmłodszym urządzeń mobilnych, deklaruje, że w ten sposób zapewnia dziecku rozrywkę. Co czwarty ankietowany przyznaje, że pozwala na korzystanie ze smartfonu lub tabletu, ponieważ chce, aby dziecko zjadło posiłek, a 18 proc. badanych potwierdza, że udostępnia swemu dziecku urządzenia mobilne po to, aby zasnęło (Bąk, 2015).

Intensywna obecność internetu nie tylko wśród dzieci, lecz także wśród rodziców wpływa negatywnie na relacje w rodzinie. To, co coraz częściej odciąga dorosłych od bycia w bliskim kontakcie z dzieckiem, to właśnie smartfony czy inne urządzenia ekranowe z dostępem do internetu.

Zagrożenia dla rozwoju i zdrowia

W pierwszych latach życia mózg człowieka rozwija się najintensywniej i jest bardzo wrażliwy na czynniki zewnętrzne, a także na działanie napięć emocjonalnych. Do prawidłowego rozwoju dziecko potrzebuje doświadczać świata wszystkimi zmysłami, a ograniczanie mu pola działania i rodzaju bodźców może mieć negatywny wpływ na rozwój struktur neuronowych jego mózgu (Mack, 2012; Walsh i in., 2018).

Poprawny rozwój dziecka wymaga interakcji angażujących wszystkie zmysły, z udziałem innych osób poświęcających mu czas i uwagę. W ten sposób dzieci rozwijają swoje umiejętności poznawcze, językowe, motoryczne i budują umiejętności społeczne. Dostęp do nowoczesnych technologii nie zastąpi wspólnej zabawy z bliskimi, czytania książek i innych doświadczeń, dzięki którym dzieci poznają otaczający je świat.

Trzeba także pamiętać, że intensywne korzystanie osób małoletnich z ekranowych urządzeń mobilnych, a także dostęp do treści niedopasowanych do ich wieku mogą powodować zaburzenia koncentracji. Taka sytuacja na dalszym etapie rozwoju dzieci może doprowadzić do trudności w opanowywaniu umiejętności czytania i pisania oraz nawiązywaniu kontaktów społecznych.

Nadmiarowy czas spędzany przed ekranami, szczególnie przed snem, negatywnie wpływa na jakość snu, a w efekcie na regenerację organizmu dziecka. Badania pokazują również, że takie sytuacje powodują szkody dla wzroku dzieci (Rechichi, De Mojà, Aragona, 2017). Wodzenie palcami po ekranach przez najmłodsze dzieci stanowi również zagrożenie dla rozwoju tzw. motoryki małej, czyli prawidłowego rozwoju palców i dłoni.

Dzieci spędzające dużo czasu online narażone są na uzależnienie. Coraz częściej dotyczy to nawet kilkulatków, którzy pozbawieni dostępu do sieci i swoich ulubionych treści tracą zdolność prawidłowego funkcjonowania, reagują emocjonalnie, zdarza się, że agresywnie. Dlatego tak ważne są właściwe proporcje pomiędzy czasem spędzanym przed ekranami a innymi aktywnościami.

Dzieci do ukończenia drugiego roku życia nie powinny mieć dostępu do urządzeń ekranowych (American Psychological Association, 2017), natomiast w przypadku starszych dzieci należy dołożyć starań, aby codziennie nie korzystały z urządzeń mobilnych tak intensywnie. Dobrym pomysłem jest ustalenie przez rodziców dnia lub dni (np. weekendu) bez elektroniki. Warto pamiętać, aby jednorazowo dzieci miały dostęp do sieci nie dłużej niż 15–20 min. Dzienny kontakt z wszelkimi urządzeniami ekranowymi nie powinien przekraczać od 30 do 60 min (w zależności od wieku dziecka).

Zagrożenie uzależnieniem od sieci, poza intensywnością dostępu, wzmacniane jest przez nagradzanie dzieci dostępem do urządzeń elektronicznych, zachęcanie nimi do jedzenia czy wykonywania innych codziennych czynności albo wykorzystywanie ich do uspakajania dziecka, szczególnie w sytuacjach jego silnych emocji. Tymczasem dzieci, przy uważnym i kochającym wsparciu i przewodnictwie rodziców, uczą się radzić sobie z emocjami, nazywać swoje potrzeby, rozmawiać i poszukiwać rozwiązań w sytuacjach, które są dla nich wyzwaniem, czy też wymyślać aktywności, które pomogą im opanować nudę.

Relacje

Do prawidłowego rozwoju dziecko potrzebuje bliskiej relacji z dorosłym – rodzicem, opiekunem – który jest wrażliwy na jego uczucia, potrzeby i adekwatnie na nie odpowiada, który poświęca mu czas i uwagę, jest ciekawy jego świata, okazuje mu miłość i akceptację. Bezwarunkowa, niezakłócona uwaga rodzica, nastawiona na bycie z dzieckiem tu i teraz, rozwija wewnętrzne zasoby dziecka, wzmacnia jego pewność siebie, pozytywnie wpływa na odporność psychiczną dziecka.

W mózgach dzieci, które w pierwszych latach życia nie dostawały wsparcia w radzeniu sobie z intensywnymi uczuciami i przeżyciami, często nie wykształcają się ścieżki umożliwiające im radzenie sobie z różnymi stresorami w przyszłości (Boćko-Mysiorska, 2017). Rodzic, który jest nieobecny, którego uwaga w kontakcie z dzieckiem zakłócona jest innymi czynnościami, np. przeglądaniem internetu, który przerywa kontakt czy zabawę, żeby sprawdzić powiadomienia lub zajrzeć na portale społecznościowe, daje dziecku wyraźny komunikat, że coś jest dla niego ważniejsze niż ono. Dziecko zostaje samo ze swoimi przeżyciami, potrzebami czy lękami, jest porzucane w trakcie interakcji albo nawet nie udaje mu się do tej interakcji doprowadzić. Uderza to w jego fundamentalne poczucie własnej wartości i ważności dla osób, które są jego głównym punktem odniesienia.

Od kilku lat coraz częściej pojawiają się inicjatywy zachęcające rodziny do rezygnowania ze smartfonów i innych urządzeń ekranowych przez określony czas. Wiele szkół wprowadza ograniczenia dotyczące korzystania z elektroniki na terenie placówek. Na początku eksperymenty te powodują negatywne, emocjonalne reakcje wśród uczestników, jednak ich końcowy rezultat najczęściej jest pozytywny: rodziny na nowo uczą się spędzać ze sobą czas, tworzą nowe rytuały, odnajdują wspólne zainteresowania, a uczniowie poprawiają swoją koncentrację i osiągają lepsze wyniki w nauce. Oczywiście, wszelkie działania tego typu muszą uwzględniać konieczność mądrego zagospodarowania technologii w domu i szkole, a dążenie do uregulowania aktywności online dzieci nie może skutkować odcięciem ich od możliwości wykorzystania nowych mediów do nauki.

Z pożytkiem dla dziecka

Nieodpowiedzialne udostępnianie dzieciom urządzeń elektronicznych może nieść wiele zagrożeń. Jednak korzystanie przez dzieci w wieku od 3 do 6 lat z urządzeń mobilnych może też mieć pozytywny wpływ na ich rozwój społeczny, emocjonalny, moralny i poznawczy. Odpowiednio dobrane aplikacje mobilne mogą m.in.:

- zachęcać dzieci do budowania i podtrzymywania interakcji rówieśniczych oraz interakcji z osobami dorosłymi (np. rodzicami i innymi członkami rodziny),
- prezentować dzieciom pozytywne wzorce i uczyć je ważnych wartości społecznych,
- dostarczać satysfakcji związanej z wygraną, poprawianiem wyników, docenieniem ich twórczości (m.in. dzięki możliwości archiwizowania i przesyłania prac plastycznych itp.),
- umożliwiać naukę przez obraz i dźwięk, uczyć bezpiecznego i odpowiedzialnego wykorzystania technologii,
- stymulować naukę pisania, rozwój mowy i kompetencji językowych dzieci, uaktywniać inteligencję wizualną dzieci, niwelować skutki nierówności społecznych i rozwojowych.

Na podstawie: J. Pyżalski, M. Klichowski, M. Przybyła, *Szanse i zagrożenia w obszarze wykorzystania technologii informacyjno-komunikacyjnych (TIK), ze szczególnym uwzględnieniem aplikacji mobilnych przez dzieci w wieku 3–6 lat*.

Pozytywne treści

Na rynku występuje bardzo wiele aplikacji i treści, które producenci opisują jako edukacyjne. W rzeczywistości jednak okazuje się, że w procesie ich tworzenia nie biorą udziału eksperci znający specyfikę rozwoju małych dzieci. Co gorsza, nie ma również badań, które potwierdzałyby realną jakość i wartość istniejących aplikacji i materiałów edukacyjnych przeznaczonych dla najmłodszych. Technologie te powinny być interaktywne i zapewniać wszechstronny rozwój dzieci, a nie tylko oferować im możliwość przesuwania palcem po ekranie.

Poniżej zamieszczono wykaz cech, jakimi powinny wyróżniać się technologie przeznaczone dla dzieci (Klichowski, Pyżalski, Kuszak, 2017).

1. Muszą bazować na konkretnych celach pedagogicznych, odnoszących się do kształtowania umiejętności, postaw, wartości, a także stymulować procesy poznawcze.
2. Powinny umożliwiać dziecku wchodzenie w interakcje ukierunkowane na pozyskanie informacji lub podzielenie się własnym doświadczeniem.
3. Powinny integrować treści, umożliwiać konstruowanie umysłowej reprezentacji świata jako całości oraz być narzędziem towarzyszącym innym (pozamedialnym) procesom poznawania tego świata.

4. Muszą tak stymulować pracę dziecka, by jego działania miały charakter np. zabawy, gry, eksploracji. Ich zadaniem jest także stworzeniem warunków pozwalającym najmłodszym na wchodzenie w różnorakie role i eksperymentowanie.
5. Muszą być tak skonstruowane, by dziecko kontrolowało przebieg swojej zabawy; ponadto technologie powinny być dostosowane do aktualnego nastroju, samopoczucia, stanu zdrowia dziecka itp.
6. Powinny być intuicyjne; powinny bazować na krótkich zadaniach oraz mieć przejrzysty i zrozumiały układ treści.
7. Nie mogą przyczyniać się do rozpowszechniania się stereotypów (np. dotyczących ról płciowych, rasy), a także do umacniania strukturalnej i symbolicznej przemocy (np. deprecjonowania osób o niskim kapitale ekonomicznym lub promowania jednostek reprezentujących określone wyznanie).
8. Muszą mobilizować różne sfery aktywności dziecka, skłaniać do ruchu i działań niezwiązanych z ich obsługą; jednorazowa aktywność dziecka, polegająca tylko na obsłudze urządzenia elektronicznego, nie powinna trwać dłużej niż 20 minut.
9. Powinny włączać osoby dorosłe bliskie dziecku w zabawę małoletniego, zarówno w kontekście facylitacji, kontroli, jak i wsparcia oraz stymulacji.

Pomimo że odpowiednio dobrane treści internetowe mogą mieć pozytywny wpływ na rozwój dzieci, to zbyt wczesne i intensywne korzystanie z urządzeń elektronicznych może być dla nich szkodliwe.

Internet w domu

Każda rodzina, uwzględniając swoje wartości, potrzeby i zwyczaje, powinna ustalić własne zasady dotyczące korzystania z nowych technologii i internetu. Dzieci muszą rozumieć, dlaczego korzystanie z mediów elektronicznych jest regulowane zasadami. Ponadto najmłodsi internauci powinni być świadomi, że ograniczenie dostępu do sieci nie jest wymierzoną w nich karą. Stanowi natomiast wartość samą w sobie i powinno być postrzegane w kategorii zysków. Dzieci muszą być pewne, że stanowisko rodziców – związane z koniecznością ustalenia przejrzystych zasad korzystania z urządzeń dających dostęp do internetu – wynika z troski o dobro dzieci i zmierza do wzmocnienia wzajemnych więzi, jest wyrazem szacunku i otwartości.

Pewne ustalone reguły związane z dostępem do sieci oraz urządzeń ekranowych powinny obejmować wszystkie osoby w rodzinie, w tym dorosłych. Dzieci bowiem uczą się o wiele lepiej, obserwując to, co robią rodzice, niż tylko słuchając wydawanych przez nich dyspozycji i nakazów. Bliskie dorosłe osoby pełnią w życiu dzieci i młodzieży bardzo istotną rolę, tworząc odpowiednie wzorce zachowania. Dlatego też rozmowy na temat internetu i/lub treści zamieszczanych w sieci, a także zasad korzystania z niej powinny być regularnym zwyczajem, a nie jednorazowym incydentem.

Poniżej zamieszczono kilka rozwiązań, które warto wprowadzić do swojej rodziny, ustalając zasady korzystania z urządzeń ekranowych.

- Poranne i wieczorne rytuały (począwszy od kolacji aż do zaśnięcia dzieci) powinny być czasem wolnym od urządzeń ekranowych. Szczególnie istotne jest to, aby rodzice nie udostępniali dzieciom mediów elektronicznych minimum godzinę przed zaśnięciem. Badania wykazują, że małe dzieci, którym zezwolono przed snem na korzystanie z urządzeń ekranowych, sypiają w nocy znacznie krócej niż maluchy pozbawione takiego dostępu. Przyczyną takiej sytuacji są nie tylko treści zamieszczone w mediach, ale przede wszystkim niebieskie światło emitowane przez urządzenia ekranowe, które hamuje uwalnianie melatoniny, pobudza organizm, a tym samym ma niekorzystny wpływ na jakość i długość snu dziecka.
- Dobrym pomysłem jest wyłączenie telefonów na noc i włączanie ich dopiero rano. Warto też pamiętać o tym, aby ładować telefony w innym pomieszczeniu niż to, w którym śpi dziecko (Shifrin, Brown, Jana, 2015).
- Wszystkie rodzinne posiłki, nie tylko w domu, i spotkania przy stole powinny być wolne od mediów. To dobry moment na budowanie relacji – rozmowę, okazanie zainteresowania, wspólną zabawę. Korzystanie z urządzeń podczas posiłków odwraca uwagę od jedzenia i powoduje, że dzieci jedzą niejako automatycznie, bez świadomości tego, co i ile jedzą, oraz bez zwracania uwagi na smak, zapach czy teksturę potraw. Sprzyja to tworzeniu się nieprawidłowych nawyków żywieniowych i jest związane z otyłością i przyrostem masy ciała u dzieci.
- Dobrze jest zadbać o czas rodzinny bez elektroniki – to mogą być wszystkie te momenty, kiedy rodzina jest razem, albo określone sytuacje, np. w samochodzie, podczas spaceru, w drodze do przedszkola, podczas zabawy itd. Każda taka okazja to czas na pogłębianie relacji i poznawanie dziecka.
- Ważne jest, żeby ustalić kiedy, ile czasu i w jaki sposób dzieci mogą korzystać z mediów elektronicznych. W przypadku najmłodszych największy potencjał edukacyjny ma oglądanie odpowiednio dobranych treści czy korzystanie z aplikacji mobilnych wspólnie z opiekunami.

Rodzice powinni zwracać uwagę na tworzenie się nowych nawyków i rytuałów u dzieci, ponieważ te szybko przyzwyczajają się do konkretnych rozwiązań (np. dostępności do tabletu, kiedy bliski dorosły chce porozmawiać przez telefon).

Pamiętaj!

- Zadbaj o to, aby dzieci przed ukończeniem drugiego roku życia nie miały kontaktu z urządzeniami ekranowymi, w tym z tabletami i smartfonami.
- Pilnuj, aby starsze dzieci nie korzystały z urządzeń mobilnych codziennie.
- Ustal dzień lub dni w tygodniu (np. weekend) bez urządzeń ekranowych.
- Pamiętaj, aby jednorazowo dzieci miały dostęp do urządzeń mobilnych nie dłużej niż 15–20 min, a dzienny kontakt z wszelkimi urządzeniami ekranowymi nie przekraczał (w zależności od wieku dziecka) od 30 do 60 min.
- Uwzględniaj – podczas udostępniania dzieciom w wieku 3–6 lat urządzeń dotykowych – indywidualny etap rozwoju tych młodych osób.
- Umożliwiaj dzieciom korzystanie tylko ze sprawdzonych i dostosowanych do ich wieku treści. Monitoruj aplikacje i materiały, do których mają dostęp zarówno w domu, jak i poza nim (np. podczas zabaw z rówieśnikami).
- Sprawdzaj aplikację, zanim pokażesz ją dziecku.
- Towarzysz dzieciom podczas korzystania z mediów elektronicznych.
- Tłumacz, co się dzieje na ekranie urządzenia, a także wskazuj związek między treściami obecnymi w mediach a rzeczywistością.
- Unikaj prezentowania dzieciom treści, w których akcja toczy się bardzo szybko. Zadbaj o to, aby chronić dzieci przed obrazami zawierającymi zbyt wiele migoczących i jaskrawych elementów. Nie są one bowiem dostosowane do etapu rozwoju dzieci i ich możliwości percepcyjnych.
- Pamiętaj o tym, aby nie udostępniać dzieciom urządzeń mobilnych minimum godzinę przed snem. Promieniowanie emitowane przez ekrany sprzętów elektronicznych (zwłaszcza tabletów i smartfonów) źle wpływa na zasypianie i jakość snu. Dziecięca sypialnia powinna być strefą bez elektroniki.
- Pamiętaj, aby wyłączać urządzenia ekranowe, kiedy są nieużywane.
- Nie należy traktować możliwości korzystania z urządzeń mobilnych jako nagrody, a zakazu ich używania – jako kary. W opinii dzieci taka postawa zwiększa atrakcyjność tych urządzeń i wzmacnia przywiązanie do nich.
- Nie powinno się także wykorzystywać mediów elektronicznych do uspokajania maluchów, ponieważ może to negatywnie wpływać na zdolność opanowywania przez nie swoich emocji.
- Nie używaj urządzeń mobilnych do motywowania dzieci (np. podczas jedzenia lub wykonywania jakichś zadań).

Bibliografia

1. American Psychological Association, (2017), *Digital Guidelines: Promoting Healthy Technology Use for Children*, zob.: bit.ly/prohete (dostęp: 02.01.2019).
2. Bąk A., (2015), *Korzystanie z urządzeń mobilnych przez małe dzieci. Wyniki badania ilościowego*, Warszawa: Fundacja Dzieci Niczyje, zob. bit.ly/mobdzie (dostęp: 02.01.2019).
3. Boćko-Mysiorska M., (2017), *Brak bliskiej relacji z dzieckiem może doprowadzić do nieodwracalnych zmian w jego mózgu*, zob. bit.ly/dzsawaz (dostęp: 02.01.2019).
4. Canadian Paediatric Society, (2017), *Screen time and young children: Promoting health and development in a digital world*, w: „Paediatrics and Child Health", nr 22 (8), Ottawa, Ontario: Canadian Paediatric Society, Digital Health Task Force, s. 461–468.
5. Cash H., McDaniel K., (2014), *Dzieci konsoli. Uzależnienie od gier*, tłum. Ludwiczak B., Poznań: Media Rodzina.
6. Chiong C., Shuler C., (2010), *Learning: Is there an app for that? In Investigations of young children's usage and learning with mobile devices and apps*, Nowy York: The Joan Ganz Cooney Center at Sesame Workshop, s. 13–20, zob. bit.ly/appforl (dostęp: 02.01.2019).
7. Fuller C., Lehman E., Hicks S., Novick M.B., (2017), *Bedtime Use of Technology and Associated Sleep Problems in Children*, w: „Global Pediatric Health", 4.
8. Klichowski M., Pyżalski J., Kuszak K., Klichowska A., (2017), *Jak technologie informacyjno-komunikacyjne mogą wspierać rozwój dziecka w wieku przedszkolnym? Studium teoretyczne, w: Małe dzieci w świecie technologii informacyjno-komunikacyjnych – pomiędzy utopijnymi szansami a przesadzonymi zagrożeniami*, Pyżalski J. (red), Łódź: Wydawnictwo Eter, s. 115–157, zob. bit.ly/techroz (dostęp: 02.01.2019).
9. LeBourgeois M.K., Hale L., Chang A.M., Akacem L.D., Montgomery-Downs H.E., Buxton O.M., (2017), *Digital media and sleep in childhood and adolescence*, w: „Pediatrics", nr 140 (Supplement 2), s. 92–96, zob. bit.ly/dmsleep (dostęp: 02.01.2019).
10. Mack A.H., (2012), *Infant Media Exposure and Toddler Development. Year Book of Psychiatry and Applied Mental Health*, Philadelphia: Elsevier, s. 22–23.
11. Pyżalski J., Klichowski M., Przybyła M., (2014), *Szanse i zagrożenia w obszarze wykorzystania technologii informacyjno-komunikacyjnych (TIK), ze szczególnym uwzględnieniem aplikacji mobilnych (TIK-mobApp) przez dzieci w wieku 3–6 lat*. Badania finansowane w ramach innowacji społecznych Narodowego Centrum Badań i Rozwoju, Poznań: Uniwersytet im. Adama Mickiewicza i Narodowe Centrum Badań i Rozwoju, zob. bit.ly/tikmapp (dostęp: 02.01.2019).
12. Rechichi C., De Mojà G., Aragona P., (2017), *Video Game Vision Syndrome: A New Clinical Picture in Children?*, w: „Journal of pediatric ophthalmology and strabismus", nr 54 (6), s. 346–355.
13. Rideout V., (2017), *The Common Sense census: Media use by kids age zero to eight*, San Francisco: Common Sense Media.

14. Robinson T.N., Banda J.A., Hale L., Lu A.S., Fleming-Milici F., Calvert S.L., Wartella E., (2017), *Screen media exposure and obesity in children and adolescents*, w: „Pediatrics", nr 140 (Supplement 2), s. 97–101.
15. Shifrin D., Brown A., Jana L., Flinn S.K., (2015), *Growing Up Digital: Media Research Symposium*, American Academy of Pediatrics, s. 1–7, zob. bit.ly/grupdig (dostęp: 02.01.2019).
16. Uhls Y.T., (2016), *Cyfrowi rodzice – dzieci w sieci. Jak być czujnym, a nie przeczulonym*, Kraków: IUVI.
17. Walsh J.J., Barnes J.D., Cameron J.D., Goldfield G.S., Chaput J.P., Gunnell K.E., Ledoux A.A., Zemek R.L., Tremblay M.S., (2018), *Associations between 24 hour movement behaviours and global cognition in USA children: a cross-sectional observational study*, w: „The Lance Child and Adolescent Health", nr 2 (11), Philadelphia: Elsevier, s. 783–791.

Rozdział II

Wyzwania i zagrożenia. Na co uważać w sieci?

II.1. Cyberprzemoc i inne formy agresji w sieci

/Szymon Wójcik/

Cyberprzemoc i agresja elektroniczna w internecie to zjawiska – pośrednio lub bezpośrednio – dotyczące większości polskiej młodzieży. Opinia publiczna dostrzega jednak te zagrożenia wówczas, gdy ma miejsce jakieś tragiczne zdarzenie (np. samobójstwo Amandy Todd, 15-latki gnębionej przez rówieśników w 2012 r., lub śmierć polskiej gimnazjalistki Ani z Gdańska w 2006 r.). Nie można też zapominać o tym, że co roku w niemal każdej polskiej szkole występują przypadki nękania dzieci przez ich rówieśników. W konsekwencji prowadzi to do tego, że wielu młodych ludzi przestaje uczęszczać na zajęcia lub jest zmuszonych zmienić klasę lub szkołę.

Warto podkreślić, że w Polsce pierwszą kampanię na temat cyberprzemocy w 2008 r. przeprowadziła Fundacja Dajemy Dzieciom Siłę (dawniej Fundacja Dzieci Niczyje). Od tego czasu Polskie Centrum Programu Safer Internet i inne organizacje podejmują liczne działania profilaktyczne i edukacyjne na rzecz redukcji cyberprzemocy. Nadal jednak skala tych przedsięwzięć nie jest zbyt duża.

Terminologia

Przemoc rówieśniczą w sieci określa się angielskim terminem *cyberbullying*. W języku polskim funkcjonuje także inne pojęcie odnoszące się do tego zjawiska – cyberprzemoc, czyli przemoc z użyciem technologii informacyjnych i komunikacyjnych (internetu i telefonów komórkowych).

Jacek Pyżalski (2012, 2014) rozróżnia z kolei agresję elektroniczną (pojedyncze akty przemocy w sieci) i *cyberbullying* (działanie intencjonalne, trwające dłuższy czas, przed którym ofiara nie może się obronić). Agresję rówieśniczą w sieci podobnie definiuje amerykańskie Centrum Badań nad Cyberprzemocą (Cyberbullying

Research Center), określając ją jako „celowe i powtarzające się krzywdzenie wywołane za pomocą komputerów, telefonów komórkowych i innych urządzeń elektronicznych" (Hinduja, Patchin, 2018, s. 2; tłum. własne).

W kontekście cyberprzemocy i agresji elektronicznej pojawiają się także pojęcia hejtu i mowy nienawiści. Pierwsze z nich pochodzi z języka potocznego i przyjmuje różne znaczenia. Niekiedy hejt utożsamia się z mową nienawiści, ale znacznie częściej pojęcie to rozumiane jest szerzej jako ogół agresywnych internetowych komentarzy, które przekraczają granice kultury wypowiedzi (Włodarczyk, 2014). Z kolei mowa nienawiści (ang. *hate speech*) ma węższe i ściślej ustalone znaczenie. Według najczęściej cytowanej definicji zawartej w dokumencie Komitetu Ministrów Rady Europy za mowę nienawiści uważa się „wszelkie formy wypowiedzi, które szerzą, propagują czy usprawiedliwiają nienawiść rasową, ksenofobię, antysemityzm oraz inne formy nienawiści bazujące na nietolerancji" (Rada Europy, 1997). Mowa nienawiści jest zatem skierowana przede wszystkim przeciwko grupom mniejszościowym.

Charakterystyka

Do podstawowych form cyberprzemocy zalicza się: wyzywanie, nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie w internecie kompromitujących informacji, zdjęć, filmów, podszywanie się w cyberprzestrzeni pod kogoś wbrew jego woli, a także wykluczanie z grupy rówieśniczej online (np. poprzez usunięcie kogoś z grona znajomych na portalu społecznościowym). Rozwój internetu oraz nieograniczona inwencja młodych ludzi powodują, że trudno wskazać wszystkie formy składające się na cyberprzemoc.

Badania prowadzone wśród młodzieży pokazują, że formy przemocy rówieśniczej w sieci i poza nią są ze sobą silnie powiązane. W zdecydowanej większości przypadków poszkodowane osoby – ofiary cyberprzemocy – doświadczają także nękania poza internetem (Pyżalski, 2012). Dlatego trzeba sobie uzmysłowić, że nie można zastanawiać się nad rozwiązaniem problemu cyberprzemocy w oderwaniu od zagadnienia przemocy rówieśniczej także w życiu realnym.

Jednocześnie cyberprzemoc ma swoją specyfikę związaną z komunikacją za pośrednictwem sieci. Po pierwsze, krzywdzące materiały mogą rozprzestrzeniać się w internecie z dużą szybkością, mając większy zasięg niż jakiekolwiek formy przemocy tradycyjnej. W najgorszych przypadkach treści prześmiewcze i/lub kompromitujące daną osobę mogą stać się wiralami (filmami, które w bardzo krótkim czasie docierają do wielu osób, stając się hitami sieci). Po drugie, zamieszczanie różnych treści w cyberprzestrzeni wywołuje u rozpowszechniających je osób mniejsze opory (tzw. zjawisko rozhamowania). Sprawcy, nie mając bezpośredniej informacji zwrotnej na temat potencjalnej reakcji ofiary, działają bez zahamowań lub w ogóle nie odbierają swojego zachowania jako formy krzywdzenia drugiego człowieka (Barlińska, Małecka, Świątkowska, 2018).

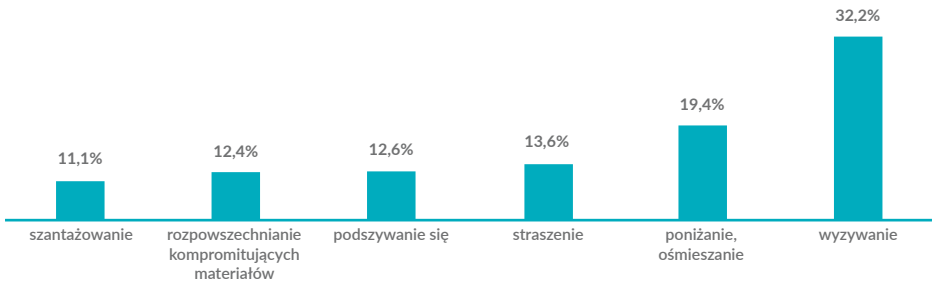
Ofiary cyberprzemocy mogą doświadczać negatywnych skutków oddziałujących na ich zdrowie psychiczne, mają wyższe ryzyko depresji, większą podatność na uzależnienie od alkoholu i/lub narkotyków, częściej doświadczają problemów z nauką, wreszcie mogą pojawić się u nich myśli lub próby samobójcze (United Nations Children's Fund, 2017).

Skala zjawiska

Istnieją spore rozbieżności w badaniach dotyczących przemocy w sieci. Skala zjawiska w dużym stopniu zależy od tego, jakie formy agresji zostały uwzględnione w danym badaniu, a także od tego, czy chodzi o jednorazowe akty, czy długotrwałe nękanie. W obszernych badaniach z 2010 r., które przeprowadzono na uczniach gimnazjum, wykazano, że do najczęstszych form agresji elektronicznej zalicza się: wyzywanie na czacie (doświadczyło go 44 proc. respondentów) lub w trakcie gry online (potwierdza je 37 proc. młodych ludzi). Ankietowani wskazali, że stali się ofiarami także innych przejawów cyberprzemocy, wśród których należy wymienić: nieprzyjemne komentarze na forum (38 proc.) lub na portalu społecznościowym (28 proc.). Przywołane przykłady są najprostszymi formami agresji elektronicznej, możliwej do zastosowania przez sprawców w sposób spontaniczny. Stosunkowo najrzadziej respondenci doświadczali następujących objawów cyberprzemocy: rozpowszechnianie w sieci niechcianego zdjęcia (12 proc.), kradzież prywatnych wiadomości (12 proc.), zakładanie fałszywego profilu (16 proc.) czy stworzenie obraźliwej strony internetowej (6 proc.) (Pyżalski, 2012).

Zbliżone wyniki uzyskano w badaniach *Nastolatki 3.0* NASK oraz Fundacji Pedagogium, które przeprowadzono w 2016 r. Respondentom zadano sześć pytań dotyczących różnych negatywnych doświadczeń online (wykres poniżej). Wyzywania kiedykolwiek doświadczyła niemal jedna trzecia badanych nastolatków (32,2 proc.). Poniżana lub ośmieszana w sieci była co piąta z ankietowanych osób (19,4 proc.). Co dziewiąty respondent (11,1 proc.) był szantażowany, a 12,4 proc. młodych ludzi przyznało, że rozpowszechniano w sieci kompromitujące ich materiały (NASK, 2016).

Wykres. Doświadczenia cyberprzemocy wśród polskich nastolatków w 2016 r.



Źródło: opracowanie własne na podstawie: NASK (2016)

W 2013 r. pytanie o cyberprzemoc włączono także po raz pierwszy do cyklicznego badania *Młodzież 2013* prowadzonego przez Centrum Badania Opinii Społecznej i Krajowe Biuro do Spraw Przeciwdziałania Narkomanii. Co ciekawe, w analizie tej ograniczono definicję przemocy elektronicznej do zamieszczania w internecie zdjęć lub filmów kompromitujących kolegów, koleżanki lub nauczycieli. Respondentów ze szkół ponadgimnazjalnych pytano o to, jak często doświadczają w szkole przemocy rówieśniczej. Odpowiedzi nastolatków były następujące: 5 proc. badanych – często, 25 proc. młodzieży – rzadko, a 71 proc. respondentów wyznało, że nigdy nie doświadczyło żadnych przejawów agresji elektronicznej. W przeciwieństwie do innych form przemocy i negatywnych zjawisk objętych badaniem poziom cyberprzemocy był taki sam w liceach, technikach i szkołach zawodowych. W przywołanych placówkach edukacyjnych okazało się, że przejawy agresji rówieśniczej występują niezależnie od środowiska społecznego młodzieży (Centrum Badania Opinii Społecznej, 2014).

W ostatnich latach zainicjowano wiele międzynarodowych projektów badawczych mających na celu pomiar skali zjawiska przemocy rówieśniczej online. Jednak ze względu na odmienność metodologii trudno jest porównywać wyniki dla różnych krajów. Począwszy od edycji 2013/2014, tematykę cyberprzemocy włączono do międzynarodowego badania Światowej Organizacji Zdrowia (WHO) – *Health Behaviour in School-aged Children* (HBSC), w którym już wcześniej znajdowały się wyniki dotyczące rówieśniczej przemocy fizycznej. W przywołanej analizie zdefiniowano cyberprzemoc jako wysyłanie – dwa, trzy razy w miesiącu lub częściej – obraźliwych wiadomości i/lub publikację obraźliwych treści na czyjś temat. W Polsce zjawisko to dotyczyło 5 proc. dziewcząt i 4 proc. chłopców. Był

to stosunkowo wysoki wynik (9. miejsce na 37 badanych państw). W analizie HBSC badano także dzieci w wieku 11 i 15 lat. Zarówno w przypadku młodszych, jak i starszych respondentów odsetek ofiar cyberprzemocy był niższy (3 proc. – młodsi i starsi chłopcy oraz młodsze dziewczęta, a 2 proc. – starsze dziewczęta) (HBSC, 2016).

Dostępne dane nie pozwalają na określenie trendów dotyczących skali występowania cyberprzemocy w Polsce. Dlatego uwzględnienie tego zjawiska w kilku dużych badaniach cyklicznych – np. *Młodzież 2013* (CBOS) czy *Health Behaviour in School-aged Children* (WHO) – umożliwi przygotowanie potrzebnego zestawienia w przyszłości. Raport Najwyżej Izby Kontroli z 2014 r., który dotyczył zjawisk patologicznych w polskich szkołach, wskazuje cyberprzemoc jako jedno z dwóch (obok dopalaczy) głównych zagrożeń nasilających się w ostatnich latach. Jednocześnie raport ten ukazuje słabość działań profilaktycznych w większości kontrolowanych placówek (Najwyższa Izba Kontroli, 2014).

Przywołane raporty zwracają także uwagę na wysoki odsetek polskiej młodzieży powiązanej – jako sprawcy bądź ofiary – z hejtem i mową nienawiści. Według badań organizacji Global Diginity z 2016 r. hejtu (definiowanego jako obraźliwe wpisy na temat innej osoby) doświadczyło 43 proc. internautów w wieku od 12 do 24 lat. Z przywołanej analizy wynika, że do hejtowania przyznało się 20 proc. młodych osób (Global Dignity, 2016).

Jeszcze bardziej niepokojące dane dotyczą kontaktu młodzieży ze zjawiskiem mowy nienawiści w internecie. Warto zwrócić uwagę na to, że w 2014 r. blisko połowa respondentów w wieku 16–18 lat natrafiła w sieci na treści wymierzone w mniejszości narodowe. Natomiast w analizie przeprowadzonej w 2016 r. 75 proc. młodzieży zadeklarowało, że w sieci miało do czynienia z wypowiedziami antysemickimi, 80 proc. badanych natrafiło na treści islamofobiczne, a 71 proc. respondentów – antyukraińskie. Trzeba sobie także uświadomić, że jednocześnie aż połowa młodych ludzi przyznaje się do stosowania w internecie mowy nienawiści. I co ciekawe, w starszych grupach wiekowych ten odsetek jest znacznie wyższy (Winiewski i in., 2017).

Prawo

W przepisach prawnych nie funkcjonuje odrębne pojęcie cyberprzemocy, jednak poszczególne jej formy mogą stanowić czyn niedozwolony w świetle prawa karnego i cywilnego. Część aktów agresji w internecie traktuje się w odniesieniu do Kodeksu karnego jako przestępstwa. Można do nich zaliczyć: znieważanie

(art. 216 k.k.), zniesławienie (art. 212 k.k.), włamanie informatyczne (art. 267 i 268a k.k.), groźby (art. 190 i 191 k.k.), nękanie – stalking (art. 190a k.k.). Niektóre z przywołanych zjawisk są karane z urzędu (jako tzw. przestępstwa publicznoskargowe), a inne – dopiero na wniosek pokrzywdzonego (przestępstwa prywatnoskargowe). Istnieją sytuacje, które nie mają znamion przestępstwa, choć ktoś upubliczniał wizerunek drugiej osoby bez jej wiedzy i zgody. Wówczas można dochodzić swoich praw, wykorzystując przepisy Kodeksu cywilnego (czyli wstępując na drogę roszczeń odszkodowawczych). Zastosowanie mogą mieć wtedy art. 23 i 24 k.c., które dotyczą naruszenia wizerunku, chronionego jako część tzw. dóbr osobistych każdego człowieka. Jeśli mamy do czynienia z wypowiedziami i publikacjami o charakterze mowy nienawiści, wówczas zastosowanie mogą mieć także art. 256 i 257 k.k.:

- „Art. 256. § 1. 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.
- 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".

Choć istnieje wiele możliwości prawnego ścigania cyberprzemocy i agresji w internecie, w praktyce nie jest to łatwe, a często wręcz niemożliwe do zastosowania. W przypadkach, w których sprawca był anonimowy, organy śledcze często umarzają postępowanie. Z kolei rozprawy cywilne mogą być czasochłonne i wiązać się z wysokimi kosztami (Podlewska, Sobierajska, 2009). Nie ma wątpliwości, że kwestii cyberprzemocy nie da się rozwiązać, odwołując się wyłącznie do prawa i wymiaru sprawiedliwości. Problem agresji w sieci wymaga kompleksowych rozwiązań profilaktycznych i interwencyjnych, które przede wszystkim będą bazować na wiedzy psychologiczno-pedagogicznej.

Przeciwdziałanie

Przeciwdziałanie zjawisku cyberprzemocy wymaga wspólnego stanowiska wielu podmiotów, zarówno rodziców/opiekunów prawnych, jak i nauczycieli. Wszystkie te osoby powinny podejmować działania profilaktyczne oraz szybko interweniować w sytuacji podejrzenia, że dziecko jest ofiarą lub sprawcą przemocy w sieci.

Ważną rolę w zwalczaniu agresji w cyberprzestrzeni pełnią rówieśnicy ofiar przestępstwa (tzw. świadkowie). Osoby te obserwują w internecie wiele niepokojących sytuacji, np. obraźliwe i krzywdzące wpisy, publikacje lub komentarze. Trzeba też pamiętać o tym, że świadkowie agresji w sieci niekiedy – w efekcie celowego lub nierozważnego działania, a czasami w poczuciu strachu przed odrzuceniem przez grupę rówieśniczą – sami krzywdzą ofiarę. Dzieje się tak dlatego, że osoby te w wielu przypadkach bardzo naturalnie przechodzą z roli świadka w rolę agresora, komentując w określony sposób kompromitujące materiały, udostępniając je lub w jakiś inny sposób wyrażając aprobatę dla negatywnych treści (np. lajkują w serwisie Facebook).

W szkole/placówce edukacyjnej rozwiązania na rzecz przeciwdziałania cyberprzemocy powinny mieć charakter systemowy (Wojtasik, 2009). Oznacza to konieczność odpowiedniego przygotowania infrastruktury informatycznej poprzez np. filtrowanie treści, wykluczenie anonimowego korzystania ze szkolnych komputerów czy sieci Wi-Fi (Stachecki, 2013). Postuluje się również ustalenie takich zasad korzystania z sieci i telefonów komórkowych, które zapobiegałyby zachowaniom agresji rówieśniczej w internecie. Byłoby dobrze, aby ustalenia te znalazły odzwierciedlenie zarówno w regulaminie szkolnym, jak i precyzyjnych regulacjach dotyczących korzystania z pracowni komputerowej. Edukacja medialna powinna także obejmować treści dotyczące umiejętności ochrony własnej prywatności w cyberprzestrzeni.

Respektowanie przez młodzież podstawowych zasad dotyczących zapewnienia jej bezpieczeństwa w internecie (np. ograniczone zaufanie do innych użytkowników, ochrona danych dostępowych do kont) może znacząco przyczynić się do przeciwdziałania niektórym formom cyberprzemocy. Równie istotne jest stworzenie odpowiedniej strategii, a także opracowanie procedur pozwalających na szybką reakcję, gdy tylko uczniowie danej szkoły/placówki edukacyjnej doświadczą w sieci agresji wymierzonej w nich. Opracowane przepisy muszą precyzyjnie określać, jak należy postępować wobec sprawców, ofiar i świadków zdarzeń (Borkowska, Macander, 2009). Przyjęcie przez placówkę odpowiednich procedur zapobiega sytuacji, w której brak reakcji czy interwencji ze strony nauczycieli wynika z ich niewiedzy wobec konkretnych metod postępowania. Niezbędnym elementem systemu zapobiegania i reagowania na takie zachowania w szkole/placówce edukacyjnej jest prowadzenie profilaktycznych zajęć edukacyjnych dla dzieci i młodzieży, a także systematyczne podnoszenie kompetencji pracowników w zakresie tej wielopłaszczyznowej problematyki.

Ważne, aby osoby, które doświadczyły lub doświadczają przemocy w sieci, wiedziały, gdzie otrzymają pomoc. Młodzi ludzie mogą skorzystać z telefonu zaufania dla dzieci i młodzieży 116 111, a ich rodzice/opiekunowie prawni oraz nauczyciele, spotykający się z tym problemem, mają do dyspozycji telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci 800 100 100.

Pamiętaj!

- Rozmawiaj z dzieckiem na temat przemocy w sieci, hejtu i mowy nienawiści. Ustalcie wspólnie, w jaki sposób można reagować na te zjawiska. Zapewnij dziecko o swoim wsparciu, jeśli doświadczy takiej sytuacji.
- Jako rodzic/opiekun prawny nigdy nie bagatelizuj sytuacji, w której twoje dziecko jest ofiarą przemocy w sieci. Reaguj natychmiast i działaj we współpracy ze szkołą/placówką edukacyjną. Wspólnie zabezpieczcie dowody (np. wykonując zrzuty ekranów).
- Rozmawiaj z dzieckiem o tym, jak może reagować jako świadek cyberprzemocy. Poinformuj dziecko, w jaki sposób może pomóc ofierze agresji w sieci, jednocześnie nie narażając się samemu na przemoc.
- Dowiedz się, czy w szkole/placówce edukacyjnej, do której uczęszcza twoje dziecko, istnieją spisane procedury działania w przypadku wykrycia cyberprzemocy, a także czy są realizowane zajęcia profilaktyczne na ten temat.
- Rozmawiaj z dzieckiem o tym, co może być uznane za mowę nienawiści i dlaczego jest ona szkodliwa.
- Zgłaszaj do administratorów i do zespołu Dyżurnet.pl strony zawierające mowę nienawiści.
- Poinformuj dziecko o tym, gdzie może uzyskać pomoc – telefon zaufania dla dzieci i młodzieży 116 111.
- W razie pytań i wątpliwości zadzwoń pod numer 800 100 100 – telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci.

Bibliografia

1. Barlińska J., Małecka A., Świątkowska J., (2018), *Cyberbezpieczeństwo. Charakterystyka, mechanizmy i strategie zaradcze w makro i mikro skali.* Monografia, Warszawa: Texter.
2. Borkowska A., Macander D., (2009), *System reagowania w szkole na ujawnienie cyberprzemocy*, w: *Jak reagować na cyberprzemoc? Poradnik dla szkół*, wydanie II (poprawione), Wojtasik Ł. (red.), Warszawa: Fundacja Dzieci Niczyje, s. 12–22, zob. bit.ly/sysuprz (dostęp: 02.01.2019).
3. Centrum Badania Opinii Społecznej (CBOS), (2014), *Młodzież 2013. Raport z badań.* Warszawa: CBOS i KBPN.
4. Global Dignity, (2016), *Wilki i owce w internecie, czyli raport na temat hejtu wśród młodzieży*, Warszawa: IQS, Global Dignity, zob. http://bit.ly/raphejt (dostęp: 02.01.2019).
5. *Health Behaviour in School-aged Children (HBSC)*, (2016), *Growing up unequal: gender and socioeconomic differences in young people's health and well-being. Health Behaviour in School-aged Children Study: international report from the 2013/2014 survey*, Genewa: World Health Organisation, zob. bit.ly/grupueq (dostęp: 02.01.2019).
6. Hinduja S., Patchin J.W., (2018), *Cyberbullying identification: Prevention, and response*, Cyberbullying Research Center (cyberbullying.org), tłumaczenie własne, zob. bit.ly/cybulin (dostęp: 02.01.2019).
7. Konopczyński M., Lange, R., Osiecki J. i inni, (2014), *Ogólnopolskie badanie. Nastolatki wobec internetu.* Raport opracowany na zlecenie Rzecznika Praw Dziecka i NASK przez Pedagogium WSNS w okresie maj – czerwiec 2014, Warszawa: NASK – Państwowy Instytut Badawczy, zob. bit.ly/naswint (dostęp: 02.01.2019).
8. Naukowa i Akademicka Sieć Komputerowa (NASK), (2016), *Nastolatki 3.0. Wybrane wyniki ogólnopolskiego badania uczniów w szkołach*, Warszawa: NASK – Państwowy Instytut Badawczy, zob. bit.ly/wynnas3 (dostęp: 02.01.2019).
9. Najwyższa Izba Kontroli (NIK), (2014), *Przeciwdziałanie zjawiskom patologii wśród młodzieży szkolnej. Informacje o wynikach kontroli*, Warszawa: NIK, zob. bit.ly/przepat (dostęp: 02.01.2019).
10. Orange Polska, (2016), *Rodzice i dzieci wobec zagrożeń dzieci w internecie.* Raport z badania przygotowany przez TNS Polska S.A. na zlecenie Orange Polska, we współpracy z Fundacją Orange i Fundacją Dajemy Dzieciom Siłę, zob. bit.ly/rdwzagr (dostęp: 02.01.2019).
11. Podlewska J., Sobierajska W., (2009), *Prawna ochrona dzieci przed cyberprzemocą. Analiza przepisów prawnych.* Doświadczenia Helpline.org.pl, w: *Jak reagować na cyberprzemoc? Poradnik dla szkół*, wydanie II (poprawione), Wojtasik Ł. (red.), Warszawa: Fundacja Dzieci Niczyje, s. 45–72, zob. http://bit.ly/sysuprz (dostęp: 02.01.2019).
12. Pyżalski J., (2012), *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Kraków: Oficyna Wydawnicza Impuls.

13. Pyżalski J., (2014), *Elektroniczna agresja rówieśnicza – ustalenia empiryczne ostatniej dekady*, w: *Uzależnienia behawioralne i zachowania problemowe młodzieży. Teoria. Diagnoza. Profilaktyka. Terapia*, Jarczyńska J. (red.), Bydgoszcz: Wydawnictwo UKW, s. 33–47, zob. bit.ly/eagrrow (dostęp: 02.01.2019).
14. Rada Europy, (1997), Rekomendacja R (97) 20 Komitetu Ministrów Rady Europy na temat mowy nienawiści z dnia 30 października 1997.
15. Stachecki D., (2013), *Bezpieczeństwo szkolnej infrastruktury informatycznej*, w: *Szkolne standardy bezpieczeństwa dzieci i młodzieży online. Rekomendacje dla szkół*, Warszawa: Fundacja Dzieci Niczyje, s. 10–13, zob. bit.ly/bezszii (dostęp: 02.01.2019).
16. United Nations Children's Fund, (2017), *The State of the World's Children 2017. Children in a digital world*, Nowy York: UNICEF, zob. bit.ly/childdw (dostęp: 02.01.2019).
17. Ustawa z dnia 23 kwietnia 1964 r., Kodeks cywilny (Dz.U z 1964 r. nr 16, poz. 93).
18. Ustawa z dnia 6 czerwca 1997 r., Kodeks karny (Dz.U. 1997 r. nr 88, poz. 553).
19. Winiewski M., Hansen K., Bilewicz M., Soral W., Świderska A., Bulska D, (2017), *Mowa nienawiści, mowa pogardy. Raport z badania przemocy werbalnej wobec grup mniejszościowych*, Warszawa: Fundacja im. Stefana Batorego, zob. bit.ly/mnienaw (dostęp: 01.02.2019).
20. Włodarczyk J., (2014), *Mowa nienawiści w internecie w doświadczeniu polskiej młodzieży*, w: „Dziecko krzywdzone. Teoria, badania, praktyka", t. 13, nr 2, 122–158, zob. bit.ly/mnienin (dostęp: 02.01.2019).
21. Wojtasik Ł., (2009), *Przemoc rówieśnicza a media elektroniczne*, w: „Dziecko krzywdzone. Teoria, badania, praktyka", t. 8, nr 1, s. 78–89, zob. bit.ly/przerow (dostęp: 02.01.2019).

II.2. Nadużywanie internetu

/Anna Jankiewicz, Agata Kuszner, Anna Maj, Agnieszka Nawarenko/

Technologia cyfrowa sprawiła, że dzięki urządzeniom mobilnym każdy właściciel smartfonu może być stale zalogowany do sieci, mając nieograniczony dostęp do informacji i rozrywki. W sieci dyskutujemy, utrzymujemy relacje z bliższymi i dalszymi znajomymi, robimy zakupy, uczestniczymy w tele- i wideokonferencjach, wyrażamy siebie. Te często atrakcyjne i wartościowe możliwości spędzania czasu mogą jednak pochłaniać go zbyt wiele, sprawiając, że zamiast być dopełnieniem aktywności, zaczynają w naszym życiu dominować. Wielogodzinne angażowanie się w gry online, kompulsywne sprawdzanie mediów społecznościowych, wykorzystywanie każdej okoliczności na podłączenie się do publicznych sieci internetowych – to tylko wybrane przykłady nadmiernego korzystania z sieci. Dlatego tak istotne jest, aby umieć jak najszybciej rozpoznać zaburzenia związane z nadmierną potrzebą bycia online, a także wiedzieć, jak reagować na widoczne oznaki np. uzależnienia od gier komputerowych.

Skala problemu

Wyposażenie urządzeń mobilnych w stały dostęp do sieci umożliwiło młodzieży niemal nieprzerwaną komunikację w czasie rzeczywistym. Badanie przeprowadzone przez Państwowy Instytut Badawczy NASK w 2016 r. – *Nastolatki 3.0* – wykazało, że 93,4 proc. młodzieży w wieku 13–17 lat przez cały czas jest online. Ponad 30 proc. respondentów potwierdziło, że ponad pięć godzin na dobę przegląda internet, wykorzystując do tego celu swój telefon komórkowy. Wiele nastolatków ujawnia symptomy dysfunkcyjnego korzystania z cyberprzestrzeni: 83,2 proc. uczniów deklaruje, że zdarzyło im się przebywać w sieci dłużej, niż planowali. Natomiast 29,8 proc. młodych ludzi twierdzi, że przedkładało korzystanie z sieci ponad obowiązki szkolne. Co piąty ankietowany, 19 proc., przyznaje się do tego, że okłamywał rodziców, aby móc korzystać z internetu. Zdaniem 66,4 proc. respondentów obecność w cyberprzestrzeni jest doskonałym sposobem na poprawienie sobie złego nastroju (Kamieniecki i in., 2017).

Uzależnienie od gier

Angażowanie się w gry komputerowe lub sieciowe może obejmować kilka form aktywności: szybką grę w telefonie (np. podczas podróży komunikacją miejską), granie online wspólnie z kolegami, wielogodzinne, czasami całonocne, sesje. Nie oznacza to jeszcze zaburzenia. Według Światowej Organizacji Zdrowia problem

zaczyna się wtedy, gdy granie ma znaczący wpływ na życie osobiste, rodzinne, społeczne, a także na funkcjonowanie w szkole/placówce edukacyjnej. W nowej wersji Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych – ICD-11 – opublikowanej w 2018 r. wśród zaburzeń psychicznych pojawia się uzależnienie od gier komputerowych (oficjalny termin angielski: *gaming disorder*). Według *ICD-11– cechy*, *możliwości*, *zagrożenia* gra komputerowa staje się zaburzeniem, gdy grający angażuje się w nią przez co najmniej 12 miesięcy, a ponadto są spełnione trzy warunki (Taper, 2011): gracz traci kontrolę nad graniem, granie staje się priorytetem i dominuje nad innymi zainteresowaniami oraz codziennymi czynnościami, gracz kontynuuje granie mimo widocznych negatywnych konsekwencji.

Według badań z 2012 r. (Makaruk, Wójcik, Konsorcjum EU NET ADB, 2012) wśród nastolatków to chłopcy stanowią większą grupę graczy. Aż 52,5 proc. uczniów płci męskiej spędza codziennie czas na intensywnym graniu. Natomiast wśród dziewczynek jedynie 8,3 proc. przyznało, że codziennie gra, wykorzystując do tego celu internet lub urządzenia elektroniczne (Wójcik, 2013). W pracach poświęconych analizie zachowań europejskich nastolatków podczas gry (Müller i in., 2015) zauważono, że problem nadużywania tego rodzaju aktywności dotyczy 2 proc. polskiej młodzieży (Cudo, Kopiś, Strożak, 2016). W porównaniu z rezultatami badań, które opisują uzależnienie się od gier młodzieży z pozostałych krajów europejskich, Polska – z wynikiem 2,5 proc. – plasuje się na drugim miejscu (zaraz po Grecji).

Przyczyny

Przyczyny nadużywania internetu przez dzieci i młodzież są zazwyczaj złożone, często zależne od danej sytuacji życiowej młodego człowieka. Niekiedy jest to reakcja na brak jakiejkolwiek innej aktywności, która w podobny lub bardziej satysfakcjonujący sposób zaspokaja potrzebę przyjemności. Zdarza się, że zatracenie się w świecie gier może wynikać np. z poczucia odrzucenia, braku akceptacji ze strony rodziców/opiekunów i/lub rówieśników albo ma związek z doświadczaną przemocą fizyczną bądź psychiczną. Czasem wybór takiej formy aktywności stanowi dla młodzieży rodzaj ucieczki od rzeczywistości i jest sposobem na radzenie sobie z trudnymi emocjami. Nadużywanie gier przez młodych może być także związane z poczuciem braku satysfakcji życiowej, koniecznością poszukiwania sposobów na poprawienie nastroju, dowartościowania się. Niejednokrotnie taka postawa młodzieży wynika z chęci doświadczenia mocnych wrażeń, wyładowania agresji czy też zaznania poczucia dominacji (Cudo i in., 2017).

Jak poznać, czy dziecko jest uzależnione?

Dzieci i nastolatki, które mają problem z kontrolowaniem czasu online, często prezentują całe spektrum niepokojących objawów, np.: pogorszenie wyników w nauce, chroniczne zmęczenie, nagłe zmiany nastrojów, zachowania lękowe, depresyjne. Bywa też, że tych młodych ludzi wyróżnia zachowanie typowe dla osób uzależnionych od jakiegoś nałogu. Przejawia się to w ten sposób, że dzieci i nastolatki cechuje np.: nadmierne zainteresowanie grami, utrzymywanie kontaktów jedynie z innymi graczami, a tym samym wycofanie się z pozostałych relacji rodzinno-społecznych, agresja podczas próby przerwania im gry, skłonność do kłamstw i ukrywanie przywiązania do gier, irytacja spowodowana brakiem możliwości grania, a także brak zainteresowania innymi aktywnościami (Taper, 2011). Bardzo niepokojącym przejawem chorobliwej fascynacji światem gier jest oddawanie się tej aktywności kosztem nocnego odpoczynku/snu. Poniższe symptomy mogą towarzyszyć również innym dysfunkcjom użytkowania sieci, w tym nadmiernemu korzystaniu z portali społecznościowych:

- silne pragnienie/poczucie przymusu korzystania z mediów cyfrowych,
- utrata kontroli nad zachowaniem,
- objawy stanu abstynencyjnego, pojawiające się w momencie przerwania aktywności – drażliwość, złość, wściekłość, zalewający smutek, agresja,
- konieczność zwiększenia ilości czasu spędzanego w sieci,
- utrata zainteresowania innymi aktywnościami,
- zaniedbywanie podstawowych obowiązków domowych czy szkolnych,
- uporczywe kontynuowanie zachowania pomimo negatywnych konsekwencji (np. ciągłego zwracania uwagi przez rodziców, kłótni z tego powodu czy pogorszenia wyników w nauce).

Regularne obserwowanie dziecka jest ważne dla obiektywnej oceny jego prawidłowego funkcjonowania i rozwoju. Kiedy tylko rodzice lub nauczyciele zaczną podejrzewać, że młody człowiek ma problem z nadużywaniem gier, mogą skorzystać z poniższych przykładowych pytań, próbując sobie na nie odpowiedzieć (Węgrzecka-Giluń, 2012):

1. Czy dziecko staje się nerwowe lub agresywne wówczas, kiedy próbuje mu się ograniczyć czas grania?
2. Czy w przypadku, gdy dziecko przegra, natychmiast zaczyna grę od początku?
3. Czy dziecko kupiło grę za pieniądze przeznaczone na coś innego?
4. Czy zdarzyło się, że dziecko kontynuowało grę kosztem pójścia do szkoły?
5. Czy dziecko w nocy, zamiast pójść spać, angażowało się w gry? Czy było to zdarzenie jednorazowe, czy cykliczne?

Odpowiedzi twierdzące mogą pomóc rodzicom ocenić prawdopodobieństwo uzależnienia jego dziecka od gier.

FOMO – co to takiego?

FOMO (skrót od angielskiego wyrażenia *fear of missing out*) definiuje się jako uczucie lęku lub niepokoju przed wykluczeniem z jakiejś społeczności lub pominięciem. To „wszechogarniające obawy, że inni mogą właśnie przeżywać bardziej satysfakcjonujące doświadczenia, z których przez nieobecność jest się wykluczonym" (Przybylski, Murayama, DeHaan, 2013). Mimo że samo pojęcie FOMO po raz pierwszy zostało użyte przez dr. Dana Hermana już w 1996 r., to jednak dopiero od momentu pojawienia się mediów społecznościowych można mówić o wzroście zainteresowania tym zagadnieniem. Na odczucia związane z FOMO jesteśmy narażeni szczególnie w obecnych czasach, kiedy każdy, dzięki smartfonom, może być stale online, a media społecznościowe spełniają naszą ogólnoludzką potrzebę przynależności do grupy, bycia na czasie. Facebook, Twitter, Instagram dają możliwość śledzenia, „lajkowania" i komentowania na bieżąco. Tym samym ludziom może się wydawać, że nawet chwilowe wyłączenie się z aktywności medialnej spowoduje ich wykluczenie z życia społecznego lub pominięcie. Wielu badaczy uznaje FOMO za swego rodzaju chorobę cywilizacyjną, na którą narażeni są wszyscy użytkownicy mediów (bez względu na wiek).

W 2018 r. naukowcy z Uniwersytetu Warszawskiego pod kierownictwem dr Anny Jupowicz-Ginalskiej przeprowadzili badania na reprezentatywnej grupie, którą tworzyły osoby powyżej 15. roku życia. Wyniki analiz są alarmujące, ponieważ zespół wysokiego FOMO (tzw. *high FOMO*, czyli osoby o najwyższym wskaźniku FOMO według skali Andrew K. Przybylskiego) dotyczy aż 16 proc. polskich internautów. Natomiast w przypadku najmłodszych użytkowników sieci (w wieku od 15 do 24 lat) wskaźnik FOMO wynosi aż 21 proc. (Jupowicz-Ginalska, Jasiewicz, Kisilowska, 2018).

Warto sobie uzmysłowić, że istnieją takie osoby jak fomersi. Ludzie ci niemal każdą planowaną aktywność (np. zakupy, wyjazd wakacyjny, uroczystość rodzinną, przygotowany posiłek) rozpatrują pod kątem tego, w jaki sposób można ją przedstawić w mediach społecznościowych. Statystyki dowodzą, że 49 proc. badanych z wysokim FOMO sięga po telefon zaraz po przebudzeniu, 38 proc. respondentów korzysta z urządzeń ekranowych podczas posiłku, a 60 proc. zerka na nie jeszcze tuż przed zaśnięciem.

Nadużywanie czy uzależnienie?

Ciągłe zaglądanie do telefonu lub innego urządzenia może dawać jego właścicielowi złudne poczucie bezpieczeństwa i panowania nad swoim życiem. W rzeczywistości jednak prowadzi do ryzykownych cyfrowych nawyków, np. ciągłego, wręcz kompulsywnego sprawdzania e-maili, powiadomień z serwisów społecznościowych. A to z kolei może powodować negatywne konsekwencje w budowaniu choćby relacji rodzinno-społecznych poza siecią.

Godne zauważenia jest to, że 36 proc. badanych osób z grupy wysokiego FOMO ma świadomość uzależnienia się od mediów społecznościowych. Połowa ankietowanych potwierdza, że korzysta z serwisów społecznościowych znacznie dłużej, niż zaplanowali. Osoby, które mają problem z określeniem właściwych proporcji w dostępie do sieci, pozostają online nie tylko podczas ważnych spotkań z bliskimi czy przyjaciółmi (32 proc.), ale także w sytuacjach, kiedy jest to społecznie zakazane, np. podczas nabożeństwa w kościele (20 proc.), wykładu na uczelni lub w czasie lekcji (37 proc.). Zatrważające jest też to, że internauci z grupy wysokiego FOMO, ulegając presji aktywności w sieci, ignorują własne bezpieczeństwo w momencie przechodzenia przez pasy (29 proc.) czy w trakcie prowadzenia samochodu (25 proc.).

Rys. 1. FOMO – grupa wysokiego ryzyka

Osoby z wysokim wskaźnikiem FOMO charakteryzują się często niższą samooceną w porównaniu z przeciętnymi internautami. Wynika to z faktu, że w mediach społecznościowych niemal każdy kreuje własny wizerunek, prezentując lepszą wersję siebie (np. dzięki selfie w wystudiowanej pozie z odpowiednią mimiką, prezentacji zdjęcia z egzotycznych wakacji). Internauci z wysokim FOMO są przekonani, że inni ludzie żyją lepiej, ciekawiej, pełniej. Niestety takie ciągłe porównywanie się z pozostałymi użytkownikami sieci może prowadzić do poczucia, że jest się gorszym (33 proc.) i bezużytecznym (33 proc.).

Innym niepokojącym efektem FOMO jest brak chęci do podejmowania nowych wyzwań. Jak wynika z sondażu przeprowadzonego w USA i Wielkiej Brytanii (Thompson, 2012), ponad połowa badanych w wieku od 18 do 34 lat stwierdziła, że nie jest w stanie poświęcić więcej czasu i energii na zgłębianie innych swoich pasji (poza aktywnością w sieci) lub poznawanie nowych treści. Uzależnienie od bycia stale online może wzbudzać niepokój w momencie odłączenia dostępu do sieci (np. wskutek zerwania połączenia internetowego, przebywania w jakimś miejscu/sytuacji bez telefonu), ale także wywoływać objawy psychosomatyczne (np. syndrom fantomowych wibracji czy też – charakterystyczne dla okresu abstynencji od różnych używek – zawroty głowy, bóle brzucha, nudności).

FOMO jest kolejnym zagrożeniem wynikającym z uzależnienia się od internetu, a w szczególności od mediów społecznościowych. Wpływa również negatywnie na ogólną kondycję psychofizyczną i funkcjonowanie zarówno dorosłych, młodzieży, jak i dzieci w świecie.

Pamiętaj!

- Ustal czas przeznaczony na aktywności w internecie. Obserwuj dziecko i zwróć szczególną uwagę na niepokojące zachowania (np. nadmierną agresję, odizolowanie, nadwrażliwość, utratę zainteresowania innymi aktywnościami).
- Rozmawiaj z dzieckiem. Zasygnalizuj mu, że się o nie martwisz, spróbuj wytłumaczyć swoje obawy.
- Spróbuj dowiedzieć się, co jest powodem uzależnienia twojego dziecka od internetu, a także w jakich sytuacjach korzysta ono intensywniej z sieci.
- Spróbuj stopniowo ograniczać dziecku czas spędzony na korzystaniu z internetu. Dbaj o to, aby nagradzać dziecko za każdy postęp.
- Postaraj się wspólnie z dzieckiem znaleźć pomost między czasem spędzanym w świecie wirtualnym a rzeczywistym. Angażuj je w ten sposób, aby bycie offline przynosiło mu radość, tzw. JOMO (ang. *joy of missing out*). Zaproponuj offline challenge (cyfrowy detoks), który polega na odłączeniu się od wirtualnej rzeczywistości na minimum 48 godzin.
- Pamiętaj, że swoją postawą wobec mediów cyfrowych wpływasz na zachowanie swoich dzieci w tym obszarze. Jesteś dla nich przykładem.

- Skontaktuj się z psychologiem lub poradź się innego specjalisty, jeśli samodzielnie nie będziesz w stanie poradzić sobie z problemem.
- W razie pytań i wątpliwości zadzwoń pod numer 800 100 100 – telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci.

Bibliografia

1. Cudo A., Dobosz M., Basaj Ł., (2017), *Nałogowe korzystanie z gier komputerowych a funkcjonowanie interpersonalne i intrapersonalne młodzieży.* Badania pilotażowe, w: „Rozprawy Społeczne", nr 11 (1), s. 40–49.
2. Cudo A., Kopiś N., Strożak P., (2016), *Problematyczne używanie Internetu oraz problematyczne korzystanie z gier komputerowych wśród studentów kierunków społecznych i humanistycznych*, w: „Hygeia Public Health", nr 51 (4), s. 389–397.
3. Ferrari A., (2016), DIGCOMP: *Ramy odniesienia dla rozwoju i rozumienia kompetencji cyfrowych w Europie*, tłum. Urban K., Lublin: Wydawnictwo Fundacji ECCC, zob. http://www.academia.edu/23203045/DIGCOMP_Ramy_odniesienia_dla_rozwoju_i_rozumienia_kompetencji_cyfrowych_w_Europie (dostęp: 02.01.2019).
4. Jupowicz-Ginalska A., Jasiewicz J., Kisilowska M., Baran T., Wysocki A., (2018), *FOMO. Polacy a lęk przed odłączeniem – raport z badań*, Warszawa, zob. https://www.wdib.uw.edu.pl/attachments/article/1992/FOMO.%20Polacy%20a%20lęk%20przed%20odłączeniem%20-%20raport%20z%20badań.pdf (dostęp: 02.01.2019).
5. Kamieniecki W., Bochenek M., Tanaś M., Wrońska A., Lange R., Fila M., Loba B., Konopczyński F., (2017), *Raport z badania. Nastolatki 3.0*, Warszawa: NASK – Państwowy Instytut Badawczy, zob. https://akademia.nask.pl/publikacje/Raport_z_badania_Nastolatki_3_0.pdf (dostęp: 02.01.2019).
6. Makaruk K., Wójcik Sz., Konsorcjum *EU NET ADB, (2012), EU NET ADB. Badanie nadużywania internetu przez młodzież w Polsce*, Warszawa: Fundacja Dzieci Niczyje, zob. https://www.saferinternet.pl/pliki/publikacje/raport-eu-net-adb-pl-final.pdf (dostęp: 02.01.2018).
7. Międzynarodowa Statystyczna Klasyfikacja Chorób i Problemów Zdrowotnych ICD-11, https://icd.who.int/browse11/l-m/en#/http%3a%2f%2fid.who.int%2ficd%2fentity%2f1448597234 (dostęp z dnia 30.01.2019).
8. Müller K.W., Janikian M., Dreier M., Wölfling K., Beutel M.E, Tzavara C., Richardson C., Tsitsika A., (2015), *Regular gaming behavior and internet gaming disorder in European adolescents: results from a cross-national representative survey of prevalence, predictors, and psychopathological correlates*, w: „European Child and Adolescent Psychiatry", nr 24 (5), s. 565–574.

9. Przybylski A.K., Murayama K., DeHaan C.R., Gladwell V., (2013), *Motivational, emotional, and behavioral correlates of fear of missing out*, w: „Computers in Human Behavior", nr 29 (4), s. 1841–1848.
10. Taper A.E., (2011), *Gry MMORPG – cechy, możliwości, zagrożenia*, w: „Media i społeczeństwo. Medioznawstwo, komunikologia, semiologia, socjologia mediów", nr 1, s. 180–193, zob. http://www.mediaispoleczenstwo.ath.bielsko.pl/art/180_taper.pdf (dostęp: 02.01.2019).
11. Thompson J.W., (2012), *Fear of Missing Out (FOMO)*, Nowy York, zob. https://web.archive.org/web/20150626125816/http://www.jwtintelligence.com/wp-content/uploads/2012/03/F_JWT_FOMO-update_3.21.12.pdf (dostęp: 02.01.2019).
12. Węgrzecka-Giluń J., (2012), *Patologiczny hazard i Internet. Przewodnik dla Rodziców. Uzależnienia behawioralne*, Warszawa: Fundacja ETOH.
13. Wójcik S., (2013), *Gry online – korzystanie i nadużywanie wśród młodzieży. Wyniki badania EU NET ADB*, w: „Dziecko krzywdzone. Teoria, badania", t. 12, nr 1, s. 81–98, zob. http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-1fce3204-eb50–4e4d-83e7-debaad7a4ed0/c/Wojcik_S_2013_Gry_online_korzystanie_i_naduzywanie.pdf (dostęp: 02.01.2019).

II.3. Niebezpieczne treści

/Anna Borkowska, Oliwia Chojnacka, Anna Kwaśnik, Michał Marańda
Zuzanna Polak, Martyna Różycka, Marta Witkowska, Szymon Wójcik/

Dzieci korzystające z internetu mogą uzyskiwać dostęp do niebezpiecznych treści takich jak pornografia lub materiały przesycone przemocą i nienawiścią. W opinii samych dzieci jest to najpowszechniejsze i najbardziej dotkliwe zagrożenie. Ich zdaniem głównym źródłem internetowych zagrożeń są przede wszystkim serwisy wideo, w których pojawiają się treści pornograficzne i przemoc (Livingstone, Kirwil, Ponte, 2013).

W niniejszym rozdziale omówiono najważniejsze kategorie szkodliwych treści internetowych, ich charakterystykę i wpływ na młodych użytkowników oraz przedstawiono narzędzia pomocne w kontroli rodzicielskiej, które mogą zapobiegać styczności dzieci z materiałami i treściami postrzeganymi jako szkodliwe dla ich rozwoju poznawczego oraz emocjonalnego.

Niebezpieczne treści w internecie to materiały, które mogą wywołać negatywne emocje u odbiorcy lub promują niebezpieczne zachowania (Polak, Różycka, Marańda, 2014). Zalicza się do nich przede wszystkim:

- treści pornograficzne dostępne bez żadnego ostrzeżenia, w tym materiały prezentujące seksualne wykorzystywanie dzieci;
- treści obrazujące przemoc, obrażenia fizyczne, deformacje ciała, np. zdjęcia lub filmy przedstawiające ofiary wypadków, okrucieństwo wobec zwierząt;
- treści nawołujące do samookaleczeń lub samobójstw, bądź zachowań szkodliwych dla zdrowia, np. ruch promujący anoreksję (pro-ana), zachęcanie do zażywania niebezpiecznych substancji, np. leków czy narkotyków;
- treści dyskryminacyjne, nawołujące do wrogości, a nawet nienawiści wobec różnych grup społecznych lub jednostek[1].

W przypadku dzieci wszystkie te materiały mogą wpływać negatywnie na ich rozwój emocjonalny, poznawczy i społeczny (por. Villani, 2001; Livingstone, Smith, 2014; Valkenburg, Peter, Walther, 2016). Kontakt z treściami szkodliwymi, których młody człowiek nie potrafi odpowiednio zinterpretować i którym bezgranicznie wierzy, może prowadzić u niego do trwałego pogorszenia nastroju, obniżenia poczucia bezpieczeństwa, a w efekcie do wypaczenia obrazu rzeczywistości.

[1] Więcej o treściach dyskryminacyjnych w rozdziale poświęconym cyberprzemocy i mowie nienawiści.

Jeśli chodzi o przemoc, w badaniach wykazano (Aronson, Wilson, Akert, 1997), że kontakt z agresją w mediach powoduje długotrwałe konsekwencje w psychice młodych ludzi. Przypuszcza się, że z jednej strony wzmacnia chęć wyrażania zachowań przemocowych, a z drugiej znieczula na losy ofiar przemocy. Natomiast treści pornograficzne prezentują często nieprawdziwe, a czasem wręcz szkodliwe zachowania i wzorce seksualne, co może wpływać na rozwój psychoseksualny młodego człowieka. Pornografia, również ta, która ukazuje dziecko w kontekstach seksualnych, może być elementem procesu uwodzenia przez osobę o skłonnościach pedofilskich. Ma na celu oswojenie dziecka ze sferą seksu i zachęcenie do własnej aktywności. Jeżeli chodzi o materiały propagujące niebezpieczne zachowania, należy zwrócić uwagę na to, że kontakt z tego typu treściami może wzmocnić typową dla okresu dojrzewania chęć eksperymentowania. Dzieci i nastolatki mogą dowiedzieć się, w jaki sposób używać leków czy innych łatwo dostępnych substancji w celach odurzających, zostać zachęcone do samookaleczeń czy przejścia na wyniszczającą organizm dietę.

Według wyników najnowszej edycji badań *EU Kids Online* (Pyżalski, Zdrodowska, Tomczyk, 2019) tylko 28 proc. polskich 9–17-latków jednoznacznie zadeklarowało, że nie miało kontaktu z niebezpiecznymi treściami. Aż 43 proc. miało do czynienia z brutalnymi obrazami, a 37 proc. z treściami na temat tego, jak popełnić samobójstwo. Co trzeci polski nastolatek zetknął się w ciągu roku poprzedzającego badanie z mową nienawiści. Z kolei badania Fundacji Dajemy Dzieciom Siłę pokazują, że z pornografią w internecie ma kontakt średnio 43 proc. dzieci w wieku 11–17 lat (Makaruk, Włodarczyk, Michalski, 2017). Badania ilościowe prowadzone na reprezentatywnych próbach dowodzą więc, że kontakt z niebezpiecznymi treściami jest jednym z najpowszechniejszych zagrożeń, na jakie mogą natrafić młodzi ludzie w internecie.

Treści niebezpieczne to szeroki termin obejmujący różnego rodzaju materiały o potencjalnie szkodliwym wpływie na dzieci i młodzież. Stopień szkodliwości zależy nie tylko od samych treści (filmów, obrazów), ale także od tego, w jakim wieku jest odbiorca. Niektóre mogą być akceptowalne dla użytkowników dorosłych, a stanowić niebezpieczeństwo dla dzieci. Większość z nich nie jest też zabroniona prawnie. Istnieje jednak kategoria treści nielegalnych, których rozpowszechnianie w sieci jest karalne.

Treści nielegalne

Mianem treści nielegalnych określa się materiały naruszające przepisy prawa. Zastosowanie ma tu zarówno prawodawstwo polskie, jak i Unii Europejskiej, a także umowy międzynarodowe.

W Polsce zakres treści nielegalnych regulują poszczególne ustawy, przede wszystkim Kodeks karny. Komisja Europejska w 2018 r. wydała szczegółowe zalecenia odnośnie do zwalczania takich materiałów w sieci. Według zawartej tam definicji nielegalne treści to wszelkie informacje, które nie są zgodne z prawem Unii Europejskiej lub prawem państwa członkowskiego. Komisja zakreśliła główne obszary tematyczne treści, które uznaje za nielegalne (Zalecenie Komisji (UE) 2018/334):

A. Treści terrorystyczne, czyli wszelkie materiały nawołujące do terroryzmu lub promujące terroryzm. To również treści stworzone przez organizacje terrorystyczne, które wymieniono w wykazach Unii Europejskiej lub Organizacji Narodów Zjednoczonych, albo treści, które można takim grupom przypisać.

B. Materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych, czyli:

- wszelkie przedstawienia organów płciowych dziecka w celach seksualnych;
- nagabywanie dzieci, które nie osiągnęły wieku przyzwolenia, przez osobę dorosłą za pośrednictwem technologii informacyjno-komunikacyjnych do celów seksualnych;
- doprowadzanie/nakłanianie dziecka do udziału w przedstawieniach pornograficznych „na żywo" lub czerpanie z tego korzyści, bądź inne wykorzystywanie osoby małoletniej do lubieżnych celów, a także świadoma obecność na takich pokazach;
- wszelkie czynności związane z produkcją materiałów przedstawiających wykorzystywanie seksualne dzieci (np. produkcja filmów, oferowanie osobom małoletnim angażu w takiej produkcji, dostarczanie lub udostępnianie materiałów, dystrybucja, rozpowszechnianie lub ich przesyłanie, nabywanie lub posiadanie treści i filmów pornograficznych, a także świadome uzyskiwanie dostępu do takiej tematyki za pośrednictwem technologii informacyjno-komunikacyjnych).

C. Nielegalne nawoływanie do nienawiści, czyli publiczne zachęcanie do przemocy lub agresji skierowanej przeciwko określonej grupie osób/członkowi danej grupy, zdefiniowanych według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej.

Najbardziej skuteczną metodą, która uniemożliwia dostęp do treści bezprawnych, jest usuwanie niepożądanych materiałów, niezależnie od tego, w jakim kraju one się znajdują. W katalogu treści nielegalnych szczególne miejsce zajmują materiały prezentujące seksualne wykorzystywanie dzieci. W większości krajów świata takie treści są ścigane i tępione. Istnieje tu także daleko posunięta współpraca międzynarodowa. Instytucje walczące z tego typu materiałami należą do stowarzyszenia International Association of Internet Hotlines (INHOPE). Obecnie zrzesza ono 51 zespołów, które podejmują działania zapobiegające rozpowszechnianiu wykorzystywania nieletnich do celów seksualnych. W Polsce członkiem Stowarzyszenia INHOPE jest, działający w ramach Państwowego Instytutu Badawczego NASK, zespół Dyżurnet.pl, który ściśle współpracuje z polską policją oraz dostawcami treści i usług internetowych.

Obecnie wyzwaniem dla organów ścigania nadal pozostają portale/strony anonimizujące użytkowników internetu, czyli utrudniające identyfikację sprawców rozpowszechniających nielegalne treści, a także umożliwiające dostęp do celowo ukrytych zasobów internetu, np. The Tor Project, The Freenet Project, I2P (Invisible Internet Project). Szacuje się, że z samego oprogramowania Tor korzysta codziennie około 3 mln ludzi. Znajduje się tam około 50–60 tys. zanonimizowanych serwisów, z których połowa jest używana do nielegalnych celów (np.: handlu narkotykami, dystrybucji plików CSAM (materiałów przedstawiających wykorzystywanie seksualne dzieci).

W przyszłości, mając na względzie walkę z nielegalnymi treściami, należy położyć zdecydowany nacisk na działania uniemożliwiające publikację zakazanych materiałów. Nową jakość w tym zakresie przynoszą tworzone obszerne zbiory zawierające identyfikatory nielegalnych zdjęć i filmów (tzw. *hash value*), które następnie mogą być używane przez platformy internetowe do ich rozpoznania i zaprzestania dalszego publikowania lub przesyłania. Ciągle jednak istotna jest kwestia zgłaszania nielegalnych treści przez użytkowników do administratorów serwisów albo do punktu kontaktowego Dyżurnet.pl.

Treści pornograficzne

W literaturze można spotkać wiele definicji pornografii, większość odnosi się do tekstów lub wizerunków (na grafikach, zdjęciach, filmach) przedstawiających sceny erotyczne o treści nieprzyzwoitej, podkreślając cel przekazu, którym jest wywołanie podniecenia u odbiorcy (Makaruk i in., 2017).

Polskie prawo karne mówi o treściach pornograficznych przede wszystkim w art. 202 Kodeksu karnego. Z zapisu w k.k. wynika zakaz prezentowania materiałów pornograficznych osobie, która sobie tego nie życzy (art. 202 § 1 k.k.), a także małoletniemu poniżej 15. roku życia i/lub udostępniania mu przedmiotów o takim charakterze (art. 202 §2 k.k.). Karalne jest również organizowanie reklamy lub promocji działalności polegającej na rozpowszechnianiu treści pornograficznych (art. 200 § 5 k.k.).

Kodeks karny nie definiuje pornografii wprost, ale bezpośrednią definicję pornografii sformułował Sąd Najwyższy. Według niej „treści pornograficzne (...) to zawarte w utrwalonej formie (np. film, zdjęcia, czasopisma, książki, obrazy) lub nie (np. pokazy na żywo) prezentacje czynności seksualnych człowieka (zwłaszcza ukazywanie organów płciowych człowieka w ich funkcjach seksualnych), i to zarówno w wymiarze niesprzecznym z ich biologicznym ukierunkowaniem, jak i czynności seksualnych człowieka sprzecznych z przyjętymi w społeczeństwie wzorcami zachowań seksualnych" (Wyrok Sądu Najwyższego – Izba Karna z dnia 23 listopada 2010 r.).

W związku z obowiązującymi przepisami prawa w serwisach i portalach internetowych, które mogą zawierać treści pornograficzne, wprowadza się odpowiednie ostrzeżenie, często wymuszające deklarację pełnoletności. Zazwyczaj jest to jednak jedynie komunikat wymagający kliknięcia przycisku „OK" lub „Wchodzę".

Na przestrzeni lat przeprowadzono wiele badań na temat skutków oglądania pornografii. Zdaniem badaczy dostęp do tego typu materiałów ma wiele negatywnych konsekwencji, np. uzależnia od pornografii, powoduje efekt eskalacji (osoby korzystające z pornografii szukają coraz bardziej ekstremalnych bodźców), prowadzi do zaburzeń w odczuwaniu satysfakcji seksualnej oraz dysfunkcji seksualnych, staje się przyczyną kryzysu w związkach, promuje przedmiotowy sposób traktowania drugiego człowieka, zwłaszcza kobiet, a także jest przyczyną podejmowania innych zachowań ryzykownych. Pornografia i inne treści o charakterze seksualnym mają szczególnie szkodliwy wpływ na dzieci i młodzież. Wyniki badań potwierdzają, że kontakt z takimi treściami często kształtuje fałszywe poglądy na sferę seksualności i stanowi wypaczoną edukację seksualną. Wiele dzieci trafia na treści pornograficzne wbrew swojej woli, w momencie kiedy nie są na nie przygotowane. Nastolatki mogą celowo poszukiwać treści o charakterze seksualnym, co jest związane z procesem dojrzewania i zaciekawieniem sferą seksualności. Trafiając na pornografię,

otrzymują treści, które nie tylko nie przekazują im żadnej wartościowej wiedzy o ludzkiej seksualności, lecz także mogą całkowicie zniekształcić ich postrzeganie tej sfery życia. Badania prowadzone wśród młodzieży wskazały na związek między oglądaniem filmów pornograficznych online a postrzeganiem kobiet jako obiektów seksualnych. Takie przekonania są kształtowane przez pornografię, w której kobieta prawie nigdy nie jest pokazywana jako równoprawna partnerka mężczyzny, lecz niemal zawsze występuje w sytuacji podporządkowania. Badania dowodzą również, że oglądanie materiałów pornograficznych może prowadzić do wczesnego podejmowania zachowań o charakterze seksualnym, zwiększać przyzwolenie na nawiązywanie przypadkowych kontaktów seksualnych oraz wpływać na angażowanie się w inne ryzykowne zachowania w tej dziedzinie, takie jak posiadanie wielu partnerów czy też używanie podczas seksu substancji psychoaktywnych. Co więcej, zaobserwowano zależność między intensywnym oglądaniem pornografii a stosowaniem przemocy seksualnej. Dodatkowo treści pornograficzne mogą być dla nastolatków źródłem nieadekwatnych wzorów wyglądu i kompleksów dotyczących własnego ciała. Widoczny jest też związek między nałogowym oglądaniem pornografii a występowaniem problemów psychicznych i mniejszym zadowoleniem z życia. Badania wykazały, że dziewczęta mające kontakt z prezentowanymi w mediach seksualizującymi materiałami częściej doświadczają depresji (Wojtasik, Wójcik, Włodarczyk, 2017).

W 2017 r. Fundacja Dajemy Dzieciom Siłę na zlecenie Ministerstwa Zdrowia w ramach Narodowego Programu Zdrowia 2016–2020 przeprowadziła badania *Kontakt dzieci i młodzieży z pornografią* (Makaruk i in., 2017). Z raportu z badań wynika, że aż 43 proc. dzieci i nastolatków w wieku 11–18 lat miało kontakt z materiałami pornograficznymi i seksualizującymi. Może niepokoić fakt, że 18 proc. respondentów co najmniej raz w tygodniu styka się z takimi treściami. Dzieci i młodzież najczęściej sięgają po materiały prezentujące osoby nagie (69 proc. ankietowanych), ale – co warto podkreślić – aż 60 proc. badanych widziało też treści przedstawiające stosunek seksualny. Niestety aż 22 proc. młodych internautów w wieku 13–18 lat oglądało materiały pornograficzne zawierające agresję słowną i fizyczną.

Wnioski opracowane przez Fundację Dajemy Dzieciom Siłę dowodzą, że oglądanie treści pornograficznych może nieść za sobą negatywne skutki psychospołeczne, a także zachęcać młodych ludzi do podejmowania ryzykownych zachowań seksualnych. Osoby, które kiedykolwiek miały kontakt z pornografią, trzy razy częściej otrzymują nagie lub półnagie zdjęcia (seksting), a także pięć razy częściej

je wysyłają. Natomiast ci spośród młodych internautów, którzy codziennie korzystają z dostępu do pornografii, dwukrotnie częściej odbywają wczesną inicjację seksualną (zanim jeszcze ukończą 15 lat). Przywołane badania z 2017 r. pokazały, że w Polsce większość rodziców nie stosuje żadnych zabezpieczeń na urządzeniach, do których mają dostęp ich dzieci. Raport wykazał także, że dorośli rzadko rozmawiają z dziećmi na temat bezpieczeństwa online.

Treści przemocowe

Do treści przemocowych zaliczyć należy przede wszystkim: materiały, filmy, zdjęcia, informacje, gry prezentujące akty agresji i przemocy, brutalne zachowania wobec ludzi i zwierząt, obrażenia fizyczne, drastyczne sceny z udziałem ofiar wypadów, wulgarny język. Publikowanie materiałów zawierających przemoc – poza nielicznymi wyjątkami (np. rozpowszechnianie pornografii związanej z prezentowaniem przemocy czy szerzenie nienawiści na tle rasowym) – nie jest zabronione prawem, a tym samym trudno z nim walczyć.

Przemoc jest obecna w mediach od wielu lat. Jednak do popularności treści bazujących na agresji słowno-fizycznej przyczynił się rozwój nowoczesnych technologii. Przemoc słowno-fizyczna bardzo często pojawia się w dostępnych w internecie filmach i grach komputerowych (przeznaczonych zarówno dla dorosłych, jak i dla dzieci). Niepokojące jest to, że materiały oparte na agresji niejednokrotnie pełnią funkcję rozrywkową. Dzieci i młodzież jako użytkownicy sieci najczęściej stykają się z treściami przemocowymi w serwisach społecznościowych, na kanałach filmowych i streamingowych.

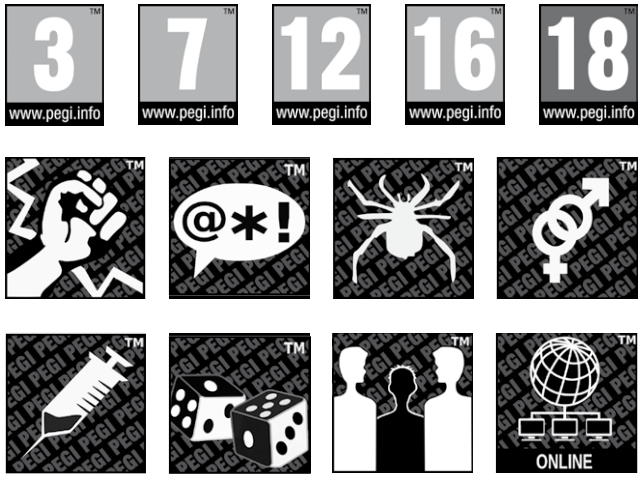
Zarówno łatwość publikacji materiałów w sieci, jak i brak skutecznych mechanizmów ich weryfikacji przed opublikowaniem pozwalają zamieszczać w internecie – obok wartościowych produkcji – także te zawierające treści brutalne i drastyczne, szokujące lub wywołujące sensację. Przykładem tego rodzaju twórczości stały się popularne ostatnio wśród młodzieży tzw. patostreamy, czyli regularne transmisje na żywo prezentujące zachowania uznawane za społecznie nieakceptowalne, takie jak wulgarne odzywki, wyzywanie i poniżanie, bójki, libacje alkoholowe czy narkotykowe. Patostreamerzy zbierają wokół siebie fanów, budują bazy subskrybentów, a także pozyskują środki finansowe poprzez zbieranie donejtów (z ang. *donates* – datki, darowizny) od widzów.

Stopień oddziaływania mediów na zachowania dzieci i nastolatków zależy od wielu czynników, np. rodzaju materiału, osobowości młodego internauty, specyfiki środowiska, w którym się wychowuje. Treści związane z przemocą (w tym seksualną) u części najmłodszych odbiorców mogą negatywnie oddziaływać na psychikę, prowadząc do tworzenia się postaw lękowych i/lub wzrostu agresywności wobec innych. Najmłodsi internauci, obcując z takimi treściami, stają się mniej wrażliwi na krzywdę innych osób, mogą wykazywać niższy poziom empatii i chęci niesienia pomocy (Mrug, Madan, Cook, 2015).

Ograniczenie wpływu niebezpiecznych treści na młodych użytkowników internetu musi odbywać się wielowymiarowo. Z jednej strony polega na edukowaniu i uświadamianiu im szkodliwości tych materiałów, a ponadto na uwrażliwieniu najmłodszych internautów na konieczność zgłaszania takich publikacji, ilekroć na nie natrafią w sieci. Z drugiej strony powstrzymanie oddziaływania niepożądanych treści wiąże się z koniecznością wprowadzenia zabezpieczeń technicznych. Rodzice mogą wyposażyć urządzenia, których używa dziecko (np. telefon komórkowy, komputer), w odpowiednie programy filtrujące. Najmłodsi internauci powinni korzystać z zaufanych stron internetowych pod kontrolą rodziców. Starsi powinni być przez dorosłych przygotowani na możliwość kontaktu z tego rodzaju przekazami i zachęcani do rozmów na temat takich incydentów.

Należy też zadbać, aby dzieci i nastolatki korzystały z gier komputerowych odpowiednich do ich wieku, niezawierających elementów agresji. Bardzo przydatny jest Ogólnoeuropejski System Klasyfikacji Gier z 2003 r. (więcej na pegi.info/pl). System ten wspomaga rodziców podczas zakupu gier komputerowych. Zgodnie z założeniami PEGI ocenia gry pod względem zawartych w nich treści, a także kryterium wiekowego gracza. Co warte podkreślenia, Ogólnoeuropejski System Klasyfikacji Gier zupełnie nie odnosi się do umiejętności graczy, a jedynie do obecności niebezpiecznych treści. Szczególną uwagę należy zwrócić na gry komputerowe przeznaczone tylko i wyłącznie dla osób dorosłych (oznaczenie PEGI 18). Obecnie systemem PEGI lub podobnymi do niego posługują się także największe sklepy z aplikacjami na urządzenia mobilne.

Rys. 2. Oznaczenia stosowane w klasyfikacji gier PEGI



Źródło: www.pegi.info

Treści autodestrukcyjne

Za niebezpieczne treści uznawane są nie tylko materiały zawierające pornografię i przemoc, lecz także takie, które wywołują negatywne emocje, nadmierne pobudzenie, uzależnienie, wprowadzają w błąd lub zachęcają do zachowań autodestrukcyjnych. Tego typu materiały mogą sprawić, że świat stanie się dla dziecka niezrozumiały, zagrażający i przestanie czuć się w nim bezpiecznie. Mogą zachęcać też do zachowań zagrażających zdrowiu lub życiu oraz wpływać na kształtowanie się fałszywych przekonań na temat świata oraz siebie.

W internecie dzieci mogą mieć również dostęp do treści, które przedstawiają zachowania antyspołeczne w pozytywnym świetle, np. opisują, jak zdobyć narkotyki i je zażywać lub jak je zastąpić legalnymi substancjami (np. lekami) o podobnym działaniu. Inne strony mogą zachęcać do zachowań autoagresywnych, jak samookaleczanie, zaburzenia odżywiania i samobójstwa. Strony, które pochwalają zachowania autodestrukcyjne, są niebezpieczne dla zdrowia i życia dziecka, ponieważ dzięki nim może się ono dowiedzieć, w jaki sposób skrzywdzić siebie, oraz jednocześnie utwierdzić się w przekonaniu, że tego typu zachowania są jedynym właściwym wyjściem z problematycznej sytuacji. Mogą nawet zawierać wskazówki, w jaki sposób ukryć te zachowania przed rodziną i przyjaciółmi.

Jednym z przykładów są materiały online zachęcające do zachowań anorektycznych (pro-ana) i bulimicznych (pro-mia). Dla osób, które znajdują się w grupie ryzyka zachorowania na zaburzenia odżywiania, kontakt z takimi materiałami może być bardzo niebezpieczny, przy czym trudno jednoznacznie oszacować, jak duży odsetek młodzieży jest dotknięty tym problemem. Wyniki badań przeprowadzonych w ostatnich latach (Makaruk i in., 2017) pokazują, że 41,5 proc. dziewcząt i 14,3 proc. chłopców w wieku 14–17 lat miało kontakt z treściami promującymi skrajne odchudzanie.

Wiele badań zwraca uwagę na instruktażowy charakter stron pro-ana. Prezentują one szkodliwe i często drastyczne metody odchudzania się, które mogą być naśladowane przez odbiorców. Badacze wykazali również, że kobiety i dziewczęta korzystające w sieci z materiałów promujących treści pro-ana miały niższą samoocenę, częściej porównywały się z innymi i postrzegały siebie jako cięższe, niż były w rzeczywistości. Taka postawa prowadziła do tego, że dla zwolenniczek pro-ana jedyną szansą na osiągnięcie w przyszłości szczęścia i spełnienia było zwiększenie liczby i częstotliwości ćwiczeń, a także zmiana żywienia (Bardone-Cone, Cass, 2007). Co ciekawe, zarówno u kobiet, jak i mężczyzn uwewnętrznienie ideologii pro-ana korelowało z nasileniem się dążenia do bycia przesadnie chudym (Juarez J. i in., 2012). Treści o charakterze pro-ana i/lub materiały promujące nadmierną dbałość o dietę cieszą się dużą popularnością. Są znacznie częściej komentowane i lepiej oceniane, dlatego też mogą docierać do relatywnie dużej grupy odbiorców. Może to narażać nastoletnich odbiorców nie tylko na dostęp, ale też kopiowanie zachowań autodestruktywnych. Co istotne, dziewczęta w wieku 13–17 lat stanowią w sieci najliczniejszą społeczność zainteresowaną zgłębianiem tego typu materiałów (Syed-Abdul, Fernandez-Luque, Jian, 2013).

Poważnym problemem są w tym kontekście także strony pochwalające samookaleczanie się lub samobójstwa. Mogą to być treści publikowane przez pojedyncze osoby lub całe grupy tematyczne. Wiele z nich zawiera dokładne instrukcje, w jaki sposób dokonać samookaleczenia lub popełnić samobójstwo, oraz nierzadko zachęca do takich rozwiązań jako jedynych i słusznych sposobów na przeżywane trudności. W przypadku stron dotyczących samookaleczeń i samobójstw korzystanie z ich treści może również wspierać czynnik identyfikacji z grupą ludzi wypowiadających się na ten temat.

Treści o charakterze autodestrukcyjnym są dla dzieci i młodzieży szeroko dostępne w internecie. Z badań *EU Kids Online 2018* wynika, że aż 43 proc. młodych ludzi w wieku 11–17 lat miało styczność z treściami zawierającymi informacje, jak popełnić samobójstwo, a 42 proc. – jak zrobić sobie samemu krzywdę. Jedynie nieco mniej, bo 38 proc., miało kontakt z treściami pro-ana i pro-mia, a 37 proc. – z instrukcjami na temat brania narkotyków (Pyżalski i in., 2019). Tak wysokie odsetki wskazują na szkodliwe treści jako jeden z najbardziej rozpowszechnionych czynników ryzyka w internecie.

Narzędzia kontroli rodzicielskiej

Najskuteczniej będziemy chronić dzieci i młodzież przed niebezpiecznymi treściami, towarzysząc im przy eksploracji internetu i rozmawiając o tym, co napotykają w sieci. Jednocześnie możemy korzystać z rozwiązań technicznych, które mają na celu ochronę dzieci podczas odwiedzania przez nie stron internetowych i uruchamiania aplikacji. Na rynku istnieje obecnie bardzo wiele narzędzi kontroli rodzicielskiej. Obejmują one programy autonomiczne, oprogramowanie wbudowane w system operacyjny, funkcje bezpiecznego wyszukiwania w wyszukiwarkach internetowych.

Oprogramowania autonomiczne to w większości przypadków rozwiązania płatne, wymagające zakupienia, pobrania i zainstalowania programu lub aplikacji. Swoje produkty oferują tu wszyscy najwięksi producenci oprogramowania antywirusowego. Oprócz oprogramowania na komputery PC na rynku znaleźć można coraz więcej aplikacji na mobilne systemy operacyjne (iOS, Android i inne).

Większość najpopularniejszych systemów operacyjnych oferuje opcje kontroli rodzicielskiej wbudowane w system. Rodzice nie muszą w takim wypadku instalować dodatkowych aplikacji. Na komputerze wyposażonym w system Windows 7 można aktywować moduł ochrony rodzicielskiej, który umożliwia kontrolowanie czasu korzystania z komputera oraz ograniczenie dostępu do wskazanych gier i aplikacji. Moduł znajdziemy w panelu sterowania. W przypadku tabletów i smartfonów z systemem Android warto odpowiednio skonfigurować Google Play, przeglądarkę oraz aplikację serwisu YouTube. W nowszych wersjach systemu istnieje także możliwość stworzenia profilu ograniczonego, który będzie stanowił bezpieczną przestrzeń dla dziecka. Właściciele urządzeń mobilnych z systemem iOS (iPad, iPhone) mogą ograniczyć dziecku dostęp do wybranych

treści, korzystając z funkcji „Ograniczenia", która znajduje się w ustawieniach ogólnych. Określimy tam m.in. ograniczenie wiekowe dotyczące wyświetlanych filmów oraz używanych programów[2].

Kolejną grupą narzędzi kontroli rodzicielskiej są filtry bezpiecznego wyszukiwania: SafeSearch (dla wyszukiwarki Google) i Bezpieczne wyszukiwanie (dla przeglądarki Bing). Pozwalają one zatrzymać wyniki wyszukiwania i blokować spośród nich treści niepożądane. Ten typ zabezpieczeń ma ograniczone możliwości konfiguracji, do tego jest darmowy i dostępny dla wszystkich zalogowanych użytkowników. Często programy kontroli rodzicielskiej wymuszają na wyszukiwarkach korzystanie z takich opcji.

Głównymi zadaniami oprogramowania kontroli rodzicielskiej są weryfikacja i blokowanie treści szkodliwych dla dzieci. Może to się odbyć na kilka sposobów, zależnie od wybranego oprogramowania:

- blokowanie określonych typów stron internetowych zdefiniowanych przez osobę dorosłą ze względu na kategorię tematyczną (np.: serwisy erotyczne, serwisy wideo, portale społecznościowe);
- blokowanie konkretnych adresów internetowych zdefiniowanych jako czarna lista;
- udostępnianie tylko stron zdefiniowanych jako bezpieczne (biała lista).

Współczesne narzędzia kontroli rodzicielskiej oprócz filtrowania zapewniają dodatkowe funkcje. Zależnie od wybranego oprogramowania będą to: ograniczenie czasowe korzystania z komputera, blokowanie określonych typów gier (zgodnie z klasyfikacją PEGI), blokowanie programów, tworzenie raportów ze statystykami, a także wysyłanie powiadomień.

Podczas korzystania z oprogramowania do kontroli rodzicielskiej należy pamiętać, że jego skuteczność będzie uzależniona od możliwości aplikacji, a także przede wszystkim właściwej konfiguracji, uwzględniającej wiek dziecka. Zbyt rygorystyczne obostrzenia mogą powodować irytację zarówno młodego użytkownika, jak i jego opiekuna. Często prowadzi to do całkowitej rezygnacji z zastosowania kontroli rodzicielskiej. Dlatego tak ważne są stałe monitorowanie aktywności dzieci i młodzieży, a także częste dostosowywanie ustawień do indywidualnych potrzeb.

[2] Dokładne instrukcje dostępne są na stronie dzieckowsieci.pl.

Należy też pamiętać, że programy kontroli rodzicielskiej są jedynie narzędziem wspomagającym ochronę dzieci podczas korzystania z internetu, a najlepiej sprawdzają się przy najmłodszych użytkownikach sieci.

Pamiętaj!

- Pamiętaj, że filtr kontroli rodzicielskiej pomaga ograniczyć kontakt dziecka z potencjalnie niebezpiecznymi dla niego stronami internetowymi, zawierającymi szkodliwe treści. Zwróć uwagę na to, że dzieci i młodzież rzadziej łączą się z internetem, korzystając z komputera stacjonarnego, a coraz częściej wykorzystują do tego celu urządzenia mobilne (np. smartfon, tablet, konsolę do gry).
- Pamiętaj, że żadne narzędzie nie zapewnia gwarancji ochrony dziecka przed zetknięciem się z ryzykownymi i szkodliwymi treściami. Dlatego tak ważne są umiejętność mądrej reakcji ze strony osoby dorosłej oraz udzielenie wsparcia. Zachęcaj dzieci do dzielenia się z tobą wszelkimi niepokojącymi sytuacjami, jakie je spotkały w sieci czy których były świadkami.
- Uczul dziecko na zagrożenia związane z korzystaniem z publicznych/otwartych sieci Wi-Fi (hotspotów). Mogą one w nieograniczony sposób umożliwiać dostęp do szkodliwych treści i narażać najmłodszych użytkowników sieci na wiele zagrożeń (np. na utratę danych i/lub nawiązanie niebezpiecznych kontaktów).
- Staraj się towarzyszyć dzieciom w odkrywaniu bogactwa internetu i rozmawiaj z nimi o ich zainteresowaniach. Jeśli dzieci będą wiedzieć, że rodzice interesują się ich aktywnością online, wówczas chętniej w trudnej sytuacji zwrócą się do dorosłych o pomoc.
- Ucz dziecko krytycznego podejścia do informacji. Dyskutuj o treściach, które są prezentowane online, podkreślając, że nie każda wiadomość przeczytana w sieci jest prawdziwa. Internet jest kopalnią wiedzy, a niestety często też przestrzenią niesprawdzonych i potencjalnie szkodliwych doniesień i porad, w której każdy może przedstawić się jako ekspert oferujący najlepsze rozwiązanie problemu. Porozmawiaj z dzieckiem o sposobach weryfikacji wiedzy pozyskiwanej online.

- Wspieraj dzieci, pomagając im uodpornić się na obraz świata rozpowszechniany w internecie, a w szczególności w mediach społecznościowych. Wyjaśnij, że bardzo często promuje się wyidealizowany świat i nierealne do osiągnięcia kanony piękna. Pomóż dzieciom i młodzieży stworzyć ich pozytywny wizerunek online. Nie zaniedbuj rozmów o tym, co warto, a czego nie warto ujawniać w sieci.
- Porozmawiaj z dzieckiem/nastolatkiem o tym, że internet może stać się idealną przestrzenią dla osób głoszących radykalne, niekiedy szokujące, poglądy czy tych, którzy prezentują rażące zachowania w celu zdobycia jak największej popularności. Zwróć uwagę, że internauci (np. youtuberzy, blogerzy) wykorzystują swoją widownię w celu zwiększenia oglądalności lub finansowania dalszej aktywności w sieci.
- Pamiętaj, że zawsze możesz anonimowo zgłosić na stronie www.dyzurnet.pl treści, które są twoim zdaniem nielegalne bądź szkodliwe.

Bibliografia

1. Aronson E., Wilson T.D., Akert R.M., (1997), *Psychologia społeczna. Serce i umysł*. Poznań: Zysk i S-ka.
2. Bardone-Cone A.M., Cass K.M, (2007), *What does viewing a pro-anorexia website do? An experimental examination of website exposure and moderating effects*, w: „International Journal of Eating Disorders", t. 40 (6), s. 537–548.
3. Custers K., Van den Bulck J., (2009), *Viewership of pro-anorexia websites in seventh, ninth and eleventh graders*, w: „European Eating Disorders Review", t. 17 (3), s. 214–219.
4. Decyzja ramowa Rady 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych, zob. bit.ly/decramr (dostęp: 02.01.2019).
5. Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym, zob. bit.ly/prawaut (dostęp: 02.01.2010).
6. Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady (UE) z dnia 11 maja 2005 r. dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady 84/450/EWG, dyrektywy 97/7/WE, 98/27/WE i 2002/65/WE Parlamentu Europejskiego i Rady oraz rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady, zob. bit.ly/nieuczp (dostęp: 02.01.2019).
7. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2011/92/z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW, zob. bit.ly/wyksekd (dostęp: 02.01.2019).
8. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW, zob. bit.ly/2HGYulx (dostęp: 02.01.2019).
9. Dziecko w sieci, zob. dzieckowsieci.pl (dostęp: 02.01.2010).
10. Jett S., LaPorte D.J., Wanchisn J., (2010), *Impact of exposure to pro-eating disorder websites on eating behaviour in college women*, w: „European Eating Disorders Review", t. 18 (5), s. 4104–4116.
11. Juarez J., Soto E., Pritchard M.E., (2012), *Drive for muscularity and drive for thinness: the impact of pro-anorexia websites*, w: „Eating Disorders", t. 20 (2), s. 99–112.
12. Kirwil L., (2011), *Polskie dzieci w internecie. Zagrożenia i bezpieczeństwo. Część 2. Częściowy raport z badań EU Kids Online II przeprowadzonych wśród dzieci w wieku 9–16 lat i ich rodziców*, Warszawa: SWPS – EU Kids Online – PL, zob. bit.ly/poldzin (dostęp: 02.01.2019).
13. Livingstone S., Kirwil L., Ponte C., Staksrud E., (2013), *In their own words: what bothers children online?*, with the EU Kids Online network, w: EU Kids Online, London: London School of Economics and Political Science, zob. bit.ly/bochion (dostęp: 02.01.2019).
14. Livingstone S., Smith, P.K., (2014). *Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age.* „Journal of child psychology and psychiatry", 55 (6), 635–654.
15. Makaruk K., Włodarczyk J., Michalski P., (2017), *Kontakt dzieci z pornografią. Raport z badań*, Warszawa: Fundacja Dajemy Dzieciom Siłę, zob. bit.ly/kdzporn (dostęp: 02.01.2019).
16. Mrug S., Madan A., Cook E.W., Wright R.A. (2015), *Emotional and physiological desensitization to real-life and movie violence*, „Journal of youth and adolescence", nr 44 (5), s. 1092–1108.
17. Ogólnoeuropejski System Klasyfikacji Gier (PEGI), zob. pegi.info/pl (dostęp: 01.02.2019).
18. Polak Z., Różycka M., Marańda M., Szeląg M., (2015), *Zagrożenia internetowe. Wybrane zjawiska*, Warszawa: NASK, zob. bit.ly/zagrint (dostęp: 02.01.2019).
19. Pyżalski J., Zdrodowska A., Tomczyk Ł., Abramczuk K., (2019), *Polskie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski*, Poznań: Wydawnictwo Naukowe UAM.
20. Rouleau C.R., von Ranson K.M., (2011), *Potential risks of pro-eating disorder websites*, „Clinical Psychology Review", nr 31 (4), s. 525–531.

21. Stowarzyszenie Twoja Sprawa, (2017), *Raport z badań naukowych: Podsumowanie literatury i badań naukowych wskazujących na negatywne skutki korzystania z pornografii w kontekście ochrony dzieci i młodzieży*, Warszawa: Stowarzyszenie Twoja Sprawa, zob. http://bit.ly/negskpo (dostęp: 02.01.2019).
22. Syed-Abdul S., Fernandez-Luque L., Jian W.S., Crain S., Chuluunbaatar E. i in., (2013), *Misleading health-related information promoted through video-based social-media: anorexia on YouTube*, „Journal of Medical Internet Research", t. 15 (2).
23. Ustawa z dnia 6 czerwca 1997 r., Kodeks karny, (Dz.U. 1997 nr 88, poz. 553), zob. bit.ly/u970606 (dostęp: 02.01.2019).
24. Wojtasik Ł., (2006), *Kontakty dzieci z niebezpiecznymi treściami w internecie. Raport z badań Gemius/FDN*, Warszawa: Fundacja Dzieci Niczyje, zob. bit.ly/niebtri (dostęp: 02.01.2019).
25. Wojtasik Ł., Wójcik S., Włodarczyk J., Makaruk K., (2017), *Kontakt dzieci i młodzieży z pornografią. Co wiemy i co możemy zrobić?*, Warszawa: Fundacja Dajemy Dzieciom Siłę.
26. Wyrok Sądu Najwyższego – Izba Karna z dnia 23 listopada 2010 r., IV KK 173/10, LEX nr 667510.
27. Valkenburg P.M., Peter J., & Walther J.B., (2016). *Media effects: Theory and research.* „Annual Review of Psychology", 67, 315–338.
28. Villani S., (2001). *Impact of media on children and adolescents: a 10-year review of the research.* „Journal of the American Academy of child & adolescent psychiatry", 40 (4), 392–401.
29. Zalecenie Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie, zob. bit.ly/zwaniet (dostęp: 02.01.2019).

II.4. Uwodzenie dzieci i młodzieży w internecie

/Marta Wojtas/

Internet jest przestrzenią komunikacyjną, którą wykorzystuje większość młodych osób, narażając się niekiedy na różne niebezpieczne sytuacje. Zdarza się, że w wyniku zawarcia znajomości w internecie dzieci stają się ofiarami sprawców, którzy dążą do tego, aby wykorzystać je seksualnie, zwerbować do grup przestępczych, sekt lub zachęcać do zachowań szkodliwych dla życia lub zdrowia. Tego typu sytuacje są wyzwaniem nie tylko dla organów ścigania, ale także instytucji odpowiedzialnych za bezpieczeństwo i profilaktykę.

Terminologia i charakterystyka zjawiska

Zjawisko uwodzenia dzieci za pośrednictwem internetu, określane w anglojęzycznej literaturze przedmiotu jako *grooming*, to szczególna kategoria relacji tworzona między osobami dorosłymi a dziećmi w celu ich uwiedzenia i wykorzystania seksualnego. Przemoc seksualna w procesie groomingu może przybierać różnorodne formy, począwszy od prezentowania dziecku materiałów pornograficznych, wyłudzania intymnych zdjęć, zmuszania do tworzenia nagrań w trakcie wykonywania czynności seksualnych, aż po molestowanie fizyczne i/lub gwałt podczas spotkania poza siecią. Chociaż proces uwodzenia dzieci i nastolatków w sieci nie zawsze kończy się bezpośrednim kontaktem sprawcy z ofiarą, to jednak zawsze jest procederem głęboko krzywdzącym. Zdaniem terapeutów konsekwencjami groomingu są typowe objawy urazu psychicznego powstałe na skutek wykorzystywania seksualnego.

Najmłodsi internauci są najbardziej narażeni na niebezpieczne kontakty na portalach społecznościowych, a także podczas korzystania z aplikacji, które umożliwiają komunikację między użytkownikami. To tam pojawia się przestrzeń, aby nawiązywać relacje z nieznajomymi, często bez odpowiedniej weryfikacji tego, z kim naprawdę prowadzona jest rozmowa. Stwarza to pole do szeregu nadużyć ze strony sprawców, którzy po to, aby rozpocząć znajomość z dzieckiem, mogą zmienić swoją tożsamość, podając się za kogoś, kim w rzeczywistości nie są. Portale społecznościowe to miejsca, w których młode osoby publikują wiele informacji osobistych, nie zabezpieczając ich przed dostępem nieznajomych, wskutek czego sprawca w łatwy sposób może gromadzić wiedzę na temat swojej potencjalnej ofiary.

W ostatnich dekadach niezwykle popularne wśród dzieci i młodzieży stały się gry online. Bardzo wiele platform i witryn przeznaczonych do tej formy aktywności wyposażono w możliwość przesyłania wiadomości, udostępniania zdjęć, filmów oraz prowadzenia rozmów audio i wideo. Badania działalności przestępców internetowych potwierdzają, że sprawcy coraz częściej wykorzystują ten kanał do kontaktu z ofiarami.

Skala zjawiska

Wyniki badań dowodzą, że wiele młodych osób może być narażonych na kontakt ze sprawcami. Niemal jedna czwarta młodych internautów (23,1 proc.) przyznała, że zdarzyło im się spotkać bezpośrednio z dorosłym poznanym w sieci. Zapytano tych nastolatków, którzy zdecydowali się na taki krok, kogo poinformowali o spotkaniu. Okazało się, że 39 proc. respondentów poinformowało rodziców, 27 proc. – kolegów, 5 proc. – innego dorosłego. Niepokoi fakt, że aż 29 proc. młodych internautów nie poinformowało nikogo o tym, co zaszło (Naukowa i Akademicka Sieć Komputerowa, 2016). Wynika z tego, że niemal 7 proc. polskich nastolatków spotkało się bez wiedzy rodziców lub innych bliskich dorosłych z osobami poznanymi w sieci. Tym samym młodzi internauci mogli mieć kontakt ze sprawcą.

Badania dotyczące groomingu przeprowadzone w Wielkiej Brytanii na próbie 1718 osób w wieku 11–16 lat pokazały, że 42 proc. respondentów otrzymywało materiały od obcych ludzi poznanych w internecie. Z kolei 37 proc. badanych dodało nieznajomego do grona znajomych na komunikatorze, a 35 proc. – na portalu społecznościowym (Webster i in., 2012). Można zatem wywnioskować, że dzieci oraz młodzież często decydują się na działania ryzykowne w sieci, przez co mogą być narażone na kontakt z dorosłymi sprawcami.

Grooming jest procesem trudnym do identyfikacji przez rodziców oraz innych bliskich dorosłych z otoczenia dziecka. Sprawca dąży do utrzymania w tajemnicy relacji z ofiarą, manipulując jej emocjami i wzmacniając zaangażowanie w kontakt. Niektóre sygnały w zachowaniu dziecka lub nastolatka mogą sugerować, że znajduje się w relacji ze sprawcą online. Do symptomów pozwalających zdiagnozować, czy młody internauta został uwiedziony przez osobę dorosłą w sieci, można zaliczyć np.: wycofanie się, izolację od rodziny, posiadanie pornografii na swoich urządzeniach z dostępem do sieci, otrzymywanie wiadomości, prezentów czy pieniędzy od nieznajomych, prowadzenie w tajemnicy rozmów z obcymi, szybkie wyłączanie urządzeń elektronicznych i zabezpieczanie ich hasłem przed rodzicami (Netsafe, 2015).

Niektóre z wyżej wymienionych zachowań mogą się pokrywać z typowymi dla wieku rozwojowego tendencjami do ochrony własnej prywatności przed rodzicami, a także potrzebą autonomii. Trzeba jednak sobie uzmysłowić, że w kontekście zjawiska uwodzenia w sieci wskazane objawy nabierają niebezpiecznego i destrukcyjnego charakteru.

Charakterystyka ofiar i sprawców

Typologia młodych ofiar uwodzenia w sieci opiera się na danych uzyskanych na podstawie analizy dowodów przestępstw, w tym rozmów online sprawców z ich ofiarami. Wnioski z badań przeprowadzonych w ramach *European Online Grooming Project* (Webster i in., 2012) pozwoliły wyróżnić dwa typy osób, które przeważają jako pokrzywdzone w procederze uwodzenia w internecie. Należą do nich:

A. osoby szczególnie wrażliwe i ufne (ang. *vulnerable victims*) ze względu na: dużą potrzebę uwagi i bliskości emocjonalnej, trudności w kontaktach z rodzicami, poszukiwanie związków miłosnych w sieci. Osoby te pragnęły pozostać w relacji ze sprawcą i wykazywały się lojalnością wobec niego, co było głównym czynnikiem wywołującym opór przed ujawnieniem go. Ofiary z tej grupy czuły się samotne i miały niskie poczucie własnej wartości. Niektóre z nich doświadczyły już wcześniej wykorzystywania seksualnego. Dla tego typu ofiar sprawca był „mentorem", który zdobył ich zaufanie i wspólnie z nimi starał się rozwiązywać jego bieżące problemy.

B. osoby podejmujące zachowania ryzykowne (ang. *risk-taking victims*) poszukują nowych bodźców, mogą nie zachowywać osobistych granic w kontaktach z innymi. Ofiary z tej grupy, przekonane o kontrolowaniu sytuacji, stały się szczególnie podatne na szantaż ze strony sprawcy w związku z poczuciem współodpowiedzialności za to, co zaszło. W gronie pokrzywdzonych z tej grupy znajdują się zazwyczaj osoby pewne siebie i otwarte, ale – co warto podkreślić – bardziej w kontaktach online niż bezpośrednich relacjach. Niejednokrotnie ofiary same inicjują kontakty seksualne, a wyrażając na nie zgodę, narażają się na spotkanie ze sprawcą.

Tego typu ofiary rzadko ujawniają sytuację ze względu na poczucie odpowiedzialności i winy.

Na podstawie cech ofiar i tendencji, które wymieniono powyżej, możemy mówić jedynie o czynnikach ryzyka zwiększających prawdopodobieństwo zaangażowania się w relację ze sprawcą. Nadal nie opracowano żadnego zestawienia cech osoby mogącej stać się typową ofiarą groomingu. W toku badania zjawiska uwodzenia dzieci i młodzieży w internecie zidentyfikowano również czynniki stanowiące możliwą ochronę młodych osób przed zaangażowaniem się w tego typu relację. Nastolatki, którym udało się uniknąć urazu i zakończyć kontakt ze sprawcą online, charakteryzowały się umiejętnością rozpoznawania zjawiska i obrony przed kontaktami, które wydawały im się niepokojące, rozumienia komunikatów dotyczących bezpieczeństwa w sieci oraz pewnością, że mogą się zwrócić po pomoc do osób ze swojego otoczenia (Webster i in., 2012).

Zidentyfikowano również kilka profili sprawców. Przestępcy ci różnią się między sobą sposobem nawiązywania i podtrzymywania relacji z ofiarą, a także ujawniania swojej tożsamości lub celu działań wobec dziecka (np. inicjując spotkanie bezpośrednie lub pozyskując intymne zdjęcia lub filmy). Sprawcy przestępstw seksualnych – niezależnie od motywacji i sposobu realizacji kontaktu z dzieckiem – nawet jeśli działają wyłącznie w sieci, są tak samo niebezpieczni jak ci, którzy krzywdzą w kontakcie bezpośrednim (Wolak, Finkelhor, 2013).

Uwodzenie dzieci i nastolatków w internecie nie zawsze jest procesem rozciągniętym w czasie. Czasem, ze względu na różne zachowania sprawców i ofiar, może trwać bardzo krótko (zaledwie kilka minut) (INHOPE, 2012). Zdarza się jednak tak, że kontakt sprawcy z ofiarą ma charakter relacji trwającej powyżej kilku miesięcy. Przestępca działający w sieci, aby osiągnąć zamierzony cel, może przejawiać następujące zachowania:

1. Poszukuje ofiary wśród dzieci/nastolatków aktywnych online.
2. Rozpoznaje zainteresowania ofiary oraz jej potrzeby emocjonalne. W wielu przypadkach może tego dokonać poprzez analizę treści publikowanych przez dzieci na ich profilach i stronach dostępnych dla wszystkich użytkowników. Sprawcy często używają tematów atrakcyjnych dla dzieci i nastolatków, np. związanych z aktualnymi trendami.
3. Zdobywa zaufanie dziecka/nastolatka. Sprawca nawiązuje relację i stara się zaprzyjaźnić z potencjalną ofiarą, a także oswoić ją ze sobą. Ponadto przestępca wykazuje zainteresowanie przeżyciami i problemami młodego internauty.
4. Izoluje swoją ofiarę. Przestępca gromadzi informacje, które mogą pomóc utrzymać w tajemnicy relację z dzieckiem/nastolatkiem przed jego domownikami. W tym celu sprawca pyta np. o lokalizację komputera, użytkowników danego sprzętu elektronicznego, osoby z najbliższego otoczenia, jej/jego relacje z domownikami, zainteresowanie rodziców. Często też przestępca, prosząc ofiarę o zachowanie ich znajomości w tajemnicy przed bliskimi, używa argumentów typu: „nie mów nikomu, bo to taki nasz wspólny sekret", „nie mów nikomu, bo inni będą chcieli zniszczyć naszą przyjaźń".
5. Porusza intymne tematy, oswajając dziecko/nastolatka ze szkodliwymi treściami, a także zachęcając do niebezpiecznych zachowań. Oprócz podejmowania rozmów związanych z seksualnością sprawca może również namawiać do robienia sobie intymnych zdjęć. Zdarza się, że przestępca wysyła ofierze swoje zdjęcia intymne albo zachęca ją do oglądania stron pornograficznych. Takie działania pozwalają sprawcy ocenić podatność dziecka/nastolatka na jego zabiegi i uległość ofiary. Niejednokrotnie bywa też tak, że przestępca używa pozyskanych materiałów (np. zdjęć, filmów) do tego, aby szantażować ofiarę lub zmusić ją do zachowania ich znajomości w tajemnicy albo wymóc dalszą uległość (Palmer, Stacey, 2004).
6. Zrzuca na dziecko/nastolatka odpowiedzialność lub współodpowiedzialność za swoje czyny. Dzieci wskutek takich rozmów podejmują czynności seksualne, doświadczając przy tym negatywnych emocji (np. wstydu, poczucia winy). Pedofile mogą wykorzystywać słabość i niedojrzałość swojej ofiary, aby ją szantażować. W ten sposób sprawca pragnie zwiększyć nad nią kontrolę (np. wmawiając, że jest winna tego, co się stało), a jednocześnie odebrać jej szansę na uzyskanie pomocy.
7. Używa przemocy, szantażu i gróźb, jeśli nie otrzymuje od ofiary tego, czego chce. Zdarza się, że sprawca manipuluje dzieckiem/nastolatkiem, zapowiadając, że opublikuje jego intymne zdjęcia w internecie, wyśle je do szkoły i rodziców/opiekunów prawnych, a nawet że zabije rodzinę.
8. Używa wzmocnień pozytywnych, kreując się na miłego człowieka, zainteresowanego losem dziecka, któremu niejednokrotnie ofiarowuje prezenty.
9. Dąży do osiągnięcia celu, czyli spotkania swojej ofiary lub uzyskania od niej materiałów o charakterze pornograficznym.

Najmłodsi internauci ze względu na uwarunkowania rozwojowe są ufni i nie zawsze potrafią obiektywnie ocenić sytuację, w której się znajdują. Wiele małoletnich ofiar, całkowicie zmanipulowanych przez działania sprawców, zupełnie nieświadomie wpada w ich pułapkę (Lanning, 2005). Zdarza się jednak, że młode osoby same poszukują w sieci kontaktów o charakterze seksualnym. W takich przypadkach ofiary mogą nie stawiać oporu przed wykorzystaniem seksualnym. Bywają też sytuacje skrajne, w których małoletni dopuszczają się prostytucji w sieci, sprzedając zdjęcia czy realizując sekspokazy dla osób dorosłych. Większość młodych ludzi zachowujących się w ten sposób to ofiary wykorzystania seksualnego lub innego rodzaju przemocy, dzieci z placówek opiekuńczych lub pozbawione opieki, a w związku z tym szczególnie narażone na różnego rodzaju niebezpieczeństwa (Palmer, Stacey, 2004).

Analiza problematyki uwodzenia dzieci w internecie uczy, że warto również zwrócić uwagę na czynniki zewnętrzne. Mogą one determinować zachowanie użytkowników sieci, a także zwiększać podatność młodych ludzi na groźne kontakty w tym środowisku. Czynniki zewnętrzne są związane z kulturą masową oraz dostępem do szkodliwych treści online. Jednym z nich jest seksualizacja przekazów medialnych, która obniża próg wrażliwości dzieci i młodzieży, a także normalizuje zachowania mogące godzić w integralność dzieci. Powszechność dostępu najmłodszych użytkowników internetu do pornografii w sieci może narazić ich na niebezpieczne kontakty ze sprawcami. Badania potwierdzają, że około 43 proc. nastolatków w Polsce miało dostęp do materiałów o charakterze seksualnym online (Makaruk, Włodarczyk, Michalski i in., 2017). Respondenci z tej grupy pięciokrotnie częściej zamieszczają swoje intymne zdjęcia w sieci, a także trzykrotnie częściej otrzymują takie materiały od innych użytkowników.

Prawo

Problem uwodzenia dzieci za pośrednictwem internetu jest problemem międzynarodowym. Warto sobie jednak uświadomić, że systemy ustawodawcze poszczególnych państw rozmaicie go interpretują. W Polsce uwodzenie małoletnich osób w sieci jest przestępstwem ściganym na mocy art. 200a Kodeksu karnego:

- „Art. 200a § 1. Kto w celu popełnienia przestępstwa określonego w art. 197 § 3 pkt 2 lub art. 200, jak również produkowania lub utrwalania treści pornograficznych, za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej nawiązuje kontakt z małoletnim poniżej lat 15, zmierzając, za pomocą wprowadzenia go w błąd, wyzyskania błędu lub niezdolności do należytego pojmowania sytuacji albo przy użyciu groźby bezprawnej, do spotkania z nim, podlega karze pozbawienia wolności do lat 3.
- § 2. Kto za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej małoletniemu poniżej lat 15 składa propozycję obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych, i zmierza do jej realizacji, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2”.

Warto zwrócić uwagę, że karany jest już sam kontakt z dzieckiem, mający na celu wykorzystanie seksualne lub uzyskanie materiałów o takim charakterze, niezależnie od tego, czy te przestępstwa w jego konsekwencji się wydarzyły.

Pamiętaj!

- Porozmawiaj z dzieckiem o problemie uwodzenia w sieci. Wytłumacz, że nawiązywanie kontaktów przez internet może być niebezpieczne, bo trudno zweryfikować, czy osoba, z którą się rozmawia, jest tym, za kogo się podaje.
- Porozmawiaj z dzieckiem o jego znajomych z internetu. Jeśli w gronie swoich znajomych ma osoby, których nie zna z życia realnego, warto, aby je usunęło lub ograniczyło dostęp do publikowanych przez siebie materiałów.
- Zaoferuj dziecku wsparcie i powiedz, żeby zawsze informowało Cię, jeśli jakaś obca osoba będzie poruszała tematy związane z seksualnością lub inne, które je zaniepokoją.
- Poinformuj dziecko o możliwości zgłoszenia takiej sytuacji policji.
- Bądź uważna (-y), nietypowe zmiany w zachowaniu dziecka mogą niekiedy świadczyć o tym, że jest w niebezpiecznej relacji.
- W razie wątpliwości szukaj wsparcia specjalistów – skontaktuj się z telefonem dla rodziców i nauczycieli w sprawie bezpieczeństwa dziecka 800 100 100.

Bibliografia

1. Child Exploitation and Online Protection Command (CEOP), (2007), *Strategic overview 2006–2007. Final report*, Londyn: Child Exploitation and Online Protection Command.

2. Davidson J., Lorenz M., Martellozo E., Grove-Hills J., (2009), *Evaluation of CEOP ThinkU-know internet safety programme and exploration of young people's internet safety knowledge*, Londyn: Child Exploitation and Online Protection Centre (CEOP).
3. DOMO, (2018), *Data never sleeps 5.0*, zob. bit.ly/datnevs (dostęp: 02.01.2019).
4. Federal Bureau of Investigation (FBI), (2011), *Child Predators. The online threat continues to grow*, Federal Bureau of Investigation, zob. bit.ly/chipred (dostęp: 02.01.2019).
5. International Association of Internet Hotlines (INHOPE), (2012), *Paedophiles 'internet groom' minors for sex in just 8 mins*, Amsterdam, zob. bit.ly/ingroom (dostęp: 02.01.2019).
6. International Centre for Missing and Exploited Children (ICMEC), (2017), *Online grooming of children for sexual purposes. Model legislation and global review*, International Centre for Missing and Exploited Children.
7. Kirwil L., (2010), *Polskie dzieci w internecie. Zagrożenia i bezpieczeństwo na tle danych dla UE. Wstępny raport z badań EU Kids Online przeprowadzonych wśród dzieci w wieku 9–16 lat i ich rodziców*, Warszawa: Szkoła Wyższa Psychologii Społecznej, zob. bit.ly/poldzin (dostęp: 02.01.2019).
8. Lanning K.V., (2005), *Compliant child victims: Confronting an uncomfortable reality, w: Viewing child pornography on the internet*, Quayle E., Taylor M. (red.), Kent: Russell House Publishing, s. 49–60.
9. Livingstone S., Haddon L., (2009), *EU Kids Online and EU Kids Online II*, w: „Zeitschrift für Psychologie (Horizons), nr 217 (4), s. 4–7, zob. bit.ly/eukidso (dostęp: 02.01.2019).
10. Makaruk K., Włodarczyk J., Michalski P., (2017), *Kontakt dzieci z pornografią. Raport z badań*, Warszawa: Fundacja Dajemy Dzieciom Siłę, zob. bit.ly/kdzporn (dostęp: 02.01.2019).
11. Naukowa i Akademicka Sieć Komputerowa, (2016), *Nastolatki 3.0. Wybrane wyniki ogólnopolskiego badania uczniów w szkołach*, Warszawa: NASK – Państwowy Instytut Badawczy, zob. bit.ly/wynnas3 (dostęp: 02.01.2019).
12. Netsafe, (2015), *Grooming and online predators.* Netsafe – Online Safety for New Zealand, zob. bit.ly/onlpred (dostęp: 02.01.2019).
13. Palmer T., Stacey L., (2004), *Just one click. Sexual abuse of children and young people through the internet and mobile phone technology*, Essex: Barnardo's, zob. bit.ly/sexabch (dostęp: 02.01.2019).
14. Rogers P., Capitanini L., (2012), *Predators use gaming systems' live video features to find kids*, NBC Chicago, zob. bit.ly/predliv (dostęp: 02.01.2019).
15. Ustawa z dnia 6 czerwca 1997 r., Kodeks karny, (Dz.U. 1997 nr 88, poz. 553), zob. bit.ly/u970606 (dostęp: 02.01.2019).
16. Webster S., Davidson J., Bifulco A., Gottschalk P., Caretti V., Pham T., Grove-Hills J., Turley C., Tompkins C., Ciulla S., Milazzo V., Schimmenti A., Craparo G., (2012), *European Online Grooming Project. Final Report*, zob. bit.ly/ongrpro (dostęp: 02.01.2019).
17. Wolak J., Finkelhor D., (2013), *Are crimes by online predators different from crimes by sex offenders who know youth in-person?*, w: „Journal of Adolescent Health", nr 53 (6), s. 736–741.

II.5. Zagrożenie dla prywatności

/Anna Rywczyńska/

Problematyka prywatności to jeden z kluczowych elementów bezpieczeństwa w kontekście technologii cyfrowej. Funkcjonalności globalnej sieci poniekąd przyzwyczają jej użytkowników do częstego dzielenia się informacjami, danymi osobowymi, których nie ujawnialiby w innych warunkach. Media społecznościowe preferują, aby ich członkowie podawali prawdziwe dane osobowe. Podobna sytuacja ma miejsce podczas korzystania z aplikacji, które wymagają szczegółowych danych do logowania. Warto też pamiętać o tym, że smartfony mogą być na stałe podpięte do kont bankowych, a wyszukiwarki zapisują obszerną historię aktywności internautów w sieci. Często zdarza się, że użytkownicy internetu automatycznie akceptują żądania witryn i usług sieciowych, zapominając, że mają prawo chronić swoje dane poprzez rezygnację z uciążliwych aplikacji (np. odwołujących się do różnych informacji zapisanych w urządzeniu, takich jak: kontakty, zdjęcia, hasła, a także pobierających, zdaniem ich właścicieli, zbyt wiele danych lub wymagających co chwilę skonfigurowania).

Ustawienia prywatności znajdują się zarówno w konsolach do gier (urządzenia te w ostatnich latach były narażone na ataki ze strony cyberprzestępców), jak w smartfonach, gdzie eliminują przykładowo działanie usług lokalizacyjnych.

Ochrona prywatności wiąże się nie tylko z poznaniem możliwości technologicznych używanego urządzenia, ale przede wszystkim z umiejętnością zarządzania swoją obecnością w sieci. W przypadku młodych użytkowników najważniejszą rolę odgrywają rodzice, którzy sami często decydują o początkach obecności dziecka online, do nich też należy przygotowanie dzieci do świadomego prowadzenia internetowych aktywności. To opiekun musi wiedzieć, kiedy dziecko może samodzielnie założyć profil w sieci społecznościowej oraz o jakich zagrożeniach myśleć, decydując o wyborze ustawień prywatności – czyli tego, kto może mieć dostęp do zdjęć, filmów czy postów udostępnianych przez dziecko.

Często pada pytanie, na kim spoczywa główna odpowiedzialność za edukację dzieci i młodzieży w kwestiach bezpieczeństwa w internecie, i odpowiedź jest prosta – na wszystkich osobach i instytucjach pracujących z dziećmi oraz na rzecz dzieci. Obok zadań rodziców nieoceniona jest funkcja szkoły, która w ramach działań edukacyjnych i wychowawczych musi przygotować

uczniów do efektywnego wykorzystywania technologii cyfrowej, w tym do poszanowania własnej i cudzej prywatności m.in. w środowisku szkolnym, co jest jednym z ważnych elementów profilaktyki cyberprzemocy.

W jaki sposób regulacje prawne chronią prywatność?

Prywatność to prawo do ochrony swoich osobistych informacji przysługujące każdemu człowiekowi, ale też umiejętność takiego zachowania, które pomaga ludziom chronić swoje dane oraz dane innych osób. Prywatność jest chroniona przez prawo, m.in. przez Konstytucję RP, w której w art. 47 pojawia się zapis: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym".

Kodeks cywilny także zapewnia ochronę dóbr osobistych człowieka. W art. 23 tego dokumentu można przeczytać, że: „Dobra osobiste człowieka, 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 wieku".

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., które na mocy art. 99 ogólnego rozporządzenia o ochronie danych stosuje się od 25 maja 2018 r., wymusza wyższy stopień ochrony danych personalnych przez firmy internetowe, portale, serwisy bądź aplikacje. Dokument reguluje też dostęp do zakładania kont na portalach społecznościowych. W przypadku usług społeczeństwa informacyjnego, skierowanych bezpośrednio do osób małoletnich, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Państwa członkowskie Unii Europejskiej mogą przewidzieć w swoim prawie niższą granicę wiekową wynoszącą co najmniej 13 lat. Prawo dotyczy też prywatności w kontekście naruszeń dobrego imienia oraz rozpowszechniania pornografii z udziałem osób małoletnich. Kodeks karny za wykroczenie przeciwko ochronie danych traktuje: uporczywe nękanie (art. 190a), zniesławienie (art. 212), zniewagę (art. 216), przestępstwa przeciwko ochronie informacji – włamanie informatyczne (art. 265, art. 267, art. 268, art. 268a). Opublikowanie w internecie w jakiejkolwiek formie zdjęcia osoby małoletniej w wieku poniżej 18 lat jest przestępstwem ściganym na podstawie art. 202 Kodeksu karnego.

Prywatność w świetle badań

Żadne rozwiązania technologiczne ani prawne nie zabezpieczą naszej prywatności, a w szczególności prywatności najmłodszych użytkowników internetu, jeśli nie będą podparte świadomością, w jaki sposób zarządzać informacjami o sobie w sieci oraz w jaki sposób chronić prywatność swoich bliskich i znajomych. Internet jest rozszerzeniem codzienności, przestrzenią, w której zwłaszcza młodzi użytkownicy utrzymują kontakty z rówieśnikami, prezentują swoje zainteresowania, prowadzą dyskusje i dzielą się pasjami. Najnowszy raport *Nastolatki 3.0* (Kamieniecki i in., 2017) dowiódł, że 93,4 proc. najmłodszych użytkowników sieci jest online, z czego przez ponad pięć godzin aktywnie korzysta z urządzeń cyfrowych. Prawie 70 proc. respondentów codziennie kontaktuje się z koleżankami i kolegami ze szkoły za pomocą sieci. Posiadanie konta na przynajmniej jednym portalu społecznościowym deklaruje blisko 95 proc. najmłodszych internatów w weku 13–17 lat. Osobiste zdjęcia i filmy publikuje 79,3 proc. dzieci i nastolatków. Ponad połowa badanych dzieli się swoimi opiniami, zamieszczając je w formie komentarzy. Co ciekawe, zdjęcia znajomych publikuje 43,5 proc. młodych ludzi. Ponad 20 proc. młodych ludzi nie widzi potrzeby ograniczania dostępności do swoich postów. Nastolatkowie wiedzą, jak zarządzać ustawieniami, ale chcą, aby ich profile/konta były widoczne dla innych użytkowników sieci i nie sprawiały znajomym trudności w wyszukiwaniu.

Jednym z najczęstszych zagrożeń sieciowych zgłaszanych przez dzieci i młodzież są przypadki przejęcia kont najmłodszych internautów. Aż 13 proc. badanych doświadczyło kradzieży tożsamości, stając się ofiarą tego, że ktoś się pod nich podszywał w cyberprzestrzeni. Wśród młodych użytkowników sieci aż 40 proc. słyszało o tym, że ich znajomi doświadczyli takiego procederu. Często przyczyną takiej sytuacji jest dzielenie się młodych ludzi między sobą hasłami do kont internetowych. Znane są przypadki pozostawiania sobie nawzajem haseł do profili, na przykład na okres wakacji, kiedy dziecko obawia się, że nie będzie miało dostępu do sieci i nie będzie w stanie reagować na posty przyjaciół. Takie wzajemne przysługi jednak nie zawsze dobrze się kończą, bo hasło może trafić w niepowołane ręce. Prywatność może być też przedmiotem ataków cyberprzestępców, którzy są w stanie stworzyć fałszywą tożsamość poprzez dostęp do danych zapisanych na urządzeniach cyfrowych wykorzystywanych przez dzieci bądź poprzez złośliwe oprogramowanie zaszyte w popularnych grach i aplikacjach.

Wizerunek w sieci

Możliwość aktywnego zaistnienia w społecznościach daje szanse wcześniej niedostępne. Można w zasadzie nieograniczonej grupie użytkowników sieci prezentować swoje dokonania, promować swoją twórczość, doświadczenie i osiągnięcia, nawiązywać relacje i przyjaźnie bez względu na odległości geograficzne. Posiadanie jak największego grona „znajomych" w portalach społecznościowych daje szczególnie młodym ludziom poczucie satysfakcji i szczęścia oraz podnosi ich samoocenę. Portale społecznościowe zmieniają sposób, w jaki ludzie się komunikują, dzielą pomysłami i wiedzą. Powodują też, że coraz bardziej zaciera się granica między życiem online a offline, między życiem prywatnym a służbowym, mieszają różne, dawniej rozdzielane środowiska. Swój wizerunek w sieci tworzymy poprzez informacje, którymi dzielimy się w komentarzach, postując, czyli pisząc na swoich profilach w sieciach społecznościowych, na blogach, w tweetach (krótkie wpisy w serwisie Twitter), publikując zdjęcia, filmy itd. Ważne też bywają treści, które inni publikują na naszych profilach – dlatego tak istotne jest, aby konfigurować ustawienia prywatności, tak abyśmy to my decydowali o tym, kto może publikować posty i widzieć nasze wpisy.

Wraz z przenoszeniem dużej części naszej społecznej aktywności do sieci rośnie wielka baza danych, która przez lata buduje nasz wizerunek i będzie wpływać na to, jak dziś i za parę lat będą nas postrzegać inni. Eric Schmidt, były dyrektor generalny Google, w wywiadzie dla „The Telegraph" (Wardrop, 2010) stwierdził, że życie prywatne młodych ludzi jest tak obficie dokumentowane w sieci, że za parę lat będziemy obserwatorami masowych zmian nazwisk spowodowanych chęcią odcięcia się od swojej internetowej przeszłości. Młodzi ludzie często nie mają świadomości, jak łatwo przez zwykłą wyszukiwarkę można znaleźć wiele rozproszonych informacji prezentujących całą wirtualną aktywność. O tym, jak ważne jest dbanie o swój wizerunek w sieci, świadczy choćby to, że w ostatnich latach powstaje coraz więcej serwisów świadczących usługi w zakresie oczyszczania internetowej reputacji (monster.com/career-advice). Te serwisy umożliwiają wyszukanie i kontrolę informacji na nasz temat, a nawet pomagają w usuwaniu niewygodnych lub nieprawdziwych wpisów. W niektórych z nich można zaznaczyć, co interesuje nas w szczególności: czy jest to własna reputacja, czy informacje na temat firmy lub dziecka. Część serwisów jest darmowa, niektóre oferują takie usługi odpłatnie.

Od lat toczyła się dyskusja o tzw. prawo do bycia zapomnianym i największą zmianę w regulacjach dotyczących obowiązku prawnego administratorów przyniósł art. 17 ust. 1 Rozporządzenia o ochronie danych osobowych (RODO), który mówi, że: „Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe (...). Prawo to ma być realizowane, gdy spełniony jest jeden spośród następujących warunków:

1. dane nie są już dłużej niezbędne do realizacji celu, w jakim zostały zebrane lub są przetwarzane;
2. podmiot danych wycofał zgodę na przetwarzanie jego danych osobowych oraz nie istnieją podstawy prawne, aby mimo to kontynuować przetwarzanie;
3. podmiot danych sprzeciwia się przetwarzaniu oraz nie występują nadrzędne, prawnie uzasadnione podstawy przetwarzania;
4. podmiot danych sprzeciwia się przetwarzaniu jego danych osobowych na potrzeby i w zakresie marketingu bezpośredniego (w tym profilowania);
5. przetwarzanie w inny sposób nie jest lub nie było zgodne z RODO lub innymi przepisami prawa;
6. dane osobowe zostały zebrane w nawiązaniu do oferowania bezpośrednio osobom poniżej 16 lat usług społeczeństwa informatycznego (np. e-handel, portale społecznościowe").

Żądanie usunięcia swojej historii przez administratora może być bardzo trudnym wyzwaniem, zwłaszcza w kontekście szybkości reakcji oraz zadbania o wszelkie miejsca w sieci, gdzie dana informacja mogła być powielona. Na pewno spowoduje to modyfikację metod postępowania z danymi osobowymi oraz potrzebę zaawansowanych prac nad systemami informatycznymi.

Rola rodziców w ochronie wizerunku małych dzieci online

Dużą rolę w ochronie prywatności dziecka w sieci odgrywa świadomy rodzic. Rodzice często rozpoczynają obecność dziecka online.

W 2010 r. firma AVG Technologies (Badania AVG Technologies, 2010) przeprowadziła badania, z których wynikało, że 81 proc. dzieci poniżej drugiego roku życia posiada swój profil w sieci, a średnia wieku, w którym dzieci w tej grupie obchodzą swoje cyfrowe narodziny, wynosi sześć miesięcy. Aż 23 proc. dzieci z tej grupy rozpoczyna cyfrowe życie w momencie, kiedy ich rodzice publikują w internecie zdjęcia z prenatalnych badań USG. Wiele krzywdy dla przyszłości dziecka mogą spowodować nieprzemyślanie opublikowane zdjęcia, filmy, komentarze, które po latach mogą być dla dzieci wstydliwe (zjawisko nosi nazwę *troll parenting*). Niezwykle ważne jest, aby takie wczesne zdjęcia dziecka pokazywać z rozwagą i dużą wrażliwością, mając na uwadze jego dorastanie. Rodzice często

przyczyniają się do szybszej, niż określają regulaminy, obecności dzieci na portalach społecznościowych. Facebook, mimo że dostępny od 13. roku życia, jest bardzo popularny wśród młodszych dzieci, które czasami przyznają, że konto pomogli im założyć rodzice.

Podobna sytuacja ma miejsce w przypadku kanałów autorskich w sieci. Treści nagrywane przez młodych „influencerów" zyskują tysiące fanów, a często za ich powstaniem stoją rodzice, którzy bądź wspierają talenty swoich dzieci, bądź też dostrzegają duży biznesowy potencjał zaangażowania całej rodziny w tego typu twórczą działalność. Jednym z przykładowych kanałów o rosnącej popularności (Sotrender.com, 2018) jest kanał „Hejka tu Lenka". Prowadzą go rodzice Lenki, oni również występują w nagraniach. Pojedyncze filmy na kanale mają blisko 1,5 mln wyświetleń, a liczba subskrybentów przekroczyła 750 tys. Na kanale można znaleźć vlogi, unboxingi – rozpakowywanie zabawek i opisywanie, co znajduje się w danych zestawach – popularne sieciowe wyzwania (tzw. *challenge*) itp. Treści pojawiają się średnio co drugi dzień. Inne znane obecnie kanały dziecięce to np. Cookie Mint, Mela Modela czy Pusheen Girl. W jednym miesiącu na kanałach pojawia się blisko 30 tys. komentarzy. Kanały najczęściej dotyczą prezentacji najnowszych zabawek, wiele z nich to kanały gamingowe, czyli poświęcone najbardziej znanym grom online, bywają kanały podróżnicze. Te, o których mowa w artykule, można z całą pewnością nazwać projektami biznesowymi posiadającymi swoich stałych reklamodawców i firmy sponsorskie. Poza nimi są również blogi zakładane samodzielnie przez młodych internautów, stopniowo walczących o uwagę internetowej widowni. Odpowiedzialność rodziców dotyczy w zasadzie wszystkich aspektów tego rodzaju działalności dzieci czy nastolatków. Rodzice muszą sobie odpowiedzieć na pytania: czy ich dziecko jest gotowe na potencjalną popularność, jak poradzi sobie z prawie pewnym hejtem, czy 9–10 lat to nie za wcześnie na taką aktywność w sieci (większość dzieci właśnie wtedy chce zacząć prowadzenie bloga). A jeśli zdecydują o prowadzeniu autorskiego kanału, to: jak nim zarządzać, czy umożliwić komentowanie, czy komentarze zablokować, czy już same „like" i „dislike" nie będą dla dziecka problemem. W jaki sposób aktywnie moderować komentarze, jeśli będą włączone? Czy taką działalność dziecko powinno prowadzić pod pseudonimem lub bez uwidoczniania twarzy – tylko głos, żeby w razie problemów z hejtem nie przeniosło się to na najbliższe otoczenie dziecka – i wreszcie czy dziecko jest gotowe i powinno być angażowane w tak ciężką i systematyczną pracę, jaką jest tworzenie kanału online, który w dalszej perspektywie ma mieć potencjał biznesowy? Istotny jest też element prawny, zgodnie z którym przed ukończeniem 13. roku życia dziecko nie może uruchamiać samodzielnie zarządzanego kanału na YouTubie.

Seksting i inne ryzykowne zachowania w sieci

Dla młodych ludzi konsekwencje niewłaściwego zarządzania swoją internetową reputacją często nie wydają się poważnym i realnym zagrożeniem. Wśród ryzykownych zachowań, jakie podejmują online, są m.in.: publikowanie nieodpowiednich zdjęć i filmów (np. przedstawiających nastolatków pod wpływem alkoholu, w niedwuznacznych sytuacjach), komentarze i linki, które mogą źle świadczyć o ich autorze (np. wpisy rasistowskie, ksenofobiczne), publikowanie negatywnych opinii na temat kolegów, nauczycieli, rodziny czy upublicznianie prywatnych informacji lub danych nieograniczonemu gronu odbiorców. W ostatnich latach zauważa się też niepokojące zjawisko uczestniczenia przez nastolatków w seksczatach wideo (tzw. sekskamerkach) oraz stale rosnące zjawisko sekstingu – czyli wymieniania się między rówieśnikami SMS-ami, zdjęciami, filmami o charakterze seksualnym.

Aspekt seksualności jest nierozerwalnie związany z dorastaniem, a rewolucja internetowa sprawiła, że dziś łatwiej można mieć dostęp do treści erotycznych. Młodzież jest nie tylko odbiorcą tych treści, ale również ich twórcą, gdy przesyła między sobą materiały o charakterze seksualnym. Analizując wyniki badań, można zaobserwować rozbieżność między liczbą osób wysyłających tego rodzaju materiały a liczbą otrzymujących je. Ma to wytłumaczenie, bowiem zjawisko sekstingu należy podzielić na dwa rodzaje: pierwotny oraz wtórny. Pierwotny jest wtedy, kiedy ktoś sam wysyła swoje np. nagie zdjęcia, a wtórny, kiedy otrzymujący takie materiały rozsyła je w celu pochwalenia się lub ośmieszenia osoby, która mu zaufała. Według badań przeprowadzonych w Polsce w 2014 r. co dziewiąty nastolatek wysłał za pośrednictwem telefonu lub internetu swoje nagie lub prawie nagie zdjęcia. Prawie jedna trzecia badanych nastolatków przyznała, że otrzymała tego rodzaju materiały. Ponad połowa młodych ludzi (58 proc.) dostrzegła obecność zjawiska przesyłania zdjęć o charakterze erotycznym wśród swoich rówieśników (Wójcik, Makaruk, 2014). Potwierdzają to również wyniki badań *Nastolatki wobec internetu* (Konopczyński, Lange, Osiecki i in., 2014), według których 25 proc. młodych użytkowników sieci przyznało, że otrzymało materiały sekstingowe, ponad 7 proc., że wysłało intymne zdjęcia, zaś 30 proc. zadeklarowało, że zna ludzi, którym zdarzyło się wysłać swoje intymne zdjęcia osobom poznanym w internecie. Jak wynika z badań, do wysyłania intymnych zdjęć przyznał się niewielki odsetek badanych, jednak na podstawie technik projekcyjnych zastosowanych w kwestionariuszu można wnioskować, że procent takich osób jest znacznie wyższy. Jednocześnie blisko co trzeci ankietow-

any zadeklarował, że prowadził wideorozmowy z osobami, których wcześniej nie znał, a co ósmy, że w trakcie takich rozmów dostał propozycję pokazania się bez ubrania (Konopczyński i in., 2014).

Konsekwencje zachowań sekstingowych bywają bardzo poważne – mogą zaważyć na życiu społecznym, karierze, mogą też nosić znamiona przestępstwa jako materiały pedofilskie. Głównym wyzwaniem w zwalczaniu negatywnych skutków sekstingu wydaje się przeciwdziałanie rozsyłaniu otrzymywanych przez nastolatków „dowodów miłości" i uczenie młodych ludzi szacunku dla czyjejś prywatności i zaufania, jakim bywamy obdarzani.

Z sekstingiem wiąże się jeszcze jedno bardzo groźne zjawisko, a mianowicie szantażowanie (tzw. sextortion) osób, od których wyłudzono intymne zdjęcia i filmy. Jest to rosnąca działalność przestępcza, w której zwalczanie, podobnie jak w zwalczanie materiałów przedstawiających seksualne wykorzystywanie osób małoletnich, zaangażowana jest międzynarodowa policja oraz zespoły reagujące na zagrożenia sieciowe (w tym w Polsce zespół Dyżurnet.pl).

Internet rzeczy w kontekście prywatności dzieci i młodzieży

Internet rzeczy (ang. *Internet of Things*) to koncept polegający na wyposażaniu przedmiotów w mechanizmy umożliwiające komunikację z innymi przedmiotami bądź systemami. Pozwala to na zdalne zbieranie danych z takich urządzeń, a często także na kontrolę nad nimi. Wśród urządzeń z dziedziny internetu rzeczy znajdują się również inteligentne zabawki. Urządzenia te, bazując na infrastrukturze internetu i technologii mobilnych, potencjalnie są podatne na wszystkie problemy związane z cyberprzestępczością. Gromadzone w nich dane dziecka, jak również dane wrażliwe rodziny (rozmowy, zapisy wideo) mogą być wykorzystane do zbudowania fałszywej tożsamości i posługiwania się nią w celach nielegalnych.

Warto przy tej okazji zwrócić uwagę na dodatkowy aspekt prywatności dzieci związany z rozwojem internetu rzeczy, w postaci tzw. technologii ubieralnej (ang. *wearables*), czyli ubrań oraz akcesoriów zawierających w sobie komputer lub zaawansowane technologie elektroniczne. Wielu ekspertów uważa, że rozwiązania, które pozornie mają zwiększyć bezpieczeństwo dzieci, mogą w konsekwencji ograniczać ich prywatność i wolność osobistą, jednocześnie zachęcając do akceptowania nadzoru. Z jednej strony naturalne jest, że rodzice chcą wykorzystać każdą możliwość, aby chronić swoje dzieci, ale z drugiej zbyt daleko posunięta inwigilacja, świadomość stałego monitoringu ze strony rodziców i nauczycieli mogą mieć bardzo duży wpływ na zachowanie i rozwój młodych ludzi.

Pamiętaj!

- Jeśli zamieszczasz w sieci zdjęcia dziecka lub filmy z jego udziałem, zastanów się, czy żadna z tych treści nie będzie dla niego w przyszłości obciążeniem i nie przyniesie mu wstydu.
- Uświadamiaj dziecko na temat jego prawa do ochrony prywatności, a także obowiązku poszanowania prywatności innych osób.
- Pamiętaj o ograniczeniu wiekowym związanym z uczestnictwem najmłodszych internautów w mediach społecznościowych.
- Kiedy dziecko zakłada swój pierwszy profil w sieci, pomóż mu mądrze skorzystać z udostępnianych przez serwis ustawień prywatności.
- Wizerunek w sieci to bardzo ważna rzecz – naucz dziecko systematycznego sprawdzania informacji na jego temat – tego, co samo publikuje, oraz treści, które mogą publikować inni internauci.
- Uczul dziecko, że emocje to zły doradca i że każdy wpis o nas świadczy – niech publikuje rozważnie.
- Internetowa twórczość to duże wyzwanie – zanim dziecko założy bloga czy kanał tematyczny w sieci, omów z nim wszystkie potencjalne zagrożenia oraz sprawdź, czy jest gotowe na publiczną aktywność.
- Pamiętaj, że europejskie rozporządzenie o ochronie danych osobowych (RODO) umożliwiło zgłaszanie do administratorów żądań usuwania dotyczących nas danych (prawo do bycia zapomnianym).

Bibliografia

1. AVG Technologies, (2010), *SMB Market Landscape Report 2010*, Stany Zjednoczone, zob. bit.ly/smbmark (dostęp: 02.01.2019).
2. Kamieniecki W., Bochenek M., Tanaś M., Wrońska A., Lange R., Fila M., Loba B., Konopczyński F., (2017), *Raport z badania. Nastolatki 3.0*, Warszawa: NASK – Państwowy Instytut Badawczy, zob. bit.ly/rapnas3 (dostęp: 02.01.2019).
3. Konopczyński M., Lange, R., Osiecki J. i inni, (2014), *Ogólnopolskie badanie. Nastolatki wobec internetu*, raport opracowany na zlecenie Rzecznika Praw Dziecka i NASK przez Pedagogium WSNS w okresie maj – czerwiec 2014, Warszawa: NASK – Państwowy Instytut Badawczy, zob. bit.ly/naswint (dostęp: 02.01.2019).
4. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. nr 78, poz. 483), zob. bit.ly/konst97 (dostęp: 02.01.2019).

5. Livingstone S., Carr J., Byrne J., (2016), *One in three: Internet governance and children's rights. Office of Research – Innocenti Discussion Paper 2016–01*, Florence: UNICEF Office of Research, zob. bit.ly/integov (dostęp: 02.01.2019).
6. Majak K. (2013), *Troll parenting, czyli rodzice wyśmiewają własne dzieci w internecie*, NaTemat.pl, zob. bit.ly/trollpar (dostęp: 02.01.2019).
7. Monster Worldwide, zob. monster.com/career-advice (dostęp: 02.01.2019).
8. Naukowa i Akademicka Sieć Komputerowa, Research.nk, (2013), *Prezentacja treści seksualnych przez młodzież poprzez wideoczaty*, NASK, Research.nk.
9. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Zgodnie z art. 99 ogólnego rozporządzenia o ochronie danych rozporządzenie zastosowano od dnia 25 maja 2018 r. (Dz.U. L 119/43 z 4.5.2016, rozdz. 15), zob. bit.ly/rodo2016 (dostęp: 02.01.2019).
10. Rywczyńska A., Jaroszewski P. (2018), I*nternet zabawek – wsparcie dla rozwoju dziecka czy zagrożenie*, Warszawa: NASK – Państwowy Instytut Badawczy, zob. bit.ly/inzabaw (dostęp: 02.01.2019).
11. Sisik N., (2018), *Siła dziecięcych twórców na polskim YouTube*, w: Sotrender.com, zob. bit.ly/dziectw (dostęp: 02.01.2019).
12. Sotrender Research Team, zob. bit.ly/sotrrep (dostęp: 02.01.2019).
13. Ustawa z dnia 23 kwietnia 1964 r., Kodeks cywilny, (Dz.U z 1964 r. nr 16, poz. 93), zob. bit.ly/u640423 (dostęp: 02.01.2019).
14. Ustawa z dnia 6 czerwca 1997 r., Kodeks karny, (Dz.U. 1997 nr 88, poz. 553), zob. bit.ly/u970606 (dostęp: 02.01.2019).
15. Wardrop M., (2010), *Young will have to change names to escape 'cyber past' warns Google's Eric Schmidt*, w: „The Telegraph", Londyn, zob. bit.ly/2MKh1vX (dostęp: 02.01.2019).
16. Wieczorek M., (2018), *YouTube trends listopad 2018 – Nie zawsze warto budzić kontrowersje*, w: Sotrender.com, zob. bit.ly/2018ytt (dostęp: 02.01.2019).
17. Wójcik S., Makaruk K., (2014), *Seksting wśród polskiej młodzieży. Wyniki badania ilościowego*, Warszawa: Fundacja Dzieci Niczyje, s. 7–14, zob. bit.ly/sxtpolm (dostęp: 02.01.2019).

II.6. Zagrożenia informacyjne

/Maciej Kępka/

Liczba generowanych obecnie danych jest wręcz porażająca. Co sekundę w internecie pojawia się kilkadziesiąt gigabajtów nowych danych. Według opracowania firmy Domo (2017) *Data never sleeps 5.0* co minutę użytkownicy Instagrama publikowali 46 740 zdjęć, użytkownicy Snapchata – 527 760 zdjęć, a użytkownicy Twittera wysyłali 456 tys. tweetów. Dodając do tego filmy na YouTubie, serwisy informacyjne, blogi oraz posty na Facebooku, otrzymujemy nieustający potok danych, który przyrasta w niekontrolowany sposób.

Przy takim natłoku informacji kluczowe okazują się umiejętności krytycznego myślenia i selekcjonowania treści. Teoretycznie dostęp do wartościowych i sprawdzonych informacji jest nieograniczony, trzeba jednak umieć i chcieć je wyłuskać z bezkresu bezwartościowych (często fałszywych) treści. Mimo łatwego dostępu do naukowej wiedzy nadal dużą popularnością cieszą się teorie spiskowe, które dzięki internetowi mogą osiągać większy niż kiedykolwiek zasięg. Fałszywe informacje (ang. *fake news*) stały się skuteczną bronią stosowaną w walce politycznej i nie tylko.

Bardzo istotnym aspektem selekcjonowania informacji jest umiejętność rozpoznania przekazu reklamowego, który biorąc pod uwagę specyfikę nowych mediów czasami nie jest łatwo na pierwszy rzut oka zauważyć. Warto także znać specyfikę nowoczesnego marketingu i jego narzędzi, takich jak reklama wirusowa (*viral marketing*) czy remarketing.

Kolejnym zagadnieniem z zakresu zagrożeń informacyjnych jest plagiatowanie. Żyjemy w społeczeństwie, w którym nadal wiele osób akceptuje ściąganie i oszukiwanie, np. poprzez kopiowanie gotowych wypracowań z internetu. Takie prace często wykorzystywane są przez uczniów bez krytycznego podejścia.

Zupełnie innym zagadnieniem z tego obszaru jest pobieranie nielegalnych plików z internetu. Wydawać by się mogło, że w dobie popularności legalnych serwisów streamingowych ściąganie nielegalnych plików jest już przeszłością. Okazuje się jednak, że nadal wiele osób decyduje się na pobieranie pirackich filmów lub oprogramowania.

Jak widać, zagrożenia informacyjne to bardzo rozległy i złożony temat. Wszystkie wspomniane powyżej zagadnienia zostaną omówione w dalszej części tego

rozdziału. Choć publikacja dotyczy bezpieczeństwa dzieci i młodzieży w internecie, to problemy te w równym stopniu, a nieraz nawet większym, odnoszą się także do osób dorosłych.

Fałszywe informacje

Fake newsy to fałszywe informacje, które rozpowszechniane są w celu dezinformacji i manipulacji ludźmi. Zjawisko to od kilku lat jest przedmiotem wielu dyskusji, szczególnie w kontekście skutecznego przeciwdziałania gwałtownemu rozwojowi tego procederu. Specyfika internetu sprawia, że celowe rozprzestrzenianie nieprawdziwych informacji może być dużo łatwiejsze i tańsze, ale samo zjawisko nie jest niczym nowym. Narzędzie to wykorzystywane było od czasów starożytności. Fake newsy z dużą skutecznością stosowała także propaganda III Rzeszy, gdzie tworzono fałszywe informacje m.in. na temat Żydów w celu wywołania niechęci pozostałej części społeczeństwa do tej mniejszości. Propaganda odnosiła sukcesy i miała duży zasięg dzięki zaangażowaniu w nią rozbudowanych instytucji państwowych. Obecnie okazuje się, że można mieć wpływ na poglądy, a nawet zachowanie społeczeństwa przy wykorzystaniu znacznie mniejszych zasobów.

W 2016 r. głośno zrobiło się o tzw. fabryce trolli, mieszczącej się w Petersburgu. Troll to osoba, która swoimi działaniami – np. wpisami lub komentarzami – dąży do wywołania reakcji, np. kłótni. Troll często posługuje się fałszywymi informacjami, obraża, prowokuje tworzy kontrowersyjne treści. W tym przypadku zadaniem kilkuset pracowników było pisanie tysięcy komentarzy z zakładanych masowo fałszywych kont w serwisach Facebook i Twitter, tworzenie treści, które miały wpłynąć na zachowania ludzi w krajach zachodnich. Według badaczy z Uniwersytetu w Edynburgu co najmniej 419 kont starało się oddziaływać na brytyjską politykę (Wyborcza.pl, 2017). W dzień referendum dotyczącego brexitu zmobilizowanych zostało prawie 4 tys. fałszywych kont używanych przez trolli (Field, Wright, 2018). Takie działania mogły mieć realny wpływ na wyniki głosowania.

Jak zostało wskazane we wstępie rozdziału, uleganie fałszywym komunikatom i późniejsze ich rozpowszechnianie wcale nie są domeną jedynie młodych ludzi. Bardzo ciekawym przypadkiem rozprzestrzenienia się fałszywej informacji jest sprawa tzw. niebieskiego wieloryba. Na początku 2017 r. w polskim internecie pojawiły się wiadomości o tajemniczej i niebezpiecznej grze o nazwie *Niebieski wieloryb*. Miała to być gra, w której dzieci wykonują różne zagrażające ich życiu i zdrowiu zadania, np. samookaleczają się. Ostatnim etapem gry miało być samobójstwo. Zadania miał zlecać poznany przez internet opiekun. Według licznych prasowych doniesień ofiarami *Niebieskiego wieloryba* padło ponad 100 dzieci w Rosji. W Polsce wybuchła medialna panika. O grze informowały praktycznie wszystkie media. Przez kilka tygodni był to bardzo głośny temat. Sytuacja w mediach miała wpływ na rodziców i profesjonalistów. W szkołach organizowano apele, ostrzegano rodziców. Ostatecznie okazało się, że cała sprawa była typowym przykładem fake newsa. Jak było naprawdę? O przypadku samobójstwa dwóch dziewczynek napisał jeden rosyjski portal. Następnie wiadomość była bezrefleksyjnie przepisywana przez kolejne serwisy. Niestety polskie media także nie dotarły do prawdziwych źródeł tej wiadomości i powielały zmyślone informacje. Ostatecznie dorośli wykreowali problem, z którym trzeba było się następnie mierzyć. Bardzo dokładny opis tego incydentu można znaleźć na blogu *Mitologia Współczesna* (mitologiawspolczesna.pl) prowadzonym przez dr. Marcina Napiórkowskiego, specjalistę od mitów konsumenckich, legend miejskich i teorii spiskowych (Napiórkowski, 2017).

Podstawą w przeciwdziałaniu fake newsom jest nauczanie dzieci i młodzieży krytycznego podchodzenia do informacji, nie tylko w kontekście internetu.

Bańka informacyjna (filtrująca)

Obecnie dla wielu osób głównym źródłem informacji są wybrane serwisy internetowe i aplikacje. Rolę dzienników informacyjnych przejmują Facebook, Twitter oraz Google. Jedną z dużych zalet tego typu rozwiązań jest stworzenie własnego, zindywidualizowanego zestawu wiadomości (ang. *news feed*). Korzystając z Facebooka, możemy świadomie klikać „lubię to" na stronach, które chcemy śledzić. Dzięki temu dostaniemy to, co faktycznie nas interesuje. Niestety tego typu podejście ma także pewne wady. Internetowe narzędzia, korzystając ze stale zmieniających się algorytmów, bardzo precyzyjnie definiują nasze poglądy, zainteresowania. W rezultacie proponują nam to, co według algorytmu powinno nas zainteresować. Co istotne, są to algorytmy, których schemat działania jest dla nas całkowicie niejawny. W ten sposób częściowo świadomie, a częściowo nieświadomie zamykamy się w tzw. bańce filtrującej. Pojęcie to zostało spopularyzowane w 2011 r. przez Eliego Parisera, który opisał je w książce pt. *The Filter Bubble: What the Internet Is Hiding from You* (Pariser, 2011).

Bańka filtrująca to sytuacja, gdy jesteśmy zamknięci w kręgu podobnych opinii i interpretacji faktów. Będąc w bańce informacyjnej, nie możemy spojrzeć na konkretne wydarzenie lub problem z różnych perspektyw. Taka sytuacja może

mieć wpływ na pogłębianie się skrajnych poglądów i radykalizację. Przykładowo podczas kampanii wyborczej dotrą do nas tylko komunikaty od partii, która według algorytmu jest najbliższa naszym przekonaniom. Nie będziemy mieli natomiast możliwości, aby poznać punkt widzenia pozostałych stron.

Marketing internetowy

Internet pod wieloma względami łamie znane nam schematy poznawcze dotyczące reklam. Okazuje się, że reklama może być tam, gdzie kompletnie się jej nie spodziewamy. W telewizji i prasie przekaz reklamowy zebrany jest w odpowiednio oznaczonych blokach. W internecie często takiego oczywistego wyróżnienia nie ma. Należy być bardzo czujnym, aby zauważyć wszystkie momenty, gdy kierowany jest do nas przekaz reklamowy. Przykładowo w serwisie YouTube, który systematycznie wypiera telewizję, jeżeli chodzi o popularność wśród młodych ludzi (Wirtualnemedia.pl, 2016), często można natknąć się na lokowanie produktu. Młody użytkownik internetu nie wie, czy jego ulubiony youtuber pije dany napój, dlatego, że go lubi, czy dlatego, że ktoś mu za to zapłacił. Niektórzy youtuberzy co prawda zaznaczają, że dany odcinek sponsorowany jest przez konkretną firmę, ale nie jest to norma.

W kontekście marketingu bardzo istotna jest także świadomość działania darmowych usług internetowych. Twórcy poszczególnych aplikacji lub serwisów udostępniają ich zawartość tylko teoretycznie za darmo. Użytkownik nie płaci co prawda pieniędzy, ale zostawia swoje dane, które właściciel usługi może wykorzystać do prezentowania przekazu reklamowego. Można powiedzieć, że użytkownik niejako płaci za usługę swoimi własnymi danymi i dodatkowo godzi się na oglądanie reklamy. Bardzo istotne jest, by zgoda ta była w pełni świadoma, także w sensie rozumienia mechanizmów m.in. profilowania. Popularne serwisy społecznościowe, np. Facebook, zbierają o nas bardzo wiele danych, które umożliwiają tworzenie profili znacznie ułatwiających precyzyjne dostosowywanie reklam.

Poniżej kilka rodzajów przekazów marketingowych, które stosowane są w internecie:

1. Remarketing

Proszę wyobrazić sobie taką sytuację: młoda osoba chce kupić plecak na wyjazd w góry. Wpisuje w Google „plecak turystyczny", przeszukuje kilka sklepów internetowych, ale akurat żaden produkt nie wzbudza jej zainteresowania. Na drugi dzień włącza komputer, wchodzi na swoją ulubioną stronę, a tam… reklamy plecaków turystycznych. Przypadek? Oczywiście, że nie. W ten sposób działają nowoczesne systemy reklam banerowych. Wiedząc, czego aktualnie szukamy, system dobiera reklamy do naszych zainteresowań, dzięki czemu znacznie wzrasta prawdopodobieństwo kliknięcia w baner. Na tym właśnie polega remarketing.

2. Content marketing

Marketing treści polega na publikowaniu przez firmy treści, które mogą okazać się przydatne i wartościowe dla potencjalnego klienta. Mogą to być np. artykuły, które nie reklamują wprost danego produktu, tylko opisują jakąś kwestię lub problem. Przykładowo zamiast tworzyć artykuł wychwalający zalety konkretnego plecaka, marketingowiec może napisać, w jaki sposób dobrać plecak do swoich potrzeb oraz jak dobrze go wyregulować, dostosowując do swojej sylwetki. Taki artykuł może okazać się bardzo popularny i stanie się on często wyszukiwany przez użytkowników za pomocą np. Google. Dzięki temu użytkownik będzie naturalnie trafiał na stronę producenta lub stronę, gdzie reklamowane są właśnie te produkty.

3. Marketing wirusowy

Często mówi się o tzw. potencjale wirusowym treści, czyli o prawdopodobieństwie dalszego udostępniania, komentowania przez użytkowników serwisów społecznościowych itp. Marketing wirusowy korzysta z tych mechanizmów. Chodzi o wykreowanie takiej treści reklamowej, która będzie na tyle ciekawa, intrygująca lub kontrowersyjna, by użytkownicy internetu chcieli ją sami podawać dalej, np. zabawny spot reklamowy. Oprócz możliwości osiągnięcia dużego zasięgu takich treści z pewnością nie do przecenienia jest niski koszt ich rozpowszechniania.

Ściąganie plików z sieci

Ściąganie nielegalnych plików z internetu może się niektórym wydawać problemem z minionych już czasów. Okazuje się jednak, że w ostatnim roku popularność tzw. torrentów rośnie. Według raportu firmy Sandvine (2018 Internet Phenomena Report) przyczyną tego może być duże rozdrobnienie na rynku serwisów streamingowych. Pojawienie się Netflixa, Showmaxa i pozostałych tego typu serwisów nie przyczyniło się do zepchnięcia piractwa na margines. Okazuje się jednak, że dla wielu konsumentów problematyczne jest opłacanie abonamentów kilku platform jednocześnie. Sięgają więc do nielegalnych źródeł. Dotyczy to nie tylko filmów, ale także gier, muzyki oraz oprogramowania komputerowego.

Najpopularniejsze sposoby na pozyskiwanie tego typu treści to wyspecjalizowane serwisy, np. Chomikuj.pl, lub oprogramowanie umożliwiające wymianę plików pomiędzy komputerami użytkowników sieci P2P (ang. *peer-to-peer*), m.in. torrenty. Inną drogą rozpowszechniania nielegalnych kopii jest przekazywanie ich pomiędzy użytkownikami z wykorzystaniem fizycznych nośników, np. pendrive'ów.

Według polskiego prawa autorskiego (Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych) mamy prawo korzystać z już rozpowszechnionych utworów będących podmiotami prawa autorskiego – filmów, książek, muzyki – oraz dzielić się nimi w ramach „dozwolonego użytku osobistego" (art. 23 tej ustawy). Prawo to nie dotyczy jednak oprogramowania komputerowego, wyłączonego z art. 77 ustawy.

Zgodnie z art. 116 Ustawy o prawie autorskim i prawach pokrewnych rozpowszechnianie bez zezwolenia utworu objętego prawami autorskimi jest przestępstwem. Warto pamiętać, że sieci wymiany plików działają w taki sposób, że osoba pobierająca jest jednocześnie osobą udostępniającą. Dlatego korzystając z tego typu rozwiązań, praktycznie łamiemy prawo. Przestępstwo ścigane jest na wniosek poszkodowanego, ale właściciele praw, np. wytwórnie muzyczne, analizują internet pod kątem udostępniania ich utworów. Często nie są to działania masowe, ale może się zdarzyć, że akurat udostępniany przez nas plik znajdzie się na celowniku. Przykładem takiej sprawy są działania prokuratury w związku z udostępnieniem filmu *Wkręceni*. W 2016 r. zarekwirowano kilkaset komputerów w całej Polsce. Akcja była zainicjowana przez dystrybutora filmu, który dysponując jedynie numerami IP komputerów nielegalnie udostępniających film, zdecydował się na złożenie zawiadomienia do prokuratury. Sprawa była dość kontrowersyjna, ponieważ spowodowała zaangażowanie bardzo wielu policjantów w akcję zatrzymywania komputerów, ale pokazała, jak realnym zagrożeniem może być nielegalne ściąganie plików („Gazeta Finansowa", 2017).

Kolejnym istotnym problemem w tej materii jest ryzyko narażenia się na atak złośliwego oprogramowania. Pliki z nielegalnego źródła mogą być zarażone złośliwym kodem. Dodatkowo serwisy, w których użytkownicy szukają nielegalnych plików lub streamingu np. z wydarzeń sportowych, pełne są agresywnej reklamy. Mniej doświadczeni użytkownicy mogą zostać skutecznie wprowadzeni w błąd np. poprzez umieszczanie na banerze przycisku „pobierz", który może sugerować, że kliknięcie w baner rozpocznie pobieranie pliku. W rzeczywistości czynność taka przeniesie ich na kolejną stronę lub zainicjuje pobieranie potencjalnie niebezpiecznego oprogramowania.

Plagiatowanie

Plagiatowanie w pierwszej kolejności kojarzy się z pracami naukowymi lub ze sztuką. Biorąc jednak po uwagę powszechny dostęp do internetu, może ono dotyczyć także prac domowych, wypracowań kopiowanych przez dzieci i młodzież. Istnieje wiele wyspecjalizowanych serwisów, w których uczniowie mogą odrabiać swoje prace domowe poprzez powielanie gotowych odpowiedzi lub wprowadzanie swojego zadania i oczekiwanie, aż rozwiąże je ktoś inny. Dodatkowo częstą praktyką jest publikowanie rozwiązań prac domowych w klasowych grupach na Facebooku.

Plagiat to termin prawny określający przywłaszczenie autorstwa cudzego utworu, czyli wykorzystanie (np. skopiowanie, rozpowszechnienie) utworu i zaprezentowanie go jako własny. Plagiatowanie może wiązać się z odpowiedzialnością karną oraz cywilną. Ponadto konsekwencje plagiatowania mogą też być zawarte w regulaminie szkoły. Podczas pracy z młodymi osobami warto jasno podkreślać, że plagiat to nie tylko kopiowanie słowo w słowo, ale także zmienianie tekstu z wykorzystaniem innych słów, w sytuacji, gdy oddana jest ta sama treść oraz konstrukcja myślowa (Stanisławska-Kloc, 2011).

Szkoły mogą korzystać z systemów antyplagiatowych, które są w stanie wskazać podobieństwo pomiędzy analizowanym tekstem a tekstami znajdującymi się w internecie. Przykładem tego typu rozwiązania jest Antyściąga.pl lub Plagiat.pl. Takie narzędzia często są stosowane w przypadku prac dyplomowych na uczelniach wyższych, mogą jednak z powodzeniem wesprzeć nauczyciela, np. języka polskiego, podczas sprawdzania wypracowań.

Plagiatowanie w sposób oczywisty kojarzy się z nielegalną praktyką. Warto jednak zwrócić uwagę na ścisłe powiązanie kwestii plagiatowania z problemem bezkrytycznego podchodzenia do informacji znalezionych w internecie.

Pamiętaj!

- Podstawą przeciwdziałania większości zagrożeniom informacyjnym jest nauczanie młodzieży krytycznego podchodzenia do informacji, nie tylko tych znalezionych w internecie.
- Korzystaj z wartościowych scenariuszy zajęć lub innych materiałów na temat umiejętności krytycznego myślenia i weryfikacji danych (SciFun, 2016).
- Naucz dziecko korzystać z narzędzi służących do weryfikacji informacji znalezionych w internecie, np. zdjęć (odwrotne wyszukiwanie przez Images.google.com lub Tineye.com).
- Zwróć dziecku uwagę, że korzystając w swoim opracowaniu z gotowych materiałów, powinno powołać się na źródło, natomiast podczas stosowania cytatu należy podać źródło, autora oraz stronę, z której tekst został zaczerpnięty, jak również odpowiednio wyróżnić go w pracy.
- Uświadom dziecku, że plagiatem jest nie tylko kopiowanie z książek czy publikacji, lecz także korzystanie z prac znajdujących się w internecie.
- Zwróć uwagę, na jakie strony zagląda dziecko, odrabiając prace domowe, oraz w jaki sposób je wykorzystuje. W uzasadnionych przypadkach wyjaśnij, że dane zachowanie nosi znamiona plagiatu, opowiedz, na czym on polega i jakie mogą być jego konsekwencje.

Bibliografia

1. Barta J., Markiewicz R. (red.), (2013), *Prawo autorskie*. Warszawa: Wolters Kluwer Polska.
2. Domo, (2018), *Data never sleeps 5.0*, zob. bit.ly/datnevs (dostęp: 02.01.2019).
3. Czarnecki M., (2017), *Jak rosyjskie trolle wkręcały Brytyjczyków w sprawie brexitu i muzułmanów*, w: Wyborcza.pl, 15.11.2017 r., zob. bit.ly/rostrol (dostęp: 02.01.2019).
4. Field M., Wright M., (2018), *Russian trolls sent thousands of pro-Leave messages on day of Brexit referendum, Twitter data reveals*, w: „The Telegraph", 17.11.2018 r., zob. bit.ly/fake10m (dostęp: 02.02.2019).
5. Napiórkowski M., (2017), *Niebieski wieloryb. Krótko o nowej niebezpiecznej legendzie*, w: „Mitologia współczesna", blog z dnia 11.03.2017 r., zob. bit.ly/niebwie (dostęp: 02.01.2019).
6. Pariser E., (2011), *The Filter Bubble: What the Internet Is Hiding from You*, Nowy Jork: Penguin Press.
7. Pawelski Ł., (2017), *„Wkręceni we Wkręconych"*, w: „Gazeta Finansowa", 21.01.2017 r., zob. bit.ly/wkrecen (dostęp: 02.01.2019).
8. Sandvine, (2018), *The Global Internet Phenomena. Report October 2018*, w: Sandvine.com, zob. bit.ly/globinte (dostęp: 02.01.2019).
9. SciFun, (2016), *Krótki film o prawdzie i fałszu*, 5.03.2016 r., zob. bit.ly/prawdai (dostęp: 02.01.2019). Jest to blisko dwugodzinny materiał popularnonaukowego youtubera, który w bardzo przystępny sposób tłumaczy wiele skomplikowanych treści (np. istotę błędów procesu rozumowania, mechanizmy manipulacji). Por. materiały Centrum Edukacji Obywatelskiej stworzone w ramach projektu *Mind over media*, Polska Szkoła Krytycznego Myślenia, zob. bit.ly/ceo-mat (dostęp: 02.01.2019).
10. Stanisławska-Kloc S., (2011), *Plagiat i autoplagiat*, w: „Infos" nr 16 (108), s. 1–4, Warszawa: Wydawnictwo Sejmowe dla Biura Analiz Sejmowych, zob. http://bit.ly/autplgt (dostęp: 02.01.2019).
11. Szymielewicz K., Iwańska K. (red.), (2018), *Cyfrowa propaganda czy „normalna" polityczna polaryzacja? Studium debaty politycznej na polskim Twitterze (wrzesień – październik 2017)*, Warszawa: Fundacja Panoptykon.
12. Wirtualne media, (2016), *Dla młodych Facebook, YouTube i Twitter są ważniejszym źródłem informacji od telewizji. Raport*, w: Wirtualnemedia.pl, 16.06.2016 r., zob. bit.ly/tvamlod (dostęp: 02.01.2019).
13. Ustawa o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. (Dz.U. z 1994 r. nr 24, poz. 83), zob. bit.ly/ustprau (dostęp: 02.01.2019).

II.7. Zagrożenia technologiczne

/Andrzej Rylski/

Korzystanie z sieci oznacza kontakt z wieloma usługami i mechanizmami, z których istnienia typowy użytkownik nie zdaje sobie sprawy. Internet, który można obserwować na co dzień (strony internetowe oraz aplikacje), stanowi jedynie sposób prezentowania treści. Znaczna część cyberprzestrzeni pozostaje dla nas niedostępna. Wraz z rozprzestrzenieniem się usług internetowych na wszystkie niemalże dziedziny życia sieć globalna przestała być sferą specjalistów od komunikacji, stała się narzędziem uniwersalnym, wykorzystywanym przez przeciętnego użytkownika zarówno do pracy, nauki, jak i rozrywki. Podczas 22. konferencji Secure 2018, zorganizowanej przez NASK i CERT Polska w Warszawie 23–24 października 2018 r., podano, że ponad 90 proc. zagrożeń technologicznych nie dotyczy serwerów sieciowych, ale konsumenckich urządzeń podpiętych do internetu i aplikacji końcowego użytkownika (Sawczuk – F5 Networks, 2018). Dlatego w niniejszym rozdziale zostanie przybliżony temat przestępstw teleinformatycznych, które mogą zagrażać bezpieczeństwu wszystkich internautów, w tym również dzieci i młodzieży.

Złośliwe oprogramowanie (*malware*)

Nazwa „złośliwe oprogramowanie" – malware (od ang. *malware* stanowiącego połączenie słów *malicious*, złośliwe, i *software*, oprogramowanie) – oznacza różnego rodzaju szkodliwe programy/aplikacje i skrypty (fragmenty kodów) celowo działające na szkodę użytkownika systemu, przykładowo zmierzające do uszkodzenia systemu (Madej, Terlikowski, 2009).

Do malware należą wirusy, zwykle fragmenty kodu modyfikujące istniejące w systemie aplikacje wykonywalne, ale także makrowirusy, skrypty udające dodatkowe funkcje w dokumentach. Te ostatnie są uruchamiane przez popularne, cieszące się zaufaniem aplikacje (np. edytor tekstu). Nazwa „wirus" pochodzi od zdolności samodzielnego powielania się i zakażania kolejnych plików i komputerów, co zwykle prowadzi do ich zniszczenia. Działanie to może być zupełnie niezauważalne dla użytkownika. Tylko niektóre efekty działania wirusów mogą zostać zaobserwowane, często też z dużym opóźnieniem względem czasu infekcji. Inną kategorią malware są robaki (ang. *worms*), czyli samodzielne programy, często udające użyteczne aplikacje, generatory kodów, a nawet programy antywirusowe. Specjalnie spreparowane strony lub reklamy zachęcają do pobrania i uruchomienia ich, obiecując w zamian dostęp do wielu użytecznych funkcji. Tymczasem po włączeniu robaki zaczynają wprowadzać niepożądane zmiany w systemie. Szczególnym rodzajem złośliwego oprogramowania są tzw. konie trojańskie, potajemnie zmieniające ustawienia systemu w taki sposób, aby obniżyć odporność na ataki hakerów. Wyspecjalizowane malware typu backdoor potrafią przejąć kontrolę nad zainfekowanym przez siebie urządzeniem, np. uniemożliwiając użytkownikowi uruchamianie kluczowych dla bezpieczeństwa ustawień czy aplikacji.

Programy typu spyware pełnią funkcje szpiegowskie, pozyskując i przesyłając bez wiedzy użytkownika dane z jego systemu do twórców spyware. Groźną odmianą malware są ransomware. Programy tego typu blokują dostęp do plików użytkownika na urządzeniu, zwykle szyfrując je. Następnie wyświetlają monit żądający okupu (wpłaty środków) w zamian za udostępnienie hasła do odszyfrowania danych. Wiele firm decyduje się zapłacić cyberporywaczom za odzyskanie dostępu do swoich danych, przez co skala tego procederu narasta. Keyloggery potrafią z kolei odczytywać sekwencje wciskanych klawiszy, dzięki czemu przechwytują hasła wpisywane przez użytkownika (Białoskórski, 2011).

Złośliwe oprogramowanie jest wysyłane głównie w sposób automatyczny, masowo infekując komputery podłączone do internetu poprzez załączniki poczty elektronicznej. Oprócz wymienionych wcześniej skutków precyzyjnie zaplanowane ataki różnego typu malware są w stanie tworzyć całe botnety, czyli sieci komputerów zombie, służące hakerom na różne sposoby np. swoją mocą obliczeniową, do generowania wirtualnej waluty (Namiestnikow, 2009).

Objawy działania malware są różnorodne. Mogą to być: niechciane okna, które pojawiają się nieoczekiwanie na ekranie komputera lub urządzenia mobilnego, podmiana domyślnej strony przeglądarki internetowej, zmiana wyglądu pulpitu, „samoistne" pojawienie się nowych aplikacji. Często jednak, na co zwrócił uwagę zespół CERT Polska, efekty działania złośliwego oprogramowania są trudne do wykrycia nawet dla doświadczonego użytkownika, ponieważ do jedynych oznak zainfekowania urządzeń elektronicznych można zaliczyć np.: wolniejszą pracę komputera/telefonu, zacinający się system komputerowy, blokadę dostępu do niektórych plików czy zmianę ustawień systemu niezainicjowaną przez użytkownika (CERT Polska, 2017). Poniżej opisano metody ochrony przed działaniami typu malware:

1. Najlepszą obroną przed złośliwym działaniem wirusów jest posiadanie na każdym urządzeniu aktualnego oprogramowania, które chroni system i wykrywa złośliwe pliki.
2. Producenci oprogramowania na bieżąco ulepszają aplikacje, starając się naprawić wykryte niedoskonałości. Dlatego należy korzystać z opcji aktualizowania systemu i zainstalowanych w nim aplikacji. W szczególności nie należy używać starszych wersji przeglądarek internetowych. Okazuje się bowiem, że nawet bardzo krótkie korzystanie z nich może doprowadzić do zarażenia urządzenia różnymi malware.
3. Kluczowa jest regularna, najlepiej codzienna, aktualizacja baz danych programów antywirusowych. Każdego dnia bowiem pojawiają się nowe odmiany malware, a program ochronny będzie działał skuteczniej, wiedząc, jakich zagrożeń ma szukać.
4. Bardzo ważne jest utrzymywanie włączonej zapory sieciowej i opcji aktywnej ochrony w programie antywirusownym (skanowanie każdego otwieranego i zapisywanego w systemie pliku).
5. Do codziennej pracy na komputerze lepiej jest wykorzystywać konto zwykłego użytkownika, natomiast konto posiadające pełnię uprawnień administracyjnych lepiej zabezpieczyć mocnym hasłem i stosować tylko na potrzeby instalacji sprawdzonego i godnego zaufania oprogramowania.
6. Dobrym zwyczajem jest zachowanie dużej dozy podejrzliwości wobec wszystkich otrzymywanych plików, także tych przesyłanych przez znajomych, i upewnienie się, że zostają przeskanowane pod kątem obecności malware przed zapisaniem na dysku.
7. Poszukiwanie informacji oraz opinii przed pobraniem programu jest praktyką wysoce godną polecenia. Jeśli komentarze użytkowników na różnych stronach internetowych (np. forum dyskusyjne, recenzja na blogu poświęconym oprogramowaniu, grupa w sieci społecznościowej) są zgodne odnośnie do przydatności i nieszkodliwości działania danej aplikacji, wówczas należy poszukać zaufanego miejsca, skąd można pobrać oprogramowanie.
8. Szczególną ostrożność należy zachować wobec aplikacji pobieranych z innych stron internetowych niż oficjalna strona producenta danego oprogramowania. Istnieje ryzyko, że oprogramowanie umieszczone w innych miejscach mogło zostać „wzbogacone" szkodliwymi dodatkami, dlatego najlepiej pobrać je w oficjalnym sklepie czy witrynie producenta tego oprogramowania.
9. Przy dokonywaniu płatności w sieci (ale także podczas wprowadzania jakichkolwiek swoich danych, np. adresu e-mail) użytkownik powinien upewnić się, że strona internetowa, która przyjmuje jego dane, posiada włączone szyfrowanie i aktualny certyfikat (można to poznać po ikonie zielonej, zamkniętej kłódki obok adresu strony zaczynającego się od https, a nie jedynie http).
10. Współcześnie wiele programów posiada opcje pomagające chronić się przed złośliwym oprogramowaniem (np. przeglądarki internetowe umożliwiają blokowanie skryptów na stronach internetowych, a edytory tekstu oferują funkcję blokowania makr w plikach pakietu Office). Warto korzystać z tych opcji i wyłączać je jedynie w szczególnych przypadkach, gdy ma się pewność, że otwierane pliki lub strony internetowe są godne zaufania.

Metoda socjotechniczna – *phishing*

Znaczna część ataków w cyberprzestrzeni nie polega na aktywnym łamaniu zabezpieczeń ani angażowaniu szkodliwego oprogramowania. Obserwuje się natomiast szybko rosnącą liczbę ataków socjotechnicznych, które wykorzystują niewiedzę, nieuwagę lub rutynowe zachowanie użytkownika, aby nakłonić go do określonych działań, narażających bezpieczeństwo urządzenia lub konta. Popularną formą oszustw internetowych jest phishing (połączenie ang. słów *password harvesting* oraz *fishing* – łowienie haseł) (Grzelak, Liedel, 2012).

Sprawcy starannie preparują „zachętę", którą może być np. strona internetowa, wiadomość e-mail lub zwykła wiadomość przesyłana przez komunikator internetowy. Specyficzną cechą techniki phishingu jest wywołanie wrażenia pośpiechu, konieczności podjęcia natychmiastowego działania, które z reguły sprowadza się do kliknięcia w proponowany link. Cyberprzestępcy usiłują podszyć się pod godnego zaufania nadawcę, dlatego przedstawiają się jako np.:

- przedstawiciel banku (informujący o konieczności weryfikacji zabezpieczeń),
- dostawca mediów (przypominający o zaległości do zapłacenia i nalegający na pilne uiszczenie należności zgodnie z załączoną, fikcyjną fakturą),
- kurier (informujący o oczekującej przesyłce i proszący o potwierdzenie adresu dostawy),
- obcokrajowiec (proszący, często z wyraźnymi błędami w pisowni, o pomoc w odzyskaniu znacznych środków pieniężnych, a także obiecujący podzielenie się majątkiem),
- znajomy (przedstawiający się tylko popularnym imieniem, chcący podzielić się zdjęciami z wakacji i/lub zdjęciami o naturze intymnej i zachęcający do ich obejrzenia).

Po kliknięciu w proponowany link otwiera się strona, która często jest łudząco podobna do prawdziwej strony, za którą się podaje, lub nawet identyczna z nią. W istocie okazuje się jednak, że jest to inna strona, przygotowana przez przestępców (Nowak-Brzezińska, 2010). Aby uśpić czujność użytkownika na ekranie pojawia się typowa prośba o zalogowanie, po czym może wyskoczyć komunikat potwierdzający prawidłowość wykonanej czynności lub informacja o przerwie technicznej. Zdarza się też tak, że cyberprzestępcy poproszą o zainstalowanie dodatkowego oprogramowania, uzasadniając to koniecznością zaktualizowania certyfikatu lub dodania „kodeku" potrzebnego do obejrzenia zawartości. Wiele osób, kiedy widzi znajomo wyglądającą stronę, wprowadza na niej swoje prawdziwe dane uwierzytelniające i w ten sposób przekazuje je przestępcom. Uruchomienie proponowanego w takich sytuacjach programu (kodeku, rozszerzenia przeglądarki) zwykle kończy się zainstalowaniem szkodliwego oprogramowania, którego typowe rodzaje omówiliśmy wcześniej.

Skuteczność metod socjotechnicznych bierze się stąd, że opierają się one na zaufaniu, jakie internauci okazują znanym instytucjom lub osobom. Niejednokrotnie okazuje się, że użytkownicy sieci z pośpiechu lub lenistwa wolą jak najszybciej kliknąć w link/ikonę, zamiast zastanowić się, czy jest to działanie bezpieczne.
Skutecznym sposobem ochrony przed phishingiem jest:

- zachowanie spokoju i nieuleganie manipulacji,
- uważna i krytyczna analiza otrzymywanych wiadomości,
- powstrzymanie się od klikania w otrzymane linki przed potwierdzeniem ich wiarygodności (faktycznego adresu, do którego prowadzą),
- powstrzymanie się przed otwieraniem załączników, zanim zostaną sprawdzone przez program antywirusowy,
- zaniechanie otwierania na swoim komputerze przypadkowych nośników pamięci (pendrive'a, płyty, karty pamięci),
- nieudostępnianie swoich prywatnych danych logowania (np. loginu, hasła, kodu PIN) osobom trzecim,
- wykorzystywanie różnych kanałów komunikacji w przypadku konieczności podzielenia się danymi do logowania (np. przesłanie hasła oraz loginu).

Jeśli treść komunikatu nie jest typowa, a zwłaszcza jeśli nadawca żąda od użytkownika podjęcia niezwłocznej decyzji, prawdopodobnie mamy do czynienia z oszustwem. W przypadku pojawienia się jakichkolwiek wątpliwości należy wnikliwie sprawdzić wiarygodność otrzymanej informacji. W tym celu można wpisać lub wyszukać w przeglądarce prawdziwą witrynę internetową danej firmy bądź skontaktować się z firmą innym sposobem (np. poprzez infolinię, czat lub formularz kontaktowy zamieszczony na oficjalnej stronie). W żadnym razie nie

powinno się otwierać otrzymanego linku, który może prowadzić do fałszywej strony, jedynie imitującej oryginał, i stworzonej tylko po to, aby wyłudzić dane internauty lub zainfekować jego urządzenia.

W celu sprawdzenia wiarygodności linku można kliknąć prawym klawiszem myszy na frazę lub obrazek zawierające aktywny link i użyć funkcji kopiowania (w zależności od przeglądarki funkcja ta może brzmieć: „Kopiuj adres odnośnika", „Kopiuj łącze" lub „Kopiuj skrót"). Następnie można wkleić skopiowany link w bezpiecznym miejscu (np. programie Notatnik) i sprawdzić, jaką witrynę ten link otworzy. Niekiedy oszuści tworzą kopię strony, sprawiając, że wygląda ona identycznie jak oryginalna. Różnice mogą dotyczyć np. użycia innej litery w adresie www.

Bywa jednak i tak, że prawdziwa domena zostaje zamaskowana i użytkownicy widzą pozornie prawidłowy adres strony. Jeśli kliknie się w link, należy powstrzymać się przed podawaniem jakichkolwiek danych na stronie, zanim nie zweryfikuje się autentyczności witryny. Każda strona, która umożliwia logowanie, powinna posiadać adres zaczynający się od liter https. Na lewo od tego adresu przeglądarka wyświetla ikonę. Jeśli widać zamkniętą kłódkę (zielonego koloru), oznacza to, że strona posiada aktualny, szyfrowany certyfikat, potwierdzający jej autentyczność – innymi słowy, godny zaufania wystawca certyfikatu potwierdza, że dana strona jest tą, za którą się podaje.

Jeśli użytkownik jest przekonany, że otrzymana wiadomość to próba oszustwa, wówczas powinien zgłosić ten fakt administratorom oryginalnej strony, pod którą oszuści usiłowali się podszyć. W tym celu można się posłużyć danymi kontaktowymi dostępnymi na oficjalnej stronie.

Bardziej ukierunkowaną formą phishingu jest spear phishing, mający na celu włamanie do systemu konkretnej firmy. Typową taktyką jest podrzucenie na terenie lub w pobliżu tego przedsiębiorstwa spreparowanego nośnika (np. płyty, pendrive'a), łudząco przypominającego typowy nośnik stosowany przez firmę. Celem sprawców jest doprowadzenie do otworzenia zawartości nośnika na komputerze działającym w firmowej sieci. W ten sposób atak jest inicjowany przez nieświadomego pracownika. Cyberprzestępcy odwołują się do jego emocji (np. nazywając plik znajdujący się na nośniku „Zwolnienia planowane na rok…"). Uruchomienie takich treści może zainfekować system szkodliwym oprogramowaniem, a w efekcie zapewnić przestępcom dostęp do wewnętrznej sieci przedsiębiorstwa oraz do przechowywanych w niej danych.

Szeroko rozumiana profilaktyka cyberzagrożeń

Powszechnie znana zasada mówiąca o tym, że lepiej jest zapobiegać niż leczyć, pozostaje bardzo trafna w przypadku cyberzagrożeń. Oprócz konkretnych metod obrony przed cyberatakiem, które zaprezentowano powyżej, istnieje także kilka kwestii, o których warto pamiętać zawsze.

1. **Zasada ograniczonego zaufania.** Nawet jeśli użytkownik sieci otrzyma od znajomego wiadomość z linkiem (np. poprzez popularny komunikator), a wraz z nią propozycję zobaczenia czegoś interesującego (np. „Zobacz, to chyba twoje zdjęcie"), to jednak przed kliknięciem w link warto sprawdzić, czy na pewno nasz znajomy jest autorem tego komunikatu. W serwisach społecznościowych często dochodzi do przejęcia kont, a niechciane oprogramowanie potrafi wysyłać wiadomości e-mail z adresu internauty bez jego wiedzy. Jeśli zatem otrzymujemy wiadomość z łączem, warto przed otwarciem go zapytać, czy rzeczywiście została ona wysłana przez naszego znajomego. Dla pewności można zadać to pytanie poprzez inny kanał komunikacyjny niż ten, który dostarczył podejrzaną wiadomość, a więc np. przez telefon, SMS, e-mail, inny komunikator.

2. **Bezpieczne i zróżnicowane hasła.** Niemal każdy internauta ma wiele kont, z których większość wymaga stworzenia hasła. Ze względów bezpieczeństwa użytkownicy cyberprzestrzeni są zmuszeni do tworzenia długich haseł, złożonych z różnych liter, cyfr i znaków. Fakt ten nie ułatwia zapamiętania wszystkich haseł przez internautę, a jednocześnie przyczynia się do powszechnej, lecz szkodliwej praktyki nadawania tego samego hasła dla różnych kont i usług. W takiej sytuacji napastnik, który odgadnie lub wykradnie hasło internauty, będzie mógł bez trudu ukraść jego tożsamość w każdym z tych miejsc. Sposobem na stosowanie różnych, bezpiecznych haseł bez konieczności ich zapamiętywania jest aplikacja typu menadżer haseł (przechowująca wszystkie hasła użytkownika w postaci zaszyfrowanej, a także pozwalająca posłużyć się odpowiednim z nich po wpisaniu tylko jednego, głównego hasła). Inną metodą jest samodzielne stworzenie propozycji, nieskomplikowanej do zapamiętania, a trudnej do odgadnięcia dla systemu do tworzenia haseł. Przykładowo użycie pierwszych liter z cytatu dobrze znanego internaucie, dodanie ważnej dla niego liczby i znaku specjalnego oraz skrótu lub początku nazwy serwisu (związanego z nowym hasłem) – tworzą mocne hasło. Może być ono skutecznym sposobem na poradzenie sobie zarówno z natłokiem haseł do zapamiętania, jak i z ryzykiem włamania na konto. Jeśli natomiast pojawi się konieczność używania jednego hasła w wielu miejscach, wówczas należy postarać się przynajmniej stworzyć unikalne, osobne, trudne do odgadnięcia hasło dla poczty e-mail, której adres podaje się przy rejestracji w różnych serwisach. Wiadomość elektroniczna przesłana na nasz adres mailowy umożliwi odzyskanie hasła do pozostałych serwisów i usług, dlatego utrata dostępu do poczty może być dotkliwa dla internauty.

3. **Kopie bezpieczeństwa.** Przechowywanie swoich danych wyłącznie w jednym miejscu (np. na komputerze, w smartfonie) grozi tym, że w pewnym momencie (np. podczas awarii urządzenia lub ataku złośliwego oprogramowania) możemy je utracić. Cała praca, zdjęcia, filmy i inne ważne dane przechowywane na urządzeniu znikną – być może nieodwracalnie. Dlatego wszystkie pliki tworzone przez użytkownika, które w przyszłości mogą być przydatne, należy chronić poprzez regularne tworzenie kopii zapasowych. Proces ten nie musi być kłopotliwy ani czasochłonny. Wystarczy jednorazowo zainstalować odpowiednie oprogramowanie, w jego ustawieniach wskazać foldery, które powinny być archiwizowane, a następnie wybrać miejsce przechowywania kopii (najlepiej, aby był to zewnętrzny dysk lub dobrze zabezpieczona usługa sieciowa).

W przypadku dużej liczby danych, które rzadko są modyfikowane przez użytkownika (kolekcja filmów, zdjęć, muzyki), kopie zapasowe można robić ręcznie, po każdej większej zmianie (np. po przekopiowaniu na komputer zdjęć z wakacji). Z kolei dokumenty częściej modyfikowane, podręczne, te pliki, na których aktualnie się pracuje (pisma, arkusze, prezentacje, projekty), lepiej jest archiwizować po każdej zmianie. W automatycznym tworzeniu kopii takich plików pomoże **usługa typu chmura** (ang. *cloud*). Zainstalowanie odpowiedniego programu, np. Dropbox, Mega, Dysk Google, OneDrive czy iCloud, sprawi, że wszystkie pliki, jakie w nim umieścimy, będą dla nas dostępne z dowolnego urządzenia podłączonego do internetu. Każda zmiana w plikach spowoduje przesłanie aktualnej wersji plików do urządzeń synchronizowanych z chmurą. Przed wyborem konkretnego producenta i pakietu usługi chmurowej należy poznać dokładnie parametry oferowanych opcji. Wiele tego typu usług oferuje darmowy pakiet, który w zupełności wystarczy dla zwykłego użytkownika sieci. Niewielki limit miejsca na pliki nie będzie problemem, jeśli planuje się trzymać tam tylko aktualne, często zmieniane dane. Ciekawymi funkcjami oferowanymi

w ramach usługi chmury jest możliwość odzyskania usuniętych plików, a także, niezmiernie przydatna, historia wersji (chmura przechowuje wówczas nie tylko aktualną wersję każdego pliku, ale też wersje wcześniejsze, np. do miesiąca wstecz). Może być to ważne w sytuacji, gdy użytkownik omyłkowo dokona niepotrzebnych zmian (np. niechcący skasuje część treści w pliku, po czym zapisze zmianę i zamknie plik, a on zdąży się zsynchronizować z chmurą).

Pamiętaj!

- Zainstaluj program chroniący przed różnymi typami niechcianego oprogramowania (nie tylko wirusami) i ustaw jego regularne aktualizacje.
- Aktualizuj system i aplikacje – zwłaszcza przeglądarki internetowe.
- Nie otwieraj odruchowo łączy przesyłanych pocztą lub komunikatorami – najpierw sprawdź, kto i po co ci je wysyła, czy nie pochodzą od bota, czy ich adres prowadzi do godnej zaufania strony oraz czy plik nie zawiera niebezpiecznych niespodzianek.
- Nie instaluj żadnych aplikacji, rozszerzeń ani kodeków proponowanych przez strony lub usługi, do których nie masz pełnego zaufania.
- Nigdy nie wprowadzaj żadnych danych (np. e-maila, loginu, hasła, PINu czy kodu z tokena), jeśli strona nie potwierdza swojej autentyczności ważnym certyfikatem (adres strony zaczyna się od https i widać obok niego zamkniętą, zieloną kłódkę).
- Unikaj logowania się do swoich usług i podawania jakichkolwiek prywatnych danych w publicznych sieciach Wi-Fi, jeśli nie masz włączonej usługi VPN (Virtual Private Network).
- Na stronie banku, zaraz po zalogowaniu, nie powinna pojawić się prośba o dodatkowe podanie kodu. Kod uwierzytelnia zlecenie konkretnej czynności jak przelew lub zmiana danych. W razie wątpliwości skontaktuj się z infolinią swojego banku.
- Upewnij się, że smartfon, tablet i komputer są zabezpieczone trudnym do odgadnięcia hasłem lub kombinacją gestów, nie zostawiaj odblokowanego urządzenia bez nadzoru.
- Wyłącz pokazywanie podglądu wiadomości na zablokowanym ekranie lub wycisz powiadomienia od numeru swojego banku – tak aby osoby postronne nie mogły zobaczyć kodu autoryzującego operacje bankowe z wiadomości przychodzącej.

Bibliografia

1. Antkiewicz R., Dyk M., Kasprzyk R., Najgebauer A., Pierzchała D., Tarapata Z., Maj M., (2014), *Koncepcja rozwoju zdolności w obszarze cyberbezpieczeństwa infrastruktur krytycznych państwa, w: Bezpieczeństwo infrastruktury krytycznej. Wymiar teleinformatyczny. Raport Instytutu Kościuszki w ramach realizowanego projektu: Cel. Cyberbezpieczeństwo*, Kraków: Instytut Kościuszki, s. 93–102, zob. bit.ly/cbzpkrt (dostęp: 01.02.2019).
2. Barlińska J., Małecka A., Świątkowska J., (2018), *Cyberbezpieczeństwo. Charakterystyka, mechanizmy i strategie zaradcze w makro i mikro skali*, monografia, Warszawa: Texter.
3. Batorowska H., Musiał E. (red.), (2017), *Bezpieczeństwo informacyjne w dyskursie naukowym*, Kraków: Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie, Instytut Bezpieczeństwa i Edukacji Obywatelskiej, Katedra Kultury Informacyjnej i Zarządzania Informacją, zob. bit.ly/bezpinf (dostęp: 02.01.2019).
4. Białoskórski R., (2011), *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku*, Warszawa: Wyższa Szkoła Cła i Logistyki w Warszawie.
5. CERT Polska, (2017), *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny z działalności CERT Polska (2014–2017)*, zob. cert.pl/publikacje (dostęp: 02.01.2019).
6. Grzelak M., Liedel K., (2012), *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, w: „Bezpieczeństwo Narodowe", nr 22, II, zob. bit.ly/bezpcyb (zob. 02.01.2019).
7. Kamluk V., *Biznes botnetowy*, w: Kaspersky Lab, zob. bit.ly/bizbotn (dostęp: 02.01.2019).
8. Kasprzyk R., (2012), *Modele ewolucji systemów złożonych i metody badania ich charakterystyk dla potrzeb komputerowej identyfikacji potencjalnych sytuacji kryzysowych*, rozprawa doktorska, Warszawa: Wydział Cybernetyki, Wojskowa Akademia Techniczna.
9. Kijewski A, (2013), *CERT Polska vs botnety*, prezentacja wygłoszona podczas konferencji Secure 2013 w dniu 9 października 2013 r., CERT Polska, NASK: Warszawa, zob. bit.ly/certpvs (dostęp: 02.01.2019).
10. Madej M., Terlikowski M. (red.), (2009), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa: Polski Instytut Spraw Międzynarodowych.
11. Namiestnikow J., (2009), *Ekonomia botnetu*, w: Kaspersky Lab, zob. bit.ly/ekobotn (dostęp: 02.01.2019).
12. Nowak-Brzezińska A., (2010), *Zagrożenia i bezpieczeństwo komputerów i danych*, zob. bit.ly/zagrbez (dostęp: 02.01.2019).
13. Sawczuk M. (F5 Networks), (2018), *Czego powinny obawiać się twoje aplikacje*, prezentacja wygłoszona 23 października 2018 r. podczas Secure 2018, zob. bit.ly/s2018f5 (dostęp: 02.01.2019). Por. Sawczuk M. (F5 Networks), (2018), *Ataki webowe to nie tylko OWASP Top 10*, prezentacja wygłoszona 23 października 2018 r. podczas Secure 2018, zob. https://youtu.be/uu9BnbVMOng (dostęp: 02.01.2019).

Rozdział III.

Rozwiązania systemowe w profilaktyce i interwencji

/Anna Rywczyńska, Szymon Wójcik/

III.1. Pozytywna profilaktyka. Rola czynników chroniących

Aktywność w mediach cyfrowych to integralna część życia młodych ludzi, dotyczą jej więc te same procesy, które istnieją w świecie realnym. Obejmuje to również kwestie związane z typowymi dla okresu dojrzewania zachowaniami ryzykownymi, czyli niosącymi niebezpieczeństwo negatywnych konsekwencji (Szymańska, 2012).

Istniejąca wiedza na temat skutecznej ochrony przed zagrożeniami wskazuje na ogromną rolę rodziny, klimatu życia emocjonalnego młodych ludzi w relacjach rodzinnych, a także w środowisku szkolnym i rówieśniczym (Walęcka-Matyja, 2013). Warto zwrócić uwagę, że przez pojęcie klimatu emocjonalnego rozumie się „relacje między członkami danej społeczności i ich doznania spowodowane różnego typu zdarzeniami" (Sołowiej, 2003). Wśród zdefiniowanych czynników ryzyka i ochrony, które mogą wpłynąć na zwiększoną lub zmniejszoną podatność dzieci i młodzieży na zachowania ryzykowne, wymienia się trzy podstawowe obszary: więź z bliskimi, zainteresowanie edukacją szkolną i relacje ze środowiskiem rówieśniczym.

Według licznych badań zachowania ryzykowne najczęściej ze sobą współwystępują. Dzieci i młodzież znajdują się w podwyższonej grupie ryzyka. A działania ryzykowne, które młodzi internauci podejmują nie tylko w sieci, potwierdzają ich podatność na zagrożenia online (Lizut, Wrońska, 2018). Efektywna profilaktyka wymaga więc dużej uważności i otwartości na wszystkie obszary aktywności dziecka czy nastolatka.

We współczesnej literaturze przedmiotu funkcjonuje termin multiple literacy (ang. *multiple* – wielokryterialność, *literacy* – umiejętność pisania i czytania) jako ten właściwszy do opisania niezbędnych kompetencji (w przeciwieństwie do innego angielskiego obowiązującego terminu – media literacy, który oznacza umiejętność korzystania z mediów).

Multiple literacy odnosi się do kształcenia ogólnej umiejętności czytania, rozumienia, interpretowania i w dobie tak głębokiej integracji technologii cyfrowej z innymi dziedzinami życia wydaje się bardzo adekwatny i potrzebny, biorąc pod uwagę jego kompleksową koncepcję.

Umiejętne włączanie internetu do zajęć przedmiotowych, uczenie kompetencji cyfrowych w relacji do potrzeb, kładzenie nacisku na krytyczne podejście do informacji, wskazywanie na twórczy potencjał nowych technologii mogą odgrywać najistotniejszą rolę chroniącą dzieci i młodzież przed pułapkami globalnej sieci.

We współczesnej profilaktyce, niezależnie od obszaru, można wyróżnić dwa generalne podejścia: profilaktykę defensywną i pozytywną. Różnią się one diametralnie podejściem do problemu zagrożeń dla dzieci i młodzieży, choć w praktyce ich stosowanie nie musi się wykluczać.

Profilaktyka defensywna (Szymańska, Zamecka, 2002), inaczej eliminacyjna, polega na redukcji czynników ryzyka i w kontekście sieci może obejmować następujące działania: instalowanie programów filtrujących, zakaz korzystania z telefonów i internetu w szkole, kontrolę czasu przebywania w sieci oraz podejmowanych przez dziecko/młodzież aktywności, dostosowanie gier i aplikacji do wieku małoletnich osób.

Warto sobie uświadomić, że dobór działań i koncepcji profilaktycznych musi być dopasowany do wieku użytkowników. Eliminacja zagrożeń może być skuteczna w przypadku najmłodszych dzieci, natomiast nie sprawdzi się w przypadku nastolatków posiadających pełną niezależność w dostępie do internetu i sposobach korzystania z niego.

Profilaktyka pozytywna, nastawiona na wzmacnianie czynników chroniących (Ostaszewski, 2005), jest oparta na promocji konstruktywnego korzystania z sieci. Do niezbędnych elementów działań profilaktycznych na rzecz bezpieczeństwa w sieci w środowisku szkolnym zalicza się (Lizut, Wrońska, 2018):

1. Rozpoznanie – na podstawie dostępnych badań lub poprzez przeprowadzenie własnych w określonej placówce – obszaru funkcjonowania online wśród dzieci i młodzieży. Byłoby dobrze, gdyby dorośli (zarówno rodzice/opiekunowie prawni, jak i nauczyciele) systematycznie inicjowali dyskusje;

pogadanki z dziećmi i młodzieżą. W ten sposób wyrażą swoje zainteresowanie ich światem, aktywnościami prowadzonymi w sieci, a także obserwowanymi trendami. Rozmowa z najmłodszymi internautami pozwoli pozyskać od nich wiele ciekawych spostrzeżeń. Bardzo ważne jest dawanie młodym ludziom przestrzeni do rozmowy, refleksji oraz budowanie atmosfery opartej na zaufaniu, zachęcającej do dzielenia się swoimi doświadczeniami. Częstą barierą w szukaniu pomocy u dorosłych jest lęk przed krytyką oraz karami (np. odebraniem telefonu/laptopa i ograniczeniem dostępu do internetu). Trzeba sobie uzmysłowić, że jednorazowe spotkania profilaktyczne z ekspertami nie zastąpią stałej obecności problematyki bezpieczeństwa w sieci w środowisku domowym i szkolnym.

2. Niezbędnym elementem efektywnych działań profilaktycznych jest rozwijanie kompetencji kadry nauczycielskiej i pedagogicznej w zakresie metod i sposobu wykorzystywania internetu przez młodych ludzi. W odniesieniu do mediów cyfrowych szkolenie pedagogów i nauczycieli powinno mieć charakter wielopłaszczyznowy. Będzie to możliwe dzięki:
   - pogłębianiu wiedzy o zagrożeniach w sieci (np. udział w konferencjach, seminariach, szkoleniach),
   - wypracowaniu w placówkach procedur reagowania na incydenty (np. na przypadki cyberprzemocy) lub wdrożeniu już istniejących ustaleń,
   - rozwijaniu kompetencji cyfrowych umożliwiających wykorzystywanie rozwiązań online w edukacji, jak również zwiększających świadomość w zakresie urządzeń i usług wykorzystywanych przez młodych ludzi,
   - powołaniu w szkole/placówce szkolnej osoby wyznaczonej do reagowania na incydenty związane z działalnością młodych internautów w sieci (np. sytuacje cyberprzemocowe, przypadki sekstingu).

Aktywizacja rodziców

Za bezpieczeństwo i efektywne korzystanie z mediów cyfrowych przez dzieci i młodzież wspólną odpowiedzialność ponoszą rodzice i nauczyciele. To właśnie dorośli powinni wypracować wspólne i spójne zasady sprzyjające dobremu i mądremu korzystaniu z sieci przez najmłodszych jej użytkowników. Jednak stopień wykorzystania cyberprzestrzeni przez dzieci i nastolatków, zarówno pozytywny, jak i niosący ryzyko, ma bezpośredni związek z kapitałem kulturowym ich rodzin. Istotnym składnikiem każdego procesu wychowania jest towarzyszenie najmłodszym na każdym etapie rozwoju. A najbardziej skuteczną metodą wychowywania do odpowiedzialnego wykorzystania urządzeń elektronicznych jest współdziałanie rodziców i nauczycieli (Pyżalski, 2013). To zarówno postawa bliskich dorosłych (ich własny przykład), jak i określone działania wychowawcze decydują o tym, jaki jest poziom kompetencji medialnych dzieci i młodzieży. Niestety wyniki badań zgodnie potwierdzają jeden fakt: w dalszym ciągu temat bezpieczeństwa w sieci jest niedostatecznie obecny w domach (Orange Polska, 2016). Okazuje się, że aż 23 proc. rodziców w ogóle nie rozmawiało z dziećmi o bezpieczeństwie w internecie. Częstym powodem takiej sytuacji jest przekonanie dorosłych, że młodzi użytkownicy cyberprzestrzeni mają na ten temat większą wiedzę od nich. Dlatego niezbędnym elementem szkolnych programów profilaktycznych powinno być angażowanie rodziców we wspólne działania na rzecz bezpieczeństwa dzieci i młodzieży w sieci, a także szkolenie dorosłych w zakresie potencjalnych zagrożeń (np. podczas wywiadówek, spotkań z ekspertami).

Integracja środowiska szkolnego – wspieranie dobrego klimatu społecznego szkoły

W zakresie profilaktyki zachowań ryzykownych bardzo istotne jest, aby budować z uczniami przyjazne kontakty, zarówno w relacji uczeń – nauczyciel, jak również wewnątrz grupy rówieśniczej. Integraja uczniów (np. wspólne wyjścia, wycieczki, imprezy) połączona z brakiem obojętności na przejawy agresji i przemocy, a także dbałość o przeciwdziałanie wykluczeniu i uprzedzeniom mogą w znaczny sposób obniżyć potencjalne występowanie zachowań ryzykownych w danej grupie młodzieży.

Promocja konstruktywnego korzystania z sieci

Nauczyciele i rodzice, którzy zajmują się zachowaniami ryzykownymi online, muszą najpierw znać ich rzeczywiste przyczyny i konsekwencje. Tylko wówczas, kiedy ich działania wychowawcze nie będą się opierały na stereotypowych przesłankach (dostrzeganiu w sieci wyłącznie zagrożeń), skupią się na paradygmacie szans wynikających z korzystania młodych z cyberprzestrzeni (Pyżalski, 2013). Bardzo dobrą metodą profilaktyczną jest nakierowanie młodych na celowe i efektywne wykorzystywanie mediów cyfrowych, a także angażowanie uczniów w akcje promujące rozwój umiejętności cyfrowych, np. naukę kodowania, tworzenia blogów lub świadomego funkcjonowania w mediach społecznościowych, oraz zachęcanie do włączania się w akcje społeczne (np. Dzień Bezpiecznego Internetu).

Taki sposób aktywizowania dzieci i nastolatków może sprawić, że poczują się współodpowiedzialni za swoje działania w sieci, wykorzystanie jej potencjału, a nade wszystko za bezpieczeństwo własne i rówieśników w internecie.

Bibliografia

1. Lizut J., Wrońska A. (red.), (2018), *Rekomendacje dotyczące profilaktyki zachowań ryzykownych online*, w: *Standard bezpieczeństwa online placówek oświatowych*, wyd. II, Warszawa: NASK – Państwowy Instytut Badawczy i WSP im. Janusza Korczaka, s. 23–25, zob. bit.ly/stndbzp (dostęp: 02.01.2019).
2. Orange Polska, (2016), *Rodzice i dzieci wobec zagrożeń dzieci w Internecie.* Raport z badania przygotowany przez TNS Polska S.A. na zlecenie Orange Polska, we współpracy z Fundacją Orange i Fundacją Dajemy Dzieciom Siłę, zob. bit.ly/rdwzagr (dostęp: 02.01.2019).
3. Ostaszewski K., (2005), *Druga strona ryzyka*, „Remedium", nr 2, s. 102, 144.
4. Pyżalski J., (2013), *Rodzina i szkoła a przeciwdziałanie zaangażowaniu młodych ludzi w ryzykowne zachowania online*, w: „Dziecko krzywdzone. Teoria, badania, praktyka", t. 12 (1), s. 99–109, zob. bit.ly/rodziszk (dostęp: 02.01.2019).
5. Sołowiej J., (2003), *Rodzina osób twórczych*, w: *Psychologia w służbie rodziny*, I. Janicka, T. Rostowska (red.), Łódź: Wydawnictwo Uniwersytetu Łódzkiego, s. 58.
6. Szymańska J., (2012), *Programy Profilaktyczne. Podstawy profesjonalnej psychoprofilaktyki*, Warszawa: Ośrodek Rozwoju Edukacji, zob. bit.ly/podprops (dostęp: 02.01.2019).
7. Szymańska J., Zamecka J., (2002), *Przegląd koncepcji i poglądów na temat profilaktyki*, w: *Profilaktyka w środowisku lokalnym*, Świątkiewicz G. (red.), Warszawa: Krajowe Biuro do spraw Przeciwdziałania Narkomanii, s. 19–32.
8. Walęcka-Matyja K., (2013), *Jakość klimatu emocjonalnego rodzin pochodzenia adolescentów jako predykator ich kompetencji emocjonalnych*, „Studia Dydaktyczne", nr 24–25, Łódź: Uniwersytet Łódzki, s. 273–287, zob. bit.ly/klemoro (dostęp: 02.01.2019).

III.2. Procedury przeciwdziałania oraz reagowania na przypadki zagrożeń związanych z aktywnością dzieci online

Nawet najlepiej realizowana profilaktyka nie wyeliminuje całkowicie występowania niebezpiecznych sytuacji w internecie. W praktyce z takimi zagrożeniami stykają się uczniowie każdej polskiej placówki edukacyjnej. W związku z tym niezwykle ważnym elementem szkolnego systemu bezpieczeństwa jest odpowiednie reagowanie na sytuacje zagrożenia ucznia w sieci.

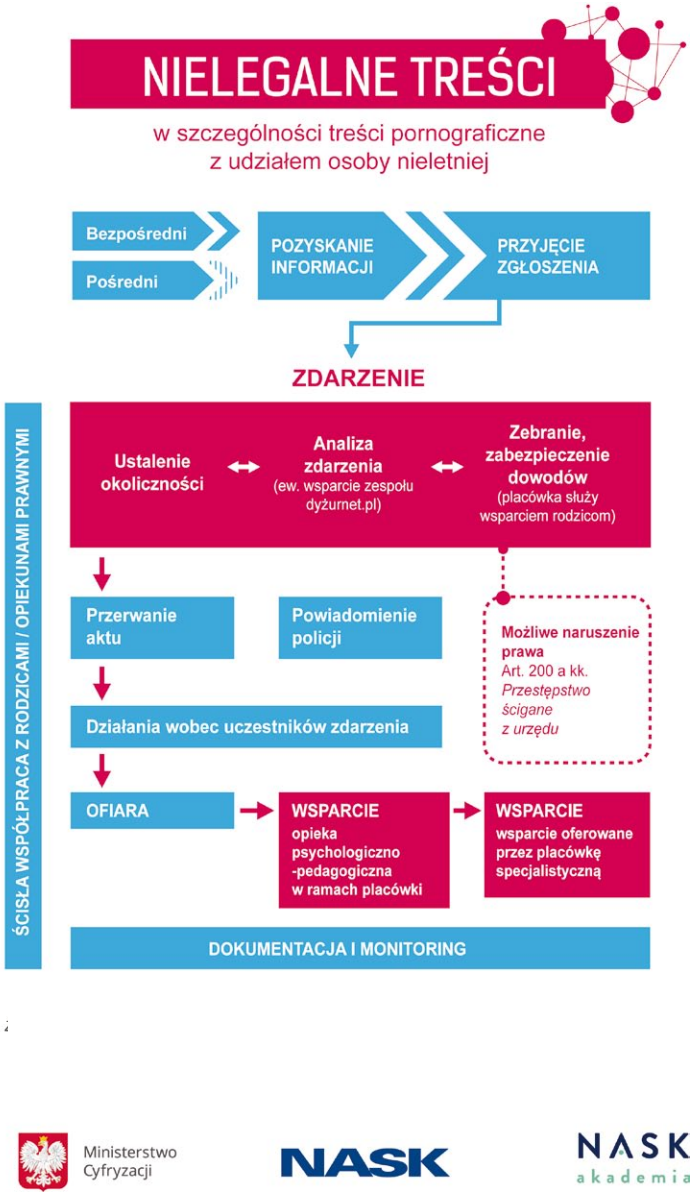
Szkoła powinna opracować procedury reagowania na takie sytuacje. Poza tym zadaniem tego miejsca jest interweniowanie w każdym przypadku ujawnienia lub podejrzenia zagrożenia wynikającego z korzystania przez uczniów z mediów elektronicznych. Procedury reagowania, spisane i rozpowszechnione wśród personelu szkolnego, muszą klarownie informować, w jaki sposób i kiedy pracownicy szkoły (dyrekcja, nauczyciele i pedagodzy) powinni postępować zarówno z ofiarami internetowych zagrożeń, jak i – w zależności od specyfiki zdarzenia – z ich sprawcami, świadkami oraz rodzicami. Zasady takie mogą być przygotowane w gronie pedagogicznym (dyrekcja i nauczyciele) przy ewentualnym udziale zewnętrznych konsultantów. A nade wszystko opracowane metody postępowania powinny być dostosowane do realiów danej placówki edukacyjnej. Nie sposób przecenić w tym przypadku roli pedagoga szkolnego, psychologa i opiekuna szkolnej pracowni komputerowej. Trzeba też pamiętać o funkcji, jaką w ustalaniu i realizacji procedur profilaktycznych pełnią wychowawcy klas. Przecież to właśnie oni każdego dnia mają lub mogą mieć kontakt z problemami swoich wychowanków, które są związane z ich obecnością w internecie.

Zasady reagowania na sytuacje zagrożenia w sieci powinny uwzględniać kilka kluczowych elementów, np.: udzielenie wsparcia ofierze oraz innym osobom biorącym udział w zdarzeniu (zarówno świadkom, jak i sprawcy, którym w większości przypadków jest również osoba niepełnoletnia, niejednokrotnie wymagająca opieki psychologicznej). Dobre praktyki szkolne muszą także zawierać wskazówki dotyczące ustalenia i dokumentowania przebiegu całej sytuacji, angażowania rodziców w rozwiązanie problemu oraz ewentualnego wsparcia instytucji zewnętrznych (zarówno poradni psychologiczno-wychowawczej, jak i – w poważniejszych przypadkach – organów prawnych).

Podjęcie decyzji o zgłoszeniu obaw lub podejrzeń dotyczących krzywdzenia dzieci i młodzieży w sieci bywa niezwykle trudne. Dzięki opracowaniu odpowiedniego sposobu postępowania w takiej sytuacji wszyscy powinni mieć jasność, jak należy się zachować. Każde domniemanie lub podejrzenie krzywdzenia młodego internauty należy potraktować poważnie. Dlatego tak istotne jest, aby osoby zgłaszające takie przypadki przestrzegały ściśle określonej procedury. W szczególności należy zadbać o kwestie związane z poufnością i przekazywaniem informacji. Warto także korzystać z dostępnych sposobów reagowania na następujące sytuacje kryzysowe w internecie: cyberprzemoc (w odniesieniu do sprawców, ofiar i świadków), seksting, uwodzenie w sieci (grooming), kontakt ze szkodliwymi treściami, nadużywanie internetu.

Metody reagowania na przypadki zagrożenia w sieci, które może dotknąć dzieci i nastolatków, omówiono wnikliwie w wielu publikacjach, m.in. w kursie e-learningowym *Bezpieczeństwo dzieci i młodzieży online. Kurs dla profesjonalistów* (edukacja.fdds.pl – Platforma edukacyjna Fundacji Dajemy Dzieciom Siłę, 2016), a także w najnowszym wydaniu publikacji *Standard bezpieczeństwa online placówek oświatowych* (Akademia NASK, 2018).

Rys. 3. Przykładowa procedura reagowania na przypadek związany z nielegalnymi treściami



Ministerstwo Cyfryzacji NASK NASK akademia

Źródło: Standard bezpieczeństwa online placówek oświatowych, NASK, Warszawa 2018, s. 45 (opracowanie Z. Polak, A. Wrońska)

Bibliografia

1. Akademia NASK, (2018), *Standard bezpieczeństwa online placówek oświatowych*, wydanie II uzupełnione (wydanie I przygotowane zostało w ramach zleconego przez Ministerstwo Cyfryzacji i Administracji zadania publicznego „Działania na rzecz bezpiecznego korzystania z internetu" realizowanego przez Fundację Odkrywców Innowacji oraz Fundację Drabina Rozwoju), Warszawa: NASK – Państwowy Instytut Badawczy i WSP im. Janusza Korczaka, zob. http://bit.ly/stndbzp (dostęp: 02.01.2019).
2. Ostaszewski K., (2005), Druga strona ryzyka, w: „Remedium", nr 2, s. 102, s. 144.
3. Platforma edukacyjna Fundacji Dajemy Dzieciom Siłę, (2016), *Bezpieczeństwo dzieci i młodzieży online. Kurs dla profesjonalistów*, w: Platforma edukacyjna dla profesjonalistów na temat ochrony dzieci i młodzieży przed przemocą, zob. edukacja.fdds.pl/? link=15587 (dostęp: 02.01.2019).
4. Pyżalski J., (2013), *Rodzina i szkoła a przeciwdziałanie zaangażowaniu młodych ludzi w ryzykowne zachowania online*, w: „Dziecko krzywdzone. Teoria, badania, praktyka", t. 12 (1), s. 99–109, zob. bit.ly/rodziszk (dostęp: 02.01.2019).
5. Sołowiej J., (2003), *Rodzina osób twórczych*, w: *Psychologia w służbie rodziny*, I. Janicka, T. Rostowska (red.), Łódź: Wydawnictwo Uniwersytetu Łódzkiego, s. 58.
6. Szymańska J., (2012), *Programy profilaktyczne. Podstawy profesjonalnej psychoprofilaktyki*, Warszawa: Ośrodek Rozwoju Edukacji, zob. bit.ly/podprops (dostęp: 02.01.2019).
7. Szymańska J., Zamecka J., (2002), *Przegląd koncepcji i poglądów na temat profilaktyki*, w: *Profilaktyka w środowisku lokalnym*, Świątkiewicz G. (red.), Warszawa: Krajowe Biuro do Spraw Przeciwdziałania Narkomanii, s. 19–32.
8. Walęcka-Matyja K., (2013), *Jakość klimatu emocjonalnego rodzin pochodzenia adolescentów jako predykator ich kompetencji emocjonalnych*, w: „Studia Dydaktyczne", nr 24–25, Łódź: Uniwersytet Łódzki, s. 273–287, zob. bit.ly/jklemor (dostęp: 02.01.2019).

III.3. Przegląd wybranych materiałów edukacyjnych PCPSI

Materiały skierowane do dzieci

- **Pakiet edukacyjny *Przygody Plika i Foldera w sieci*, zob. bit.ly/plifold**

Serie filmów *Przygody Plika i Foldera w sieci*, *Plik i Folder na ścieżkach internetu*, a także audiobook *Poznaj internet*, scenariusze zajęć dla nauczycieli i zeszyt ćwiczeń dla dzieci dostępne są w postaci elektronicznej oraz jako płyty DVD.

- **Pakiet edukacyjny *Owce w sieci*, zob. pl.sheeplive.eu**

Scenariusze zajęć z wykorzystaniem serii trzyminutowych kreskówek, których celem jest edukacja na temat zagrożeń związanych z korzystaniem przez dzieci z internetu, telefonów komórkowych i innych nowych technologii. Filmy odwołują się do motywów ludowych i bajkowych, ale odzwierciedlają również współczesną kulturę dziecięcą i młodzieżową oraz obecny styl życia. Zakończenie każdej bajki zawiera morał, mówiący, jak uniknąć zagrożeń. Pakiet jest dostępny na stronie.

- **Projekt edukacyjny *Necio.pl*, zob. necio.pl**

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

- **Projekt edukacyjny *Sieciaki.pl*, zob. sieciaki.pl**

Projekt edukacyjny skierowany do dzieci w wieku 6–12 lat. Jego celem jest edukowanie dzieci na temat bezpiecznego korzystania z internetu oraz profilaktyka zagrożeń online. Projekt obejmuje serwis edukacyjny dla dzieci, kurs e-learningowy i scenariusze zajęć lekcyjnych. Prowadzona jest także edukacyjna akcja wakacyjna.

- **Projekt edukacyjny *Kursor*, zob. edukator.pl**

Moduł programu obejmuje cykl działań dla uczniów szkół podstawowych i średnich. W skład materiałów multimedialnych wchodzą: filmy animowane, spoty promujące bezpieczne zachowania w sieci, gra fabularna, a także prezentacje i wykłady.

- **Zajęcia lekcyjne *Gdzie jest Mimi*?, zob. edukacja.fdds.pl**

Scenariusz zajęć dla uczniów klas V–VII szkół podstawowych. Celem zajęć jest poszerzenie wiedzy uczniów na temat cyberprzemocy, jej konsekwencji i roli świadków sytuacji związanych z cyberprzemocą. Zajęcia na podstawie filmu edukacyjnego *Gdzie jest Mimi*.

- **Zajęcia lekcyjne *Lekcja bezpieczeństwa*, zob. edukacja.fdds.pl**

Scenariusz zajęć dla uczniów klas V–VII szkół podstawowych. Celem zajęć jest podniesienie poziomu wiedzy uczniów na temat zagrożeń prywatności w sieci. Zajęcia prowadzone z wykorzystaniem edukacyjnego materiału filmowego.

- **Zajęcia lekcyjne *Internet bez hejtu*, zob. edukacja.fdds.pl**

Scenariusz zajęć dla uczniów klas IV–VI szkół podstawowych. Celem zajęć jest uwrażliwienie młodych ludzi na problem obrażania w internecie. Zajęcia oparte na projekcji filmu *Dodaj znajomego*.

- **Zajęcia lekcyjne *Zamiast hejtu*, zob. edukacja.fdds.pl**

Scenariusz zajęć dla uczniów klas VII–VIII szkół podstawowych. Celem zajęć jest zapoznanie uczniów z pojęciami „hejtowanie" i „mowa nienawiści", omówienie sposobów reagowania ofiary oraz świadka, a także kształtowanie i promowanie postaw empatycznych. Zajęcia na podstawie filmu edukacyjnego *Dodaj znajomego*.

Materiały skierowane do młodzieży

- **Projekt edukacyjny *Digital Youth*, zob. digitalyouth.pl**

Projekt skierowany do młodych i przez nich współtworzony. Dotyczy pozytywnego i kreatywnego wykorzystania nowych technologii oraz bezpieczeństwa online. Składa się z bloga Digitalyouth.pl, profilu na Facebooku, papierowego magazynu, corocznej konferencji Digital Youth Forum oraz spotkań i warsztatów dla młodzieży.

- **5 porad na piątkę!, zob. https://akademia.nask.pl**

Seria pięciu ulotek, które w przystępny sposób omawiają sposoby radzenia sobie z zagrożeniami w sieci:
1. *Jak sobie radzić z cyberprzemocą*, zob. bit.ly/pnpcyb1
2. *Jak możesz pomóc ofiarom cyberprzemocy*, zob. bit.ly/pnpcyb2
3. *Pięć kroków do prywatności*, zob. bit.ly/pnppryw
4. *FOMO – jak sobie z tym radzić*, zob. bit.ly/pnpfomo
5. *Emoji – wyraź siebie*, zob. bit.ly/pnpemoj.

- **Przewodnik *Wizerunek online w wakacje*, zob. bit.ly/wizonlw**

Przewodnik Akademii NASK pozwala młodzieży utrwalać miłe chwile i dzielić się z innymi wakacyjnymi wrażeniami, które pozostawią tylko dobre wspomnienia. Publikacja uświadamia młodym internautom, że publikując różne treści w sieci, kreują swój wizerunek na stałe. Przewodnik pomaga nastolatkom zadbać o to, aby zamieszczanie zdjęć i filmów z wakacyjnych przygód w sieci nie miało dla nich negatywnych konsekwencji. Ta publikacja jest częścią akcji Urzędu Ochrony Konkurencji i Konsumentów *Przed wakacjami – co warto wiedzieć?*.

- **Ulotka *Bezpieczne wakacje. Pięć porad dla nastolatków*, zob. bit.ly/waknast**

Ulotka skierowana do nastolatków zawierająca porady dotyczące urządzeń mobilnych i prywatności w kontekście wyjazdów wakacyjnych.

- **Zeszyt ćwiczeń *Web We Want. Internet, jakiego chcemy*, zob. www.webwewant.eu**

Edukacyjny zeszyt ćwiczeń dotyczący bezpiecznego, twórczego i odpowiedzialnego korzystania z internetu. Przeznaczony jest dla nastolatków w wieku 13–16 lat . Publikacja została stworzona przy współudziale młodych ludzi z całej Europy i jest dostępna w ośmiu językach. Zawarte w niej praktyczne ćwiczenia pomagają rozwijać umiejętności bardziej świadomego i odpowie-dzialnego korzystania z sieci.

- **Program profilaktyczny IMPACT, zob. impact.fdds.pl**

Program IMPACT (Interdyscyplinarny Model Przeciwdziałania Agresji i Cyberprzemocy Technologicznej) to kompleksowa propozycja profilaktyki cyberprzemocy skierowana do uczniów klas VI–VIII szkół podstawowych. Program został

opracowany przez Fundację Dajemy Dzieciom Siłę z udziałem naukowców i ekspertów z zakresu psychologii, pedagogiki oraz bezpieczeństwa informacyjnego. Składa się z cyklu dziewięciu lekcji mających formę warsztatów, podczas których młodzież pracuje nad rozwijaniem kompetencji, które przyczyniają się do ograniczenia przemocy i zwiększenia bezpieczeństwa uczniów w sieci. Oprócz scenariuszy zajęć program obejmuje podręcznik, materiały filmowe oraz prezentacje i narzędzia multimedialne.

- **Zajęcia lekcyjne *Przygody Fejsmena*, zob. edukacja.fdds.pl**

Scenariusz zajęć dla uczniów klas VII–VIII szkół podstawowych. Celem zajęć jest poszerzenie wiedzy uczestników o podstawowych zasadach bezpieczeństwa podczas korzystania z mediów elektronicznych i serwisów społecznościowych oraz wskazanie sposobów reagowania na niebezpieczne sytuacje online. Zajęcia oparte są na materiałach filmowych.

- **Zajęcia lekcyjne *Dzień z życia*, zob. edukacja.fdds.pl**

Scenariusz zajęć dla uczniów w wieku 13–15 lat poświęconych problemowi nadmiernego korzystania z internetu. Celem zajęć jest przekazanie wiedzy na temat zagrożeń płynących z nadużywania internetu i komputera (w tym gier).

- **Zajęcia lekcyjne *Uważni online*, zob. edukacja.fdds.pl**

Scenariusz zajęć przeznaczonych dla młodzieży w wieku 12–15 lat. Celem zajęć jest zapoznanie uczestników ze zjawiskiem uwodzenia online, przekazanie wiedzy na temat sposobów weryfikowania kontaktów sieciowych oraz zachęcenie do szukania pomocy w trudnych sytuacjach.

- **Zajęcia lekcyjne *Rozumiem i wybieram*, zob. edukacja.fdds.pl**

Scenariusze zajęć dla uczniów szkół podstawowych w wieku 11–14 lat oraz uczniów szkół ponadpodstawowych w wieku 15–18 lat. Celem zajęć dla uczniów młodszych jest uświadomienie uczestnikom, że nie wszystkie treści w internecie są prawdziwe, a kontakt z niektórymi z nich może być szkodliwy. Zajęcia dla szkół ponadpodstawowych mają uświadomić uczestnikom, jakie wartości są ważne w bliskich związkach między dwojgiem ludzi oraz skąd mogą czerpać rzetelną wiedzę na ten temat. Uczniowie dowiedzą się, w jakim celu powstają materiały pornograficzne oraz tego, że nie są one właściwym źródłem wiedzy o seksualności, a ich oglądanie może negatywnie wpływać na funkcjonowanie człowieka.

- **Zajęcia lekcyjne *Seksting*, zob. edukacja.fdds.pl**

Scenariusz zajęć dla młodzieży w wieku 13–18 lat. Celem zajęć jest wskazanie potencjalnie negatywnych konsekwencji wykonywania, przesyłania czy komentowania w sieci materiałów o charakterze seksualnym oraz zwrócenie uwagi uczestników na umiejętność dokonywania odpowiedzialnych wyborów, a także wskazanie im miejsc, w których mogą szukać pomocy w trudnych sytuacjach. W zajęciach jest wykorzystywany film edukacyjny *Na zawsze*.

- **Zajęcia lekcyjne *Mój wizerunek online*, zob. edukacja.fdds.pl**

Scenariusz zajęć dla uczniów klas VII–VIII szkół podstawowych. Celem zajęć jest poszerzenie wiedzy uczestników o zagrożeniach związanych z nierozważnym korzystaniem z internetu oraz omówienie zasad świadomego i rozważnego prezentowania się online.

Materiały skierowane do dorosłych

- **Scenariusze zajęć *Lubię To! Nastolatki w mediach społecznościowych*, zob. bit.ly/msp1315 oraz bit.ly/msp1618**

Publikacja składa się z dwóch zeszytów przeznaczonych do zajęć z młodzieżą w wieku 13–15 oraz 16–18 lat. Scenariusze mają wspomóc nastolatków w odkrywaniu korzyści związanych z użytkowaniem internetu i serwisów społecznościowych. Dzięki tym materiałom młodzież dowie się, jak świadomie i krytycznie korzystać z zasobów informacyjnych internetu, jak dbać o swój wizerunek w sieci, a także jak wykorzystywać możliwości mediów społecznościowych w projektach edukacyjnych i działaniach prospołecznych. W publikacji poruszono wiele ciekawych zagadnień, np.: cyfrowa tożsamość, budowanie wizerunku w mediach społecznościowych i zarządzanie nim, krytyczne podejście do informacji i postaw promowanych przez serwisy społecznościowe, przeciwdziałanie cyberprzemocy, prospołeczne wykorzystanie mediów społecznościowych w szkole/placówce edukacyjnej.

- **Przewodnik dla rodziców *Internet zabawek. Wsparcie dla rozwoju dziecka czy zagrożenie*, zob. bit.ly/inzabaw**

Publikacja przybliża zagadnienie najnowszej generacji zabawek komunikujących się z internetem, przynależnych do dziedziny IOT – Internet of Things. Eksperci NASK skupiają się w niej na przystępnym zaprezentowaniu wyników badań jakościowych i ilościowych dotyczących rozpowszechnienia tych zabawek w Polsce oraz ich podatności na cyberataki, ponadto służą radą, jak korzystać z nich bezpiecznie i z poszanowaniem prywatności dzieci. Książka ta jest przewodnikiem dla rodziców i opiekunów rozważających zakup inteligentnej zabawki.

- **Poradnik dla nauczycieli *Media społecznościowe w szkole*, zob. bit.ly/mspolsz**

Poradnik dla nauczycieli stawiających pierwsze kroki w mediach społecznościowych. Publikacja podejmuje tematykę bezpiecznego i odpowiedzialnego korzystania z mediów społecznościowych w szkole, prezentuje najpopularniejsze serwisy oraz wskazuje przykłady praktycznego ich wykorzystania w klasie.

- **Publikacja *Standard bezpieczeństwa online placówek oświatowych*, wydanie II, zob. bit.ly/stndbzp**

Opis standardów, jakie powinna spełniać placówka oświatowa w zakresie bezpieczeństwa online. Rozszerzona edycja wydawnictwa z 2015 r. opracowanego na zlecenie Ministerstwa Administracji i Cyfryzacji w ramach projektu *Działania na rzecz bezpiecznego korzystania z internetu*. Publikacja została przygotowana przez zespół ekspertów NASK – Państwowego Instytutu Badawczego i Wyższej Szkoły Pedagogicznej im. Janusza Korczaka w Warszawie.

- **Publikacja *Nastolatki wobec internetu*, zob. bit.ly/naswobi**

Publikacja podsumowuje wyniki badań z 2016 r. na temat aktywności nastolatków w internecie, edukacyjnej roli sieci i urządzeń mobilnych, przyjmowanej przez młodzież sieciowej tożsamości, zachowań małoletnich użytkowników internetu, świadomości zagrożeń i sposobów reagowania na przemoc.

- ***Poradnik nie tylko dla rodziców. Dzieci w świecie gier komputerowych*, zob. bit.ly/dzwswgk**

Poradnik dokładnie zapozna rodziców i nauczycieli ze światem gier – z ich typami, korzyściami z grania oraz niebezpieczeństwami, na jakie są narażone dzieci w przestrzeni wirtualnej. Podpowie też, jak właściwie dobierać gry i jak sprawić, że korzystanie z nowych technologii będzie bezpieczne dla najmłodszych użytkowników komputera i internetu.

- **Projekt edukacyjny *Zostań znajomym swojego dziecka*, zob. bit.ly/zznswdz**

Cały materiał, adresowany do rodziców i opiekunów, składa się z cyklu 10 filmów, broszury informacyjnej i ulotki. Treści zamieszczone w tym pakiecie edukacyjnym mają zachęcić dorosłych do aktywnego uczestnictwa w internetowym życiu dzieci, poznania ich zainteresowań i wirtualnej społeczności. Wiele miejsca jest poświęcone także zagrożeniom, na jakie najmłodsi użytkownicy sieci mogą trafić podczas zgłębiania cyberprzestrzeni.

- **Broszura *Zagrożenia internetowe. Wybrane zjawiska*, zob. bit.ly/zagrint**

Broszura jest przeznaczona dla szerokiego grona odbiorców, którzy interesują się bezpieczeństwem w internecie, a także szukają pomocy na wypadek ataku cyberprzestępców. Minisłownik, który ma formę zestawienia, pozwala poznać podstawowe wiadomości o cyberprzemocy, filtrach kontroli rodzicielskiej, materiałach prezentujących seksualne wykorzystanie małoletnich i mowie nienawiści.

- **Poradnik *Pomyśl, zanim kupisz*, zob. bit.ly/pomzank**

Publikacja zawiera porady dla dorosłych na temat tego, jak dokonać rozważnego zakupu sprzętu elektronicznego dla dzieci. Znajdziemy tu także opis zagrożeń internetowych, wskazówki, jak chronić przed nimi najmłodszych, oraz informacje o miejscach, w których na wypadek takich problemów można szukać pomocy.

- **Kurs e-learning *Bezpieczeństwo dzieci i młodzieży online*, zob. edukacja.fdds.pl**

Celem kursu jest przygotowanie profesjonalistów pracujących z dziećmi i młodzieżą do diagnozy zagrożeń online, podejmowania wartościowych działań edukacyjnych oraz skutecznej interwencji w przypadku wystąpienia problemu dotyczącego tych zagrożeń.

- **Broszura *Nadmierne korzystanie z komputera i internetu przez dzieci i młodzież*, zob. bit.ly/nadkorz**

Publikacja ta powstała w ramach kampanii *W którym świecie żyjesz?* W broszurze poruszono kwestie praktyczne i teoretyczne związane z zagadnieniem nadmiernego korzystania z sieci i komputera. Autorzy publikacji zamieścili informacje o tym, jak zarządzać czasem spędzanym przez dziecko i młodzież online, a także wskazali miejsca pomocne w sytuacji zagrożenia ze strony cyberprzestępców.

- **Scenariusz zajęć dla rodziców *Uważni rodzice*, zob. edukacja.fdds.pl**

Scenariusz zajęć przeznaczonych dla rodziców uczniów szkół podstawowych i ponadpodstawowych. Zajęcia mogą być realizowane np. przy okazji wywiadówek. Ich celem jest uwrażliwienie rodziców na problem uwodzenia dzieci w internecie, omówienie specyfiki tego zjawiska i uświadomienie rodzicom ich roli w ochronie dzieci przed uwodzeniem online.

- **Scenariusz zajęć dla rodziców *Internet bez przesady*, zob. edukacja.fdds.pl**

Scenariusz zajęć dla rodziców uczniów szkół podstawowych i średnich. Celem zajęć jest uwrażliwienie rodziców na problem nadmiernego korzystania przez dzieci z mediów elektronicznych i internetu, omówienie jego specyfiki oraz możliwych działań profilaktycznych i sposobów reagowania w sytuacji podejrzenia uzależnienia dziecka od sieci.

Nowa edycja kompendium „Bezpieczeństwo dzieci i młodzieży online" przygotowana przez Polskie Centrum Programu Safer Internet (NASK Państwowy Instytut Badawczy i Fundacja Dajemy Dzieciom Siłę) ma na celu usystematyzowanie najnowszej wiedzy dotyczącej aktywności dzieci i młodzieży w internecie. Czytelnik znajdzie w nim diagnozę zjawisk społecznych zachodzących w sieci, analizę sytuacji ryzykownych, ze szczególnym uwzględnieniem ich przyczyn i sposobów zapobiegania zagrożeniom oraz dostanie bogatą gamę wskazówek profilaktycznych i edukacyjnych. Mamy nadzieję, że wszystko to pomoże rodzicom i nauczycielom mądrze wprowadzać dzieci w świat, którego internet stał się permanentnym i nieodłącznym elementem.