Szkolne standardy bezpieczeństwa dzieci i młodzieży online

REKOMENDACJE DLA SZKÓŁ

www.fdn.pl
www.dzieckowsieci.fdn.pl

Szkolne standardy bezpieczeństwa dzieci i młodzieży online

Fundacja Dzieci Niczyje
ul. Walecznych 59
03-926 Warszawa
tel. 22 616 02 68
fdn@fdn.pl
www.fdn.pl

Opracowanie: Katarzyna Makaruk, Robert Makowski
Łukasz Wojtasik, Szymon Wójcik,
Magdalena Wróblewska, Marcin Sołodki

Skład i opracowanie graficzne:
Olga Figurska, www.lunatikot.pl

ISBN 978-83-936366-2-4

PROJEKT WSPÓŁFINANSOWANY ZE ŚRODKÓW MINISTERSTWA EDUKACJI NARODOWEJ

GŁÓWNY PARTNER

Spis treści

Wstęp

Istniejące jeszcze niedawno wyraźne rozgraniczenie pomiędzy światem realnym a światem online przestało istnieć. Do szkół trafiło pokolenie, które od najmłodszych lat wychowywało się w obecności komputera i internetu, dla którego kontakt z bliskimi przez komunikator internetowy jest bardziej naturalny niż sięgnięcie po telefon stacjonarny, a w poszukiwaniu rozrywki, zamiast włączyć np. telewizor, młodzi ludzie zaglądają do jednego z serwisów wideo. Dla tego pokolenia świat online jest kontynuacją świata realnego – to w internecie rozmawiają z kolegami z klasy, których widzieli kilka godzin wcześniej, zabijają nudę, przeglądając portale społecznościowe, w internecie szukają informacji niezbędnych do odrobienia lekcji, często telefon lub tablet są i pierwszą, i ostatnią rzeczą, którą widzą każdego dnia. To ich świat, to ich życie.

Ale częścią ich życia jest również szkoła. W niej korzystają z internetu podczas zajęć z informatyki lub w czasie przerw, a nawet lekcji, do sieci trafiają szkolne konflikty, do szkoły z kolei – konsekwencje np. nierozważnych zachowań w internecie. Nie zamierzamy demonizować zagrożeń internetowych, wiemy jednak, że szkoła powinna liczyć się z nimi i być na nie przygotowana, właśnie poprzez wdrożenie standardów bezpieczeństwa i procedur rozwiązywania sytuacji kryzysowych.

By zapewnić szkole i jej uczniom bezpieczeństwo w internecie, niezbędne są:

- bezpieczna infrastruktura sieciowa, przygotowana na poziomie sprzętowym i programistycznym,
- personel szkoły przygotowany merytorycznie,
- wyedukowani uczniowie,
- świadomi zagrożeń, współpracujący ze szkołą rodzice,
- opracowane i wdrożone procedury reagowania.

Oddajemy w Państwa ręce treściwe kompendium wiedzy na temat rozwiązywania problemów związanych z zagrożeniami internetowymi dotyczącymi dzieci i młodzieży w szkole. Przedstawiamy również propozycje edukacyjne pozwalające na przekazanie uczniom w atrakcyjny sposób podstawowych informacji dotyczących bezpieczeństwa w sieci. Publikacja obejmuje również propozycje procedur, których wdrożenie pozwala zminimalizować negatywne skutki zagrożeń, jakich nie udało się uniknąć.

Diagnoza sytuacji

Uczeń w sieci[1]

O ile jeszcze w 2008 roku dostęp do internetu miało nieco ponad 60 proc. gospodarstw domowych z dziećmi poniżej 16 roku życia, w 2012 roku odsetek ten przekroczył 90 proc. (GUS 2012). Dwie trzecie gimnazjalistów korzysta z internetu codziennie lub prawie codziennie, a tylko 1 proc. używa sieci rzadziej niż przynajmniej raz w tygodniu (EU NET ADB 2013). Internet dla nastolatków stał się najważniejszym medium – ponad 10 godzin tygodniowo spędza w nim 70 proc. osób w wieku 15-19, a tyle samo czasu na oglądanie telewizji poświęca zaledwie 30 proc. (World Internet Project Poland 2011).

Aż **98%** dzieci w Polsce w wieku 9-16 lat korzysta z internetu przynajmniej raz w tygodniu.

Nastolatkowie korzystają z sieci przede wszystkim w dni wolne od zajęć – o ile w ciągu tygodnia większość z nich spędza w internecie nie więcej niż dwie godziny dziennie (70 proc.), w weekend krócej niż dwie godziny w internecie spędza 39 proc., 36 proc. od 2 do 4 godzin, a 17 procent – ponad 4 godziny.

Korzystanie z internetu w szkole deklaruje 88 proc. nastolatków, codziennie robi to jednak jedynie 5,5 proc. Najczęściej miejscem, z którego nastolatki korzystają z internetu, jest własny pokój (73,9 proc.) lub miejsce dostępne dla wszystkich domowników (33,8 proc.).

Większość młodzieży korzysta z sieci, posługując się komputerem – najczęściej w domu (98 proc.), w szkole (69 proc.) lub u znajomych (64 proc.). Za pośrednictwem telefonu komórkowego młodzi ludzie korzystają z internetu również najczęściej w domu (44 proc.) lub w szkole (31 proc.). 29 proc. do łączenia się z internetem używa telefonów komórkowych w środkach komunikacji miejskiej lub na ulicy.

[1] Na podstawie niepublikowanego raportu: Wójcik S., (2013) *Korzystanie z internetu i zagrożenia online wśród młodziezy gimnazjalnej. Przegląd badań*, Fundacja Dzieci Niczyje

Najbardziej popularną czynnością nastolatków w internecie jest oglądanie klipów filmowych i filmów – co najmniej raz w tygodniu robi to 84 proc. gimnazjalistów (EU NET ADB). 80 proc. gimnazjalistów korzysta z kolei z komunikatorów. Inną, równie powszechną formą aktywności jest korzystanie z serwisów społecznościowych – przynajmniej raz w tygodniu zagląda do nich 79 proc. gimnazjalistów, a konto na przynajmniej jednym z portali ma 90 proc. nastolatków. Kolejne pozycje wśród form aktywności nastolatków w sieci zajmują odpowiednio: odrabianie prac domowych/poszukiwanie informacji (76 proc.), ściąganie muzyki (66 proc.). Jak podkreślają autorzy badania, wyraźne różnice w korzystaniu z internetu przez dorosłych i młodzież widać np. w kontekście poczty elektronicznej. Z tej usługi rozpowszechnionej wśród osób dorosłych korzysta tylko 52 proc. gimnazjalistów. Największe różnice ze względu na płeć można dostrzec w przypadku gier (komputerowych i online) – ponad połowa chłopców (52,4 proc.) deklaruje, że gra codziennie, równie często gra zaledwie 8,4 proc. dziewcząt.

Jednym z najistotniejszych ogniw systemu bezpieczeństwa dzieci i młodzieży w internecie są rodzice uczniów. Szczegółowe dane statystyczne znajdują się w rozdziale poświęconym omówieniu procedur zapobiegania poszczególnym zagrożeniom, wystarczy jednak wspomnieć, że według badań EU Kids Online z 2010 roku wiedza rodziców o tym, co ich dzieci robią w internecie i z czym się spotykają, jest niewielka. 58 proc. rodziców w Polsce, których dzieci miały w internecie kontakt z pornografią (zdjęcia lub filmy), jest przekonana, że ich dzieci nie widziały tego typu materiałów, 85 proc. rodziców, których dzieci otrzymały wiadomości związane z seksem, jest przekonana, że wiadomości tego typu nie trafiły do ich dzieci, 70 proc. rodziców, których dzieci spotkały się osobiście z kimś poznanym w internecie, twierdzi, że do takiego spotkania nie doszło, 90 proc. rodziców dzieci, które doświadczyły elektronicznej przemocy rówieśników (napastowanie, złośliwe, przykre wiadomości), jest przekonana, że ich dzieci nie były ofiarami cyberbullyingu. Tylko 8 proc. rodziców wie, że ich pociecha miała jakieś negatywne przeżycia związane z internetem.

W grupie wiekowej 15-19 lat internet jest najważniejszym medium.

Chociaż można by oczekiwać od rodziców przynajmniej rozmów z dziećmi na temat bezpieczeństwa online, podobnie jak nauki bezpiecznego przechodzenia przez jezdnię, jedynie trzech na pięciu uczniów gimnazjum pamięta, by rodzice rozmawiali z nim na ten temat. I chociaż 93 proc. rodziców twierdzi, że kontroluje to, co ich dziecko robi w internecie, tylko zdaniem 44 proc. gimnazjalistów rzeczywiście tak się dzieje. Oczywiście można zakładać, że kontrola rodzicielska jest na tyle dyskretna, że niezauważalna przez uczniów, trzeba się jednak liczyć również z możliwością, że przekonanie rodziców o kontrolowaniu swoich dzieci jest jedynie złudą, bo 36 proc. gimnazjalistów stwierdza, że rodzice nie kontrolują ich w żaden sposób.

Więcej na ten temat:

- *www.dzieckowsieci.fdn.pl/badania*

Nauczyciel w sieci[2]

Według najświeższych danych (badanie „Diagnoza systemu bezpieczeństwa online w szkołach", przeprowadzone przez Fundację Dzieci Niczyje we wrześniu i październiku 2013 roku wśród nauczycieli pracujących w gimnazjach), szkoły nie są przygotowane na rozwiązywanie problemów związanych z zagrożeniami w internecie. Respondenci badania przyznają, że mają niewielką wiedzę na temat zagrożeń internetowych oraz niebezpiecznych sytuacji związanych z korzystaniem przez uczniów z komputerów w trakcie zajęć lub z urządzeń mobilnych, a o incydentach związanych z zagrożeniami w sieci dowiadują się np. od własnych dzieci, które również są uczniami szkoły.

Według nauczycieli, najczęstszą formą zagrożenia doświadczaną przez ich uczniów była agresja elektroniczna na czatach lub w portalach społecznościowych (45 proc.). 40 proc. wie, że ich uczniowie padli ofiarą rozsyłania lub publikowania w internecie przykrych lub złośliwych informacji. 17 proc. nauczycieli wie, że uczniowie odwiedzają strony pornograficzne.

Za największe zagrożenie nauczyciele uznają agresję w internecie (85 proc.). Według 81 proc. poważnym problemem jest nadużywanie przez uczniów internetu. 58 proc. twierdzi, że dużym zagrożeniem są strony na temat samookaleczania, samobójstwa, skrajnego odchudzania, narkotyków, zawierające rasistowskie przekazy. 38 proc. nauczycieli do największych zagrożeń zaliczyło pornografię online.

Według informacji pochodzących od respondentów, w szkołach nie istnieją spisane procedury postępowania w przypadku incydentów związanych z zagrożeniami online, a istniejące procedury dotyczące postępowania w przypadku wystąpienia przemocy nie obejmują rozwiązań związanych z agresją elektroniczną.

Nauczyciele oceniają swój poziom wiedzy na temat bezpieczeństwa online jako przeciętny. Najbardziej znane są im rodzaje zagrożeń online – średnia 3,7 na 5-punktowej skali (gdzie 1 oznacza „niski poziom wiedzy", a 5 – „wysoki poziom wiedzy"). Kolejne pozycje zajmuje poziom wiedzy na temat uzależnienia od internetu (średnia 3,4), interwencji w przypadku zagrożeń online (3,1) oraz zapobiegania zagrożeniom (3,1). Największe braki nauczyciele dostrzegają w przypadku wiedzy na temat regulacji prawnych – średnia 2,7. Większość respondentów chciałaby się więcej dowiedzieć na temat uzależnienia od internetu (64 proc.), poznać regulacje prawne (61 proc.) oraz zdobyć wiedzę na temat zapobiegania niebezpiecznym kontaktom i ryzykownym zachowaniom online (47 proc.). Potrzebę zdobycia wiedzy na temat interwencji w przypadkach zagrożeń online wskazało 41 proc., a edukacji w zakresie zagrożeń online – 29 proc.

Jak z kolei wynika z badań potrzeb edukacyjnych nauczycieli (FDN, 2012), zagrożenia w internecie jako problem, który powinien być poruszany w trakcie zajęć edukacyjnych, są dostrzegane przez 81 proc. badanych nauczycieli, co wskazywałoby na świadomość wśród nich rangi tego zjawiska. Jeśli jednak skonfrontować te wyniki z badaniami dotyczącymi udziału dzieci w zajęciach związanych z bezpieczeństwem w internecie, czeka nas zaskoczenie. Chociaż konieczność edukacji w tym zakresie znalazła się w podstawie programowej już kilka lat temu, prawie 1/3 badanych gimnazjalistów stwierdziła, że nigdy nie miała zajęć poświęconych tej tematyce. 15 proc. pytanych o zajęcia tego typu wybrało odpowiedź „nie pamiętam". Tylko 56 proc. uczniów zadeklarowało, że brało udział w zajęciach dotyczących bezpieczeństwa w internecie. Równie zaskakująca jest odpowiedź badanych uczniów na pytanie dotyczące tego, do kogo zwróciliby się o pomoc, gdyby spotkało ich coś złego w internecie. O ile pomocy u rodziców szukałaby większość (63 proc.), do nauczyciela lub pedagoga/psychologa szkolnego zwróciłoby się zaledwie po 2 proc. uczniów (*Bezpieczeństwo dzieci w internecie*, 2013)

[2] Na podstawie niepublikowanego raportu z badań: Makaruk K., (2013) *Diagnoza stanu bezpieczeństwa online w szkołach*, Fundacja Dzieci Niczyje

Szkolne standardy bezpieczeństwa

Zapewnienie uczniom bezpieczeństwa w internecie wymaga od szkoły kompleksowych i przemyślanych rozwiązań. I to zarówno na poziomie infrastruktury technicznej, jak i na poziomie rozwiązań organizacyjnych.

Zadaniem szkolnej infrastruktury sieciowej jest przede wszystkim umożliwienie dostępu do internetu, zarówno personelowi szkoły, jak i uczniom, czy to tylko na czas zajęć, czy też poza nimi. Nie można jednak traktować szkolnej sieci jako cokolwiek powiększonej sieci domowej. Sprzęt przewidziany do rozwiązań indywidualnych i zaledwie kilku urządzeń podłączonych do sieci nie będzie w stanie zapewnić dostępu kilkudziesięciu lub kilkuset użytkownikom. Pod tym względem warto również pamiętać o zachowaniu możliwości jego skalowalności – nawet jeśli w tej chwili przewidywany jest dostęp dla kilku użytkowników, mobilne urządzenia są coraz bardziej powszechne, konieczność zapewnienia dostępu większej liczbie użytkowników może być kwestią bardzo bliskiej perspektywy. Takie rozwiązanie nie będzie również w stanie spełnić drugiego z kluczowych wymagań stawianych przed szkolną siecią. Obok zapewnienia dostępu do internetu, szkolna sieć powinna umożliwiać jego monitorowanie, ponieważ to na szkole – jako specyficznym dostawcy usług internetowych – spoczywa odpowiedzialność za zidentyfikowanie sprawcy ewentualnych nadużyć. Więcej o rozwiązaniach technicznych pisze Dariusz Stachecki w tekście „Bezpieczeństwo szkolnej infrastruktury informatycznej".

Podstawowe elementy bezpieczeństwa szkoły w internecie:

- bezpieczna infrastruktura informatyczna,
- kompetentny personel,
- działania profilaktyczne wobec uczniów,
- świadomi i współpracujący rodzice,
- przygotowane i stosowane procedury reagowania.

Odwołując się do starej prawdy mówiącej, że człowiek jest zazwyczaj najsłabszym ogniwem zabezpieczeń, nie można zapominać o użytkownikach sieci. Będą nimi przede wszystkim uczniowie, których pomysłowości zazwyczaj nikt nie jest w stanie przewidzieć, stąd – zamiast wprowadzać suche reguły i zakazy – lepiej zadbać o ich edukację, która powinna dotyczyć przede wszystkim profilaktyki sieciowych zagrożeń i wskazać im konsekwencje nierozważnych zachowań w sieci. Nie jesteśmy w stanie przewidzieć wszelkich niebezpiecznych sytuacji, warto więc również pokazać uczniom metody radzenia sobie z nimi i wskazać osoby lub instytucje, w których mogą szukać pomocy. Nie sposób tutaj przecenić roli rodziców, których warto zaangażować w edukację ich dzieci w zakresie bezpieczeństwa w internecie. Zadaniem szkoły nie jest zdjęcie z rodziców odpowiedzialności za wychowanie dzieci, nawet w tak nowym środowisku, jakim dla wielu osób jest internet, jednak biorąc pod uwagę badania wskazujące na brak ich wiedzy na temat tego, co ich pociechy robią w sieci, to zadaniem szkoły jest przygotowanie dzieci i młodzieży do samodzielnego funkcjonowania w internecie.

Internet jest bardzo wymagającym środowiskiem – zarówno ze względu na swoją różnorodność, jak i nieustanne zmiany. Edukacja na rzecz bezpieczeństwa dzieci i młodzieży w internecie oraz gotowość z radzeniem sobie z codziennymi problemami funkcjonowania młodych ludzi w sieci wymaga od nauczycieli stałego rozwoju i uaktualniania swojej wiedzy. To również kwestia zadbania o rozwiązania organizacyjne na poziomie szkoły, które – ze względu na zmienność sieci – trzeba systematycznie aktualizować. Ich podstawą powinny być jednak opracowane i wdrożone przez szkołę standardy bezpieczeństwa, pozwalające na szybkie i skuteczne reagowanie w sytuacjach konfrontacji z sieciowym zagrożeniem. W szkole powinny powstać procedury reagowania na takie sytuacje, konieczne jest też podejmowanie interwencji w każdym przypadku zagrożenia bezpieczeństwa dziecka, związanego z korzystaniem z mediów elektronicznych.

*Informacje dotyczące zapobiegania zjawisku przemocy rówieśniczej w sieci zostały zebrane w książce „**Jak reagować na cyberprzemoc. Poradnik dla szkół**". Zarówno to wydawnictwo, jak i inne materiały użyteczne dla nauczycieli, są dostępne w wersji elektronicznej na stronie **www.dzieckowsieci.fdn.pl**.*

Bezpieczeństwo szkolnej infrastruktury informatycznej

Dariusz Stachecki

Rzeczywistość informatyczna w polskiej szkole uległa w ostatnich latach istotnym zmianom. Komputery znajdują się już nie tylko w pracowniach komputerowych i są wykorzystywane nie tylko podczas lekcji informatyki. Struktura informatyczna w wielu placówkach stanowi dziś niezwykle istotny fundament organizacji pracy szkoły, i to zarówno na gruncie dydaktyczno-wychowawczym, opiekuńczym, jak i zarządzania instytucją. Dlatego niezwykle istotne jest, aby zapewnić wysoki poziom jej bezpieczeństwa.

Nowe tendencje – nowe wyzwania

Od kilku lat na całym świecie mamy do czynienia z olbrzymią ekspansją urządzeń mobilnych. W naszych kieszeniach znajdują się komputery o mocy obliczeniowej przekraczającej możliwości komputerów stacjonarnych, które kiedyś docierały do szkół z centralnych dostaw MEN. Mowa o tabletach, smartfonach i innych gadżetach. Są one także bardziej wygodne niż komputery, można je mieć zawsze przy sobie, wyposażone są w dobrej jakości kamery, mikrofony, interfejsy komunikacyjne, a długi czas pracy na baterii sprawia, że stają się idealnym narzędziem dydaktycznym. Stąd podstawowym medium sieciowym w szkołach nie są już sieci kablowe, ale bezprzewodowe.

Bardzo dużym wyzwaniem dla szkoły jest także tendencja BYOD (*Bring Your Own Device*, czyli: *przynieś własne urządzenie*), polegająca na tym, że każdy może zabrać do szkoły własne urządzenie i korzystać z niego za pośrednictwem szkolnej infrastruktury sieciowej. W związku z tym na małej powierzchni pojawia się stosunkowo duża liczba urządzeń różnej klasy, mniej lub bardziej stabilnych, które chcą jednocześnie korzystać z dostępu do sieci. Jest to spore wyzwanie, zarówno dla sieci, jak i jej administratora. Dlatego szkolna infrastruktura powinna być budowana zawsze w oparciu o profesjonalne urządzenia. Najbardziej popularne routery i access pointy z tzw. segmentu SOHO (*Small Office Home Office*) nie nadają się do pracy w warunkach szkolnych. Nie potrafią zapewnić obsługi takiej liczby urządzeń zlokalizowanych często w niewielkiej odległości od siebie. Bardzo łatwo taką sieć przeciążyć i zwyczajnie zablokować. Powinniśmy sięgnąć po profesjonalne rozwiązania z dedykowanym kontrolerem WLAN (*Wireless Local Area Network*), zapewniającym zarówno wysoką wydajność, jak i odpowiedni poziom bezpieczeństwa, z zarządzalnymi, szybkimi przełącznikami, z wysokowydajnym routerem wyposażonym system IPS i inne mechanizmy zabezpieczające przed atakami i włamaniami.

Bezpieczny dostęp do sieci Wi-Fi

Udostępniając sieć bezprzewodową w szkole, powinniśmy pamiętać, że placówka oświatowa staje się wtedy swego rodzaju dostawcą usług internetowych. Od nas zależy, jakich usług będziemy dostarczać. Publikowanie tzw. otwartych sieci nie zapewni żadnego poziomu bezpieczeństwa. Najlepiej tak zaprojektować infrastrukturę, aby odseparować od siebie sieci publiczne, dydaktyczne i administracyjne. Każdy użytkownik logujący się do sieci powinien zostać przekierowany do odpowiedniego VLAN-u (*Virtual Local Area Network*), w którym ma dostęp do usług przeznaczonych wyłącznie np. dla nauczycieli lub pracowników administracji.

Każda sieć w szkole powinna być zabezpieczona przynajmniej mocnym hasłem WPA2 Personal. Tutaj niezwykle istotna uwaga. Jeżeli chcemy, aby nasza sieć była bezpieczna, tego hasła nie wolno ujawniać – uczniowie nie powinni mieć dostępu do tej samej sieci, co nauczyciele. Opublikowanie w tej sieci pewnych wrażliwych dokumentów może mieć wtedy katastrofalne skutki.

Jednak nawet dobrze zaprojektowana i podzielona sieć, zabezpieczona hasłem, nie zapewni odpowiedniego poziomu bezpieczeństwa, przede wszystkim dostępu do informacji o użytkowniku i jego działalności. Ze względu na to, że zapewniamy dostęp do internetu, w przypadku np. złamania prawa przez osobę korzystającą ze szkolnej sieci, możemy być zobligowani przez policję lub prokuraturę do udostępnienia danych konkretnego użytkownika. Musimy zatem dysponować odpowiednią wiedzą. Takich informacji nie da się pozyskać, jeśli wszyscy użytkownicy sieci bezprzewodowej będą się do niej logowali za pomocą tej samej nazwy użytkownika i tego samego hasła. Dlatego w zastosowaniach szkolnych najlepsze są rozwiązania typu Enterprise oparte o serwer RADIUS, który przy próbie logowania do sieci każdorazowo sprawdza, czy użytkownik ma prawo dostępu. Serwer powinien też gromadzić dane o aktywności użytkownika w sieci, można to zrobić w oparciu o usługę Active Directory w systemie Windows Serwer lub FreeRadius w środowisku Linux. Korzystając z takiego rozwiązania, możemy każdemu użytkownikowi w sieci przypisać unikalny login i hasło. Bardzo dobrze, jeśli możemy również spersonalizować konta pocztowe i w oparciu o te same dane zapewnić dostęp do usług w chmurze, czyli do wirtualnego dysku sieciowego, aplikacji dostępnych poprzez przeglądarki internetowe itd.

Takie rozwiązanie ma jeszcze jedną, bardzo ważną zaletę – jego użytkownik nie może czuć się w sieci anonimowy. Korzystając z własnego loginu i hasła, ma świadomość, że jego aktywność jest rejestrowana. Praktyka pokazuje, że to skutecznie eliminuje pokusy związane z nieautoryzowanym dostępem lub zrobienia komuś „psikusa", a liczba niewybrednych komentarzy na ogólnodostępnych forach internetowych i prób dostępu do niepożądanych treści spadają do zera.

Filtrowanie treści

W pracowniach komputerowych powszechna była praktyka instalowania na komputerach specjalnego oprogramowania filtrującego treści. Nie było to jednak rozwiązanie ani wygodne, ani skuteczne. Zdarzały się sytuacje, gdy odpowiednio zabezpieczony komputer był niezdolny do działania. Oczywiście, odwołując się do starej zasady, że „bezpieczny komputer, to wyłączony komputer", musimy mieć na uwadze, że nie jesteśmy w stanie wyeliminować wszystkich zagrożeń. Możemy im jednak skutecznie przeciwdziałać.

W erze urządzeń mobilnych oraz BYOD instalowanie na urządzeniach użytkownika programów ograniczających dostęp do pewnych treści jest praktycznie niemożliwe. Niemożliwe jest też skuteczne zarządzanie takim systemem. Z praktyki wynika, że uczniowie często przynoszą własny sprzęt do szkoły, aby pobrać z sieci filmy, bo „w szkole jest szybszy internet". W taki sposób można skutecznie „zapchać" całe pasmo, co uniemożliwi pracę na lekcjach.

Najrozsądniejszym rozwiązaniem jest centralne zainstalowanie specjalnych urządzeń dedykowanych do tzw. „content filteringu", które będą filtrowały cały ruch. Jednak profesjonalne sprzętowe filtry tego typu są bardzo drogie. Ich cena zależy od liczby użytkowników, a więc i liczby licencji, która nierzadko w warunkach szkolnych zbliża się do tysiąca, a często go przekracza. Innym i stosunkowo skutecznym rozwiązaniem jest instalacja w sieci specjalnego serwera opartego najczęściej na systemie Linux, zawierającego odpowiednio skonfigurowane zapory (tzw. firewall), serwer proxy (np. Squid) i oprogramowanie filtrujące, np. DansGuardian. Praktyka pokazuje, że jest to bardzo wydajne i skuteczne rozwiązanie. Oczywiście nie da się zabezpieczyć wszystkiego, jednak każda szkoła powinna mieć możliwość edycji tzw. czarnej listy (z ang. *black list*), aby skutecznie zareagować np. na informację od użytkownika, że dany serwis jest dostępny w szkolnej sieci, chociaż powinien być zablokowany.

Odpowiednie skonfigurowanie reguł dostępu do sieci może także wyeliminować np. korzystanie z pożerających pasmo programów typu torrent i uchronić nas od zarzutów dotyczących pobierania nielegalnych materiałów z sieci. Udostępnienie tylko wybranych portów może zapewnić wydajny i niezawodny dostęp do usług edukacyjnych, które są potrzebne w szkole.

Bezpieczny dostęp do dokumentacji szkolnej

Dokumentacja szkolna to przede wszystkim dziennik elektroniczny. W wielu szkołach funkcjonuje on już jako jedyna metoda dokumentowania działalności dydaktyczno-opiekuńczej placówki. Kluczowe znaczenie ma wdrożenie odpowiednich zasad korzystania z systemu. Najlepiej wyposażyć się w taki system, który gwarantuje wysoki poziom bezpieczeństwa dostępu do danych. Dzięki systemom loginów i tzw. bezpiecznych haseł możemy mieć zapewniony dostęp do e-dziennika. Dziennik powinien również przechowywać informacje o tym, kto, do jakich danych i kiedy miał dostęp. Dobrą praktyką jest również przekazywanie loginów i haseł rodzicom osobiście i uświadomienie im, że danych tych nie należy udostępniać swojemu dziecku, bo dysponuje ono własnym kontem. Każdy użytkownik po pierwszym zalogowaniu powinien zmienić hasło na własne, takie, które odpowiada elementarnym zasadom bezpieczeństwa. Nie powinno być ono krótsze niż 8 znaków, oprócz liter powinno zawierać co najmniej jedną wielką literę, znak specjalny i cyfry. Niedopuszczalne jest zapisywanie danych dostępowych w widocznym miejscu – na przykład na karteczce przyklejonej do monitora. Ponadto hasła nauczycieli powinny być zmieniane co 30 dni, najlepiej poprzez wymuszenie zmiany przez system.

Coraz częściej jednak dokumentacja szkolna to nie tylko dziennik. To także opinie o uczniach, zalecenia poradni psychologiczno pedagogicznej, karty indywidualnych potrzeb ucznia itd. Niezwykle istotne jest, aby dostęp do tych dokumentów miały tylko upoważnione osoby. Nie mogą one być dostępne w serwisach publicznych. Złą praktyką jest również zamieszczanie takich dokumentów w serwisach oferujących przechowywanie danych w internetowej chmurze. Często regulaminy takich serwisów są tak skonstruowane, że umożliwiają operatorowi serwisu wykorzystanie naszych zasobów. Dlatego najlepiej skorzystać z serwisu, który jest dedykowany wyłącznie dla nas, oferującego najwyższy poziom zabezpieczeń.

Polityka bezpieczeństwa

Każda szkoła powinna wdrożyć politykę związaną z bezpieczeństwem pracy z wykorzystaniem infrastruktury informatycznej. Każdy użytkownik sieci powinien zapoznać się z regulaminem i zaakceptować go. Regulaminy natomiast powinny zawierać zdefiniowane od początku do końca reguły korzystania z zasobów sieci, dokładnie określać, co użytkownik może robić, a czego mu robić nie wolno. Reguły te powinny być podane do wiadomości wszystkim użytkownikom sieci.

Warto zademonstrować uczniom zapis monitoringu ich aktywności. Jeżeli będą oni wiedzieli, że ich prace w szkolnej sieci są bezpieczne, że nie zostaną zmodyfikowane lub usunięte przez złośliwe działanie rówieśników – ich poczucie bezpieczeństwa będzie wysokie. Jednocześnie świadomość, że każda aktywność jest monitorowana, że osoba za nią odpowiedzialna może być szybko zidentyfikowana, skutecznie eliminuje zakusy, by spłatać komuś figla lub świadomie wyrządzić przykrość.

Warunkiem każdego skutecznego działania jest konsekwencja. Nawet najlepiej zdefiniowana polityka bezpieczeństwa nie sprawdzi się, jeżeli nie będzie konsekwentnie realizowana. Od zasad, które wyraźnie określimy, sprecyzujemy i podamy do publicznej wiadomości, nie może być odstępstw. Na przykład, obok precyzyjnie zdefiniowanej struktury indywidualnych kont sieciowych nie mogą istnieć powszechnie znane anonimowe konta użytkowników, bo każdy, kto będzie chciał pozostać anonimowy, właśnie z takich kont skorzysta.

Nauczyciele, opiekunowie pracowni i administrator powinni reagować na każdą zgłoszoną im uwagę. Brak reakcji powoduje powstanie przekonania o bezkarności, że *zasady zasadami, a rzeczywistość rządzi się innymi prawami*. A wtedy nasze działania nie będą skuteczne.

Postulaty w zakresie edukacji na temat bezpieczeństwa dzieci i młodzieży w sieci

O bezpieczeństwo w internecie każdy jego dorosły użytkownik będzie musiał zadbać sam. Ale w przypadku dzieci i młodzieży nie sposób przecenić roli rodziców i szkoły w kształtowaniu odpowiedzialnych zachowań, pokazaniu konsekwencji zachowań ryzykownych, a przede wszystkim wskazaniu najprostszych zasad bezpieczeństwa, których stosowanie pozwala uniknąć lub ograniczyć skalę potencjalnych niebezpieczeństw. Rolą rodziców i nauczycieli jest przygotowanie dzieci do posługiwania się internetem tak, by sieć była miejscem przyjaznym, pozwalającym na rozwój dziecka, rozwijanie jego potencjału, dostęp do informacji i wiedzy, ułatwiającym kontakty z innymi ludźmi. Internet jest jednak medium i bardzo złożonym (zawiera w sobie praktycznie wszystkie znane do tej pory formy przekazu), i bardzo dynamicznym – pojawiają się i rozpowszechniają nowe usługi, a wraz z nimi – nowe zagrożenia. Jako przykład można wskazać chociażby transmisje wideo online. Jeszcze kilka lat temu jakość połączeń internetowych nie pozwalała na ich rozpowszechnienie, obecnie znajdują wiele zastosowań, między innymi zarobkowe pozowanie w serwisach erotycznych, co staje się coraz częściej również udziałem nastolatków. W równie błyskawiczny sposób rozwinęły się portale społecznościowe – kilka lat temu były jedynie ciekawostką dla hobbystów, obecnie to już poważna część życia społecznego dorosłych, ale również młodzieży i dzieci.

Jeśli którykolwiek z nauczycieli ma wątpliwości, czy rzeczywiście musi na bieżąco aktualizować swoją wiedzę o internecie, poznawać nowo powstające serwisy internetowe, interesować się nowinkami, odpowiedź jest prosta: tak, bo jego uczniowie już tam są. I mogą się zwrócić do niego z problemami, na które się natknęli w sieci. Ważne więc, by nauczyciele znali aktualne tendencje rozwoju internetu i potrafili dostrzec zagrożenia, które jeszcze niedawno nie istniały. A przede wszystkim – byli w stanie pokazać młodzieży, jak ich uniknąć. Ważne również, by nauczyciele byli w stanie przekazać wiedzę, ale nie tylko tę dotyczącą konkretnych rozwiązań, ale ich istoty, tak, by młodzi ludzie byli w stanie na tej podstawie zgeneralizować reguły rządzące tak zmiennym i nieprzewidywalnym środowiskiem, jakim jest internet. To również kwestia indywidualnego rozwoju zawodowego każdego z nauczycieli. Zatrzymując się na obecnym poziomie wiedzy, mogą oni być wkrótce skazani na sytuację, w której przestaną rozumieć swoich uczniów, bo kto kilka lat temu wiedział, co będą znaczyć pojęcia, które już weszły do powszechnego języka: *zgoglować kogoś, coś twitnąć, czy polajkować coś?*

Obecna podstawa programowa dość ogólnie wskazuje oczekiwania wobec ucznia na kolejnych etapach edukacyjnych. Na przykład dla III etapu edukacyjnego w zakresie informatyki przewiduje, że *Uczeń: (...) 5) samodzielnie i bezpiecznie pracuje w sieci lokalnej i globalnej*; w porównaniu z innymi przedmiotami wymagania te są mocno oględne. Tym bardziej, by spełnić swoja misję, szkoła jako instytucja powinna być zainteresowana rozwojem zawodowym nauczycieli i zdobywaniem przez nich jak najbardziej aktualnej wiedzy. Służyć temu mogą szkolenia skierowane do jej pracowników – nie tylko nauczycieli informatyki, ale wszystkich, którzy w trakcie swoich zajęć wykorzystują komputer i internet.

Materiały edukacyjne

Jedną z cech internetu jest jego multimedialność – to szansa na oparcie zajęć dla dzieci i młodzieży o atrakcyjne materiały, potrafiące zainteresować młodych ludzi, a jednocześnie przekazujące im sporą dawkę wiedzy merytorycznej, dzięki której będą potrafili nie tylko rozpoznać zagrożenia, ale dowiedzą się również, jak ich unikać.

W ramach programu „Dziecko w Sieci" prowadzonego przez Fundację Dzieci Niczyje przygotowano wiele materiałów edukacyjnych poświęconych bezpieczeństwu dzieci w internecie. Opracowane scenariusze zajęć oraz kursy e-learning mogą być wykorzystywane podczas zajęć szkolnych, pozaszkolnych lub imprez edukacyjnych. Do ich poprowadzenia wymagana jest jedynie podstawowa znajomość specyfiki internetu. Oprócz profilaktyki ryzykownych zachowań, celem tych materiałów jest również poinformowanie uczniów o instytucjach, w których mogą szukać pomocy w przypadku kontaktu z zagrożeniami online. W przygotowanych w ramach programu materiałach uwzględniamy również świadków zdarzeń związanych z bezpieczeństwem w internecie, przekonując ich odbiorców, że rolą świadka nie jest bierne przyglądanie się, ale aktywna pomoc ofierze i zminimalizowanie negatywnych konsekwencji.

„Dziecko w Sieci"

Materiały niezbędne do przeprowadzenia zajęć, jak również informacje na temat wydarzeń związanych z programem, publikowane są w serwisie **www.dzieckowsieci.fdn.pl**. Daje on możliwość bezpłatnego pobrania scenariuszy zajęć w wersji PDF oraz potrzebnych do realizacji zajęć materiałów multimedialnych: prezentacji, filmów, kreskówek. Nauczyciele mogą również wypełnić na stronie ankietę ewaluacyjną i otrzymać drogą elektroniczną zaświadczenie o realizacji zajęć programu „Dziecko w Sieci".

Platforma e-learning www.fdn.pl/kursy

Kursy e-learning programu „Dziecko w Sieci" dostępne są na platformie e-learningowej pod adresem **www.fdn.pl/kursy**. Warunkiem korzystania z nich jest rejestracja na platformie. Po zalogowaniu nauczyciel/opiekun grupy uczniów może m.in. śledzić postępy w realizacji kursów przez swoich podopiecznych oraz otrzymać zaświadczenie o realizacji zajęć.

Serwis www.necio.pl
Projekt edukacyjny skierowany do dzieci w wieku 4-6 lat, którego celem jest nauka bezpieczeństwa w internecie. Bohaterem serwisu www.necio.pl jest przyjazny robocik Necio, który zaprasza najmłodszych do wspólnej „zabawy w internet". Korzystając z serwisu Necio.pl, dzieci dowiedzą się, czym jest Internet, jak surfować po stronach www, bezpiecznie komunikować się z innymi, używać poczty e-mail, wybierać bezpieczne strony. Serwis pozwala także dziecku na opanowanie umiejętności posługiwania się myszką i klawiaturą.

Sieciaki.pl
Elementem programu „Dziecko w Sieci" jest również serwis internetowy Sieciaki.pl, adresowany do dzieci w wieku 6-12 lat, który może być wykorzystany w nauce bezpieczeństwa w sieci. Grupa Sieciaków (głównych bohaterów serwisu) to dzieci dobrze znające zasady bezpieczeństwa w internecie, które we współpracy z robotem Netrobim i Sztuczną Inteligencją zwalczają internetowe zło – Sieciuchy. Użytkownicy serwisu mają dostęp do materiałów multimedialnych, mogą brać udział w konkursach oraz korzystać z katalogu bezpiecznych stron „Sieciakowe BeSt" – witryn sprawdzonych i certyfikowanych przez zespół projektu Sieciaki.pl.

Dzień Bezpiecznego Internetu
W ramach programu „Dziecko w Sieci" zachęcamy nauczycieli do przygotowywania samodzielnych inicjatyw z okazji Dnia Bezpiecznego Internetu. Dzień ten jest obchodzony w pierwszy wtorek lutego. Został zainicjowany przez Komisję Europejską, jednak jego obchody już dawno wykroczyły poza kontynent. Tego dnia na całym świecie odbywają się liczne imprezy poświęcone różnym zagadnieniom bezpieczeństwa w internecie. To zazwyczaj lokalne wydarzenia, które są okazją do przekazania uczniom wiedzy na temat zagrożeń internetowych i radzenia sobie z nimi. Materiały pozwalające na samodzielne przygotowanie i poprowadzenie Dnia Bezpiecznego Internetu na terenie szkoły są dostępne w serwisie **www.dzieckowsieci.fdn.pl**.

Szkolenia dla dorosłych
Oferta edukacyjna programu „Dziecko w Sieci" jest kierowana również do rodziców uczniów i nauczycieli. Z myślą o nich przygotowano np. kompendium wiedzy na temat zagrożeń internetowych, dostępne w postaciu kursu na platformie e-learningowej lub materiałów wideo w serwisie **www.dzieckowsieci.fdn.pl**. Jedynie rodzice zaangażowani i świadomi zagrożeń, ale i wiedzący, jak sobie z nimi poradzić, są w stanie zapewnić swoim dzieciom bezpieczne dzieciństwo. Liczymy w tym przypadku również na współpracę ze strony szkół, które angażując rodziców i edukując ich np. w trakcie zebrań prowadzonych w oparciu o oferowane przez nas materiały, mogą się przyczynić do zmniejszenia skali potencjalnych problemów związanych z bezpieczeństwem w internecie na swoim terenie.

Pełna oferta materiałów edukacyjnych programu „Dziecko w Sieci" została opisana na końcu publikacji.

Postulaty w zakresie reagowania na zagrożenia uczniów w sieci

Dostęp do wiedzy, informacji, łatwość komunikacji – to podstawowe zalety internetu. Ale niezależnie od nich sieć niesie również zagrożenia – część z nich jest specyficzna dla internetu, część to po prostu nowe oblicze dawnych problemów. Jak podkreślono we wstępie – nie należy ich wyolbrzymiać czy demonizować, jednak ze względu na powszechność dostępu do internetu, nie można ich lekceważyć. Niezależnie od skali zaangażowania szkoły w działania edukacyjne, nie sposób wykluczyć zaistnienia sytuacji, w której potencjalne zagrożenie stanie się realnym.

Niezwykle ważnym elementem szkolnego systemu bezpieczeństwa jest odpowiednie reagowanie na sytuacje zagrożenia ucznia w sieci. Szkoła powinna opracować procedury reagowania na takie sytuacje i podejmować interwencje w każdym przypadku ujawnienia lub podejrzenia zagrożenia dla dziecka związanego z korzystaniem z mediów elektronicznych. Spisane i rozpowszechnione wśród personelu szkolnego procedury reagowania powinny klarownie informować, w jaki sposób i kiedy nauczyciele, pedagodzy, dyrekcja powinni postępować z ofiarami internetowych zagrożeń oraz (w zależności od specyfiki zdarzenia) ich sprawcami, świadkami i rodzicami dziecka. Procedury takie mogą być przygotowane w gronie nauczycieli, dyrekcji, przy znaczącym udziale zewnętrznych konsultantów i powinny być dostosowane do realiów danej placówki. Nie sposób przecenić tutaj roli pedagoga szkolnego i opiekuna szkolnej pracowni komputerowej, nie zapominajmy jednak o roli, jaką mogą odegrać wychowawcy klas, którzy na co dzień mają kontakt z internetowymi problemami swoich wychowanków.

Procedury powinny uwzględniać kilka kluczowych elementów: jednym z najistotniejszych jest udzielenie wsparcia ofierze zdarzenia, o czym łatwo zapomnieć w trakcie minimalizowania jego skutków. Zawierać powinny również wskazówki dotyczące ustalenia i udokumentowania przebiegu zdarzenia, zaangażowania rodziców w rozwiązanie problemu i ewentualne wsparcie instytucji zewnętrznych – zarówno poradni psychologiczno-wychowawczej, jak i – w poważniejszych przypadkach – organów prawnych.

Groźne sytuacje związane z internetem rzadko się zamykają w definicji pojedynczego zagrożenia. Najczęstszym z nich jest cyberprzemoc, począwszy od sytuacji, które wydawać się mogą błahe, aż po te zagrażające życiu

uczniów. Właśnie cyberprzemocy poświęcamy najwięcej miejsca. Nie można jednak zignorować pozostałych, stąd postulujemy przygotowanie przez szkołę procedur adekwatnych do każdego z nich.

Cyberprzemoc

Cyberprzemoc (ang. cyberbullying) to wszelkie intencjonalne działania przy użyciu internetu, komputera i urządzeń mobilnych (telefony komórkowe, tablety itp.), które dążą do wyrządzenia krzywdy lub wywołania dyskomfortu u ofiary. O ile agresja elektroniczna dotyczyć może osób w każdym wieku, tak termin „cyberprzemoc" zarezerwowany jest dla agresji rówieśniczej, której zarówno sprawcami, jak i ofiarami, są dzieci i młodzież. Według różnych źródeł kontakt z cyberprzemocą miało od 5 proc. polskich dzieci (badania EU Kids Online 2010, taka sama średnia europejska), do 13 proc. (badania Cyberprzemoc 2010). W tych drugich badaniach do bycia przynajmniej jednorazowo sprawcą przyznało się ponad 25 proc. uczestników.

Cyberprzemoc to jednocześnie jedno z najbardziej bolesnych doświadczeń dla dziecka. Informacja w internecie rozprzestrzenia się błyskawicznie, grono widzów lub świadków upokorzenia rośnie wykładniczo. Stąd też i wiele przypadków, w których cyberprzemoc ma tragiczne konsekwencje, aż po samobójstwo ofiary.

W przypadku cyberprzemocy ofiara jest prześladowana przykrymi komunikatami lub groźbami, poniżana rozpowszechnianymi plotkami, poddana ostracyzmowi w efekcie np. wulgarnych wiadomości rozsyłanych w jej imieniu przez osobę podszywającą się pod jej internetową tożsamość lub wykluczona z grona rówieśników komunikujących się ze sobą online. Atak na ofiarę nie wymaga bezpośredniego kontaktu, ofiara nie może nigdzie czuć się bezpiecznie – ani w szkole, ani w domu, bo media elektroniczne stały się jednym z istotniejszych elementów życia młodych ludzi. Cyberprzemoc nie kończy się wraz z wyłączeniem komputera, ofiara wie albo zakłada, że nawet wtedy kolejne osoby oglądają pogrążający ją film. Co więcej, materiały służące do ataku często okazują się atrakcyjne dla jego świadków, którzy mniej lub bardziej świadomie przyłączają się do sprawcy, rozpowszechniając je. Warto pamiętać, że w wielu przypadkach cyberprzemocy dochodzi do zamiany ról – ofiara staje się sprawcą albo mszcząc się na swoim przeciwniku, albo uderzając w kolejne, niezaangażowane wcześniej osoby.

W przypadku cyberprzemocy najbardziej powszechne są formy najprostsze, niewymagające szczególnej biegłości technicznej (badania Cyberprzemoc 2010). To po prostu zwyzywanie kogoś na czacie lub wysłanie mu wiadomości, która ma go obrazić lub przestraszyć. To również przykry lub ośmieszający komentarz zamieszczony na forum internetowym, który może być zapowiedzią eskalacji cyberprzemocy.

Procedura reagowania w przypadku zaistnienia cyberprzemocy powinna uwzględniać zarówno działania wobec ofiary, jak i sprawcy. Należy w niej

również uwzględnić rolę świadków – to oni zazwyczaj są w stanie pomóc w ustaleniu okoliczności i sprawcy zdarzenia.

Zasady postępowania szkoły w przypadku cyberprzemocy zostały szczegółowo opisane w przewodniku „Jak reagować na cyberprzemoc. Poradnik dla szkół", dostępnym w wersji elektronicznej w serwisie **www.dzieckowsieci.fdn.pl**. Poniżej przytaczamy jego najistotniejsze fragmenty. Osoby chcące pogłębić swoją wiedzę na ten temat odsyłamy też do publikacji Jacka Pyżalskiego **„Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży"**. Problemowi cyberprzemocy został poświęcony również jeden z numerów kwartalnika Fundacji Dzieci Niczyje „Dziecko krzywdzone. Teoria, badania, praktyka" (vol. 8 nr 1 Cyberprzemoc, dostępny na stronach FDN).

Procedura reagowania w szkole w sytuacji cyberprzemocy

Anna Borkowska, Dorota Macander

Jednym z ważnych zadań szkoły jest przygotowanie i stosowanie algorytmu interwencji w przypadku cyberprzemocy, uwzględniającego potrzeby i realia szkolne.

Proponowana poniżej procedura zawiera zasady postępowania pracowników szkoły w sytuacji ujawnienia cyberprzemocy. Jest podpowiedzią, jak i kiedy nauczyciele (dyrektor szkoły) powinni reagować wobec ofiar, sprawców i świadków oraz w jaki sposób współpracować z rodzicami tych uczniów.

Ujawnienie przypadku cyberprzemocy

Informacja o tym, że w szkole miała miejsce cyberprzemoc, może pochodzić z różnych źródeł. Osobą zgłaszającą fakt prześladowania może być poszkodowany uczeń, jego rodzice lub inni uczniowie – świadkowie zdarzenia, nauczyciele.

Procedury postępowania przyjęte w niektórych szkołach dopuszczają anonimowe zawiadamianie o aktach przemocy na terenie szkoły, w tym także faktu cyberprzemocy, np. proponując uczniom korzystanie ze „skrzynki zaufania", do której mogą oni wrzucać anonimowe informacje dotyczące przypadków przemocy.

Warunkiem powodzenia tego typu metod jest dobre zaplanowanie, przeprowadzenie działań przygotowawczych (uzyskanie akceptacji uczniów, uczulenie ich, że fałszywe informacje to również forma przemocy itd.), a następnie konsekwentne reagowanie na zgłaszane problemy. W przeciwnym razie istnieje ryzyko potraktowania „skrzynki" jako okazji do dobrej, choć mało wybrednej zabawy, polegającej na wrzucaniu donosów i inwektyw pod adresem uczniów i nauczycieli.

Niezależnie od tego, kto zgłasza przypadek cyberprzemocy, procedura interwencyjna powinna obejmować:

- udzielenie wsparcia ofierze przemocy;
- zabezpieczenie dowodów i ustalenie okoliczności zdarzenia;
- wyciągnięcie konsekwencji wobec sprawcy przemocy oraz pracę nad zmianą postawy ucznia.

Ustalenie okoliczności zdarzenia

Wszystkie przypadki przemocy, a więc także przemocy z wykorzystaniem mediów elektronicznych, powinny zostać właściwie zbadane, zarejestrowane i udokumentowane.

1. Jeśli wiedzę o zajściu posiada nauczyciel niebędący wychowawcą, powinien przekazać informację wychowawcy klasy, który informuje o fakcie pedagoga szkolnego i dyrektora.
2. Pedagog szkolny i dyrektor wspólnie z wychowawcą powinni dokonać analizy zdarzenia i zaplanować dalsze postępowanie.
3. Do zadań szkoły należy także ustalenie okoliczności zdarzenia i ewentualnych świadków.
4. Warto zadbać o udział nauczyciela informatyki w procedurze interwencyjnej, szczególnie na etapie zabezpieczania dowodów i ustalania tożsamości sprawcy cyberprzemocy.

Zabezpieczenie dowodów

1. Wszelkie dowody cyberprzemocy powinny zostać zabezpieczone i zarejestrowane. Należy zanotować datę i czas otrzymania materiału, treść wiadomości oraz, jeśli to możliwe, dane nadawcy (nazwę użytkownika, adres e-mail, numer telefonu komórkowego itp.) lub adres strony www, na której pojawiły się szkodliwe treści czy profil.
2. Takie zabezpieczenie dowodów nie tylko ułatwi dalsze postępowanie dostawcy usługi (odnalezienie sprawcy, usunięcie szkodliwych treści z serwisu), ale również stanowi materiał, z którym powinny się zapoznać wszystkie zaangażowane w sprawę osoby: dyrektor i pedagog szkolny, rodzice, a wreszcie policja, jeśli doszło do złamania prawa.
3. Na etapie zabezpieczania dowodów cyberprzemocy i identyfikacji sprawcy warto korzystać z pomocy nauczyciela informatyki.

JAK MOŻESZ ZAREJESTROWAĆ DOWODY CYBERPRZEMOCY?

- **Telefon komórkowy**
  Nie kasuj wiadomości. Zapisuj wszystkie wiadomości, zarówno tekstowe, jak i nagrane na pocztę głosową w pamięci telefonu.
- **Komunikatory**
  Niektóre serwisy pozwalają na zapisywanie rozmów. Możesz również np. skopiować rozmowę, wkleić do dokumentu Word (lub innego edytora tekstu), zapisać i wydrukować.
- **Strony serwisów społecznościowych, www**
  Aby zachować kopię materiału, który widzisz na ekranie, wciśnij jednocześnie klawisze Control i Print Screen, a następnie wykonaj operację „Wklej" w dokumencie Word.
- **Czat**
  Podobnie jak w przypadku stron www, jeśli chcesz zachować kopię materiału, który widzisz na ekranie, wciśnij klawisze Control i Print Screen, a następnie wykonaj operację „Wklej" w dokumencie Word. Możesz też po prostu wydrukować interesującą cię stronę.
- **E-mail**
  Wydrukuj wiadomość, prześlij ją do nauczyciela lub pedagoga, który zajmuje się ustaleniem okoliczności zajścia. Zachowanie całości wiadomości, a nie tylko samego tekstu jest bardziej pomocne, ponieważ zawiera on informacje o jej pochodzeniu.

Identyfikacja sprawcy

Młodzi ludzie często mają złudne przekonanie, iż nowe technologie zapewniają im pełną anonimowość. Jak przekonują specjaliści, istnieje wiele sposobów identyfikacji źródła cyberprzemocy. Osoby zajmujące się ustalaniem okoliczności zajścia powinny mieć jednak świadomość, iż znalezienie miejsca pochodzenia materiału nie zawsze oznacza odnalezienie osoby, która jest za zdarzenie odpowiedzialna.

1. Wielu sprawców cyberprzemocy posługuje się „skradzioną tożsamością", wykorzystując telefony innych uczniów, profile w serwisach społecznościowych, ich konta pocztowe itp. do wysyłania wiadomości bądź zamieszczania krzywdzących materiałów. Trudności z wykryciem „cyberagresora" mogą się pojawić również w sytuacji, gdy materiał przesyłany jest między telefonami komórkowymi drogą bezprzewodową lub wiadomości tekstowe na telefon wysyłane są z bramki internetowej.
2. Jak pokazuje praktyka, w większości przypadków identyfikacja agresora nie jest zbyt trudna. Ofiary cyberprzemocy często potrafią wskazać sprawcę, którym najczęściej okazuje się być kolega ze szkoły, bądź przynajmniej mają przypuszczenie, kto może nim być.
3. Gdy ustalenie sprawcy nie jest możliwe, należy się skontaktować z dostawcą usługi w celu usunięcia z sieci kompromitujących lub krzywdzą-

cych materiałów. Do podjęcia takiego działania zobowiązuje administratora serwisu art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

4. W przypadku gdy zostało złamane prawo, a tożsamości sprawcy nie udało się ustalić, należy bezwzględnie skontaktować się z policją.

Działania wobec sprawcy cyberprzemocy

Gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog szkolny pełniący w szkole rolę koordynatora działań wychowawczych wobec uczniów wymagających szczególnej uwagi powinien podjąć dalsze działania.

1. Rozmowa z uczniem sprawcą przemocy o jego zachowaniu:
   - celem rozmowy powinno być ustalenie okoliczności zajścia, wspólne zastanowienie się nad jego przyczynami i poszukanie rozwiązania sytuacji konfliktowej;
   - sprawca powinien otrzymać jasny i zdecydowany komunikat o tym, że szkoła nie akceptuje żadnych form przemocy;
   - należy omówić z uczniem skutki jego postępowania i poinformować o konsekwencjach regulaminowych, które zostaną wobec niego zastosowane;
   - sprawca powinien zostać zobowiązany do zaprzestania swojego działania i usunięcia z sieci szkodliwych materiałów;
   - ważnym elementem rozmowy jest też określenie sposobów zadośćuczynienia wobec ofiary cyberprzemocy;
   - jeśli w zdarzeniu brała udział większa grupa uczniów, należy rozmawiać z każdym z nich z osobna, zaczynając od lidera grupy;
   - nie należy konfrontować sprawcy i ofiary cyberprzemocy.

2. Powiadomienie rodziców sprawcy i omówienie z nimi zachowania dziecka:
   - rodzice sprawcy powinni zostać poinformowani o przebiegu zdarzenia i zapoznani z materiałem dowodowym, a także z decyzją w sprawie dalszego postępowania i podjętych przez szkołę środkach dyscyplinarnych wobec ich dziecka.

3. Objęcie sprawcy opieką psychologiczno-pedagogiczną:
   - praca ze sprawcą powinna zmierzać w kierunku pomocy uczniowi w zrozumieniu konsekwencji swojego zachowania, zmiany postawy i postępowania ucznia, w tym sposobu korzystania z nowych technologii;
   - jeśli szkoła posiada odpowiednie warunki, pomoc psychologiczna może być udzielona sprawcy na terenie szkoły;
   - w uzasadnionym przypadku można w toku interwencji zaproponować uczniowi (za zgodą rodziców) skierowanie do specjalistycznej placówki i udział w programie terapeutycznym.

CO MOŻE POMÓC W IDENTYFIKACJI SPRAWCY?

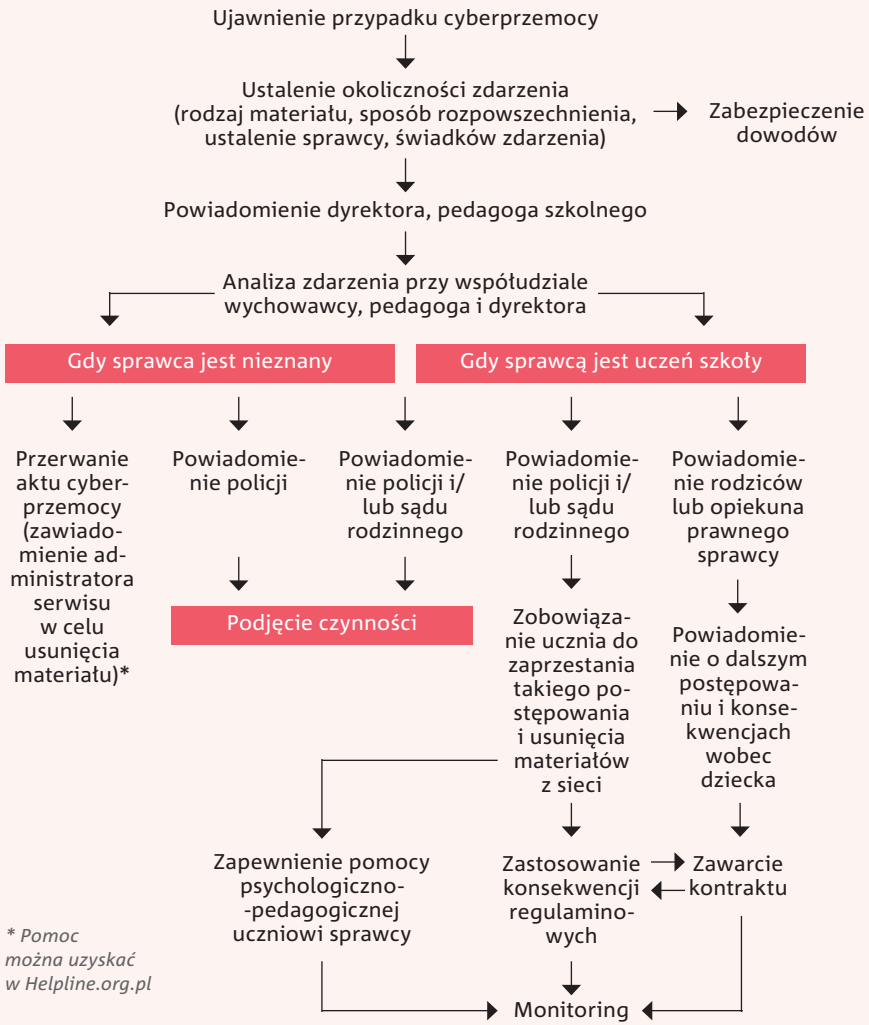
1. Świadkowie – inni uczniowie odwiedzający „obraźliwe" strony mogą posiadać informacje na temat ich autora, mogą też zidentyfikować numer telefonu komórkowego sprawcy, jeśli nie jest on zastrzeżony.
2. Kontakt z dostawcą usługi internetowej – może on nie tylko zablokować konto agresora lub usunąć szkodliwe treści, ale także podać dane sprawcy cyberprzemocy. Dane takie nie mogą być jednak udostępniane osobom prywatnym. Aby je pozyskać, konieczny jest kontakt z policją.
3. Kontakt z operatorem sieci komórkowej w przypadku, gdy numer telefonu sprawcy jest zastrzeżony – może on podjąć kroki w kierunku ustalenia sprawcy, jeśli otrzyma dane o dacie i godzinie rozmowy. Również w tym przypadku operator może udostępnić te dane tylko policji.
   - w miarę możliwości należy starać się pozyskać rodziców do współpracy i ustalić jej zasady;
   - warto wspólnie z rodzicami opracować projekt kontraktu dla dziecka, określającego zobowiązania ucznia, rodziców i przedstawiciela szkoły oraz konsekwencje nieprzestrzegania przyjętych wymagań i terminy realizacji zadań zawartych w umowie.

Zastosowanie środków dyscyplinarnych wobec sprawcy cyberprzemocy

1. Cyberprzemoc powinna podlegać sankcjom określonym w wewnętrznych przepisach szkoły. Szkoła może tu stosować konsekwencje przewidziane dla sytuacji „tradycyjnej" przemocy. Warto jednak rozszerzyć repertuar dostępnych środków, np. o czasowy zakaz korzystania ze szkolnej pracowni komputerowej w czasie wolnym i przynoszenia do szkoły akcesoriów elektronicznych (PSP, mp3) itp.
2. Należy pamiętać, iż celem sankcji wobec sprawcy jest:
   - zatrzymanie przemocy i zapewnienie poczucia bezpieczeństwa poszkodowanemu uczniowi;
   - wzbudzenie refleksji na temat jego zachowania, zrozumienie krzywdy, jaką spowodował i powstrzymanie przed podobnym zachowaniem w przyszłości;
   - pokazanie społeczności szkolnej, że cyberprzemoc nie będzie tolerowana i że szkoła jest w stanie efektywnie zareagować w tego rodzaju sytuacji.
3. Podejmując decyzję o rodzaju kary, należy wziąć pod uwagę:
   - rozmiar i rangę szkody – czy materiał został upubliczniony w sposób pozwalający na dotarcie do niego wielu osobom (określa to rozmiar upokorzenia, jakiego doznaje ofiara), czy trudno jest wycofać materiał z sieci itp.;
   - czas trwania prześladowania – czy było to długotrwałe działanie czy pojedynczy incydent;
   - świadomość popełnianego czynu – czy działanie było zaplanowane, a sprawca był świadomy, że wyrządza krzywdę koledze (niektóre akty

cyberprzemocy popełniane są nieświadomie lub z niewielką świadomością konsekwencji), jak wiele wysiłku włożył w ukrycie swojej tożsamości itp.;
- motywację sprawcy – należy sprawdzić, czy działanie sprawcy nie jest działaniem odwetowym w odpowiedzi na uprzednio doświadczone prześladowanie;
- rodzaj rozpowszechnianego materiału.

PROCEDURA REAGOWANIA WOBEC SPRAWCY CYBERPRZEMOCY



** Pomoc można uzyskać w Helpline.org.pl*

Działania wobec ofiary cyberprzemocy

1. Wsparcie psychiczne

Podobnie jak w przypadku innych form przemocy, ofiara cyberprzemocy potrzebuje pomocy i emocjonalnego wsparcia ze strony dorosłych. Musi także wiedzieć, że szkoła podejmie odpowiednie kroki w celu rozwiązania problemu.

PODCZAS ROZMOWY Z UCZNIEM OFIARĄ CYBERPRZEMOCY:

- zapewnij go, że dobrze zrobił, mówiąc ci o tym, co się stało,
- powiedz, że widzisz i rozumiesz, że jest mu trudno ujawnić to, co go spotkało,
- powiedz mu, że nikt nie ma prawa tak się zachowywać wobec niego,
- zapewnij go, że szkoła nie toleruje żadnej formy przemocy i że postarasz się mu pomóc, uruchamiając odpowiednie procedury interwencyjne,
- bądź uważny na pozawerbalne przejawy uczuć dziecka – zażenowanie, skrępowanie, wstyd, lęk, przerażenie, smutek, poczucie winy.

2. Porada

Uczeń będący ofiarą cyberprzemocy powinien otrzymać poradę, jak ma się zachować, aby zapewnić sobie poczucie bezpieczeństwa i nie doprowadzić do eskalacji prześladowania.

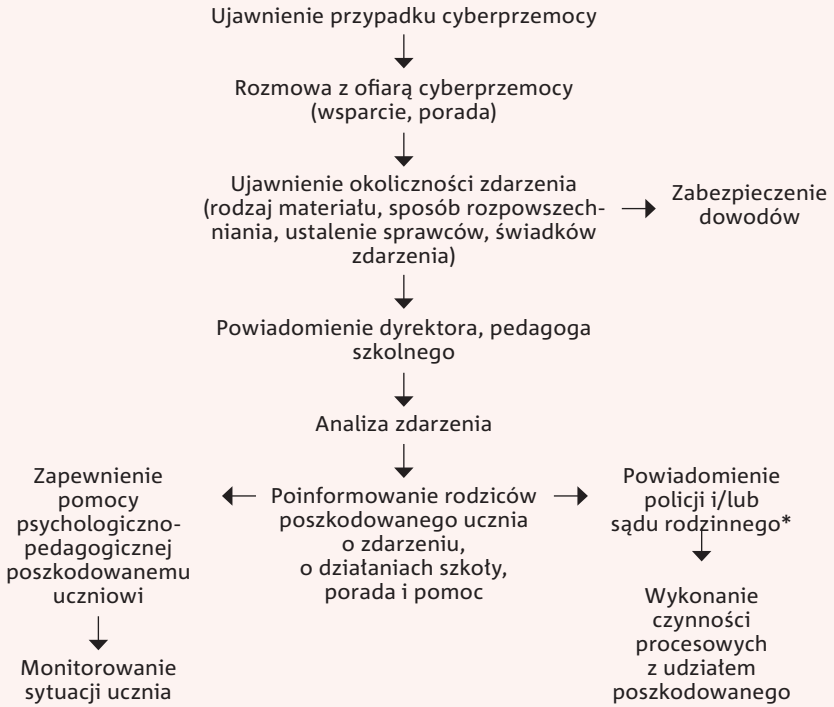
PORADŹ UCZNIOWI, ABY:

- nie utrzymywał kontaktu ze sprawcą, nie odpowiadał na maile, telefony itp.;
- nie kasował dowodów: e-maili, SMS-ów, MMS-ów, zdjęć, filmów i przedstawił je tobie lub innej osobie dorosłej;
- zastanowił się nad zmianą swoich danych kontaktowych w komunikatorach, zmianą adresu e-mail, numeru telefonu komórkowego itp.;
- jeśli korzysta z komunikatora, to ustawił go tak, żeby nikt spoza listy kontaktów nie mógł się z nim połączyć.

3. Monitoring

- Po zakończeniu interwencji warto monitorować sytuację ucznia, sprawdzając, czy nie są wobec niego podejmowane dalsze działania przemocowe bądź odwetowe ze strony sprawcy.
- Rodzice dziecka będącego ofiarą cyberprzemocy powinni być poinformowani o problemie i otrzymać wsparcie i pomoc ze strony szkoły. W rozmowie z nimi pedagog lub wychowawca przedstawiają kroki, jakie zostały podjęte w celu wyjaśnienia zajścia oraz zapewnienia bezpieczeństwa poszkodowanemu uczniowi, a także, jeśli to wskazane, zaproponować rodzicom i dziecku pomoc specjalisty (psychologa, pedagoga).

PROCEDURA REAGOWANIA WOBEC OFIARY CYBERPRZEMOCY



** Szkoła jest zobowiązana do powiadomienia policji i/lub sądu rodzinnego w przypadku przestępstw ściganych z urzędu*

Ochrona świadków zgłaszających zdarzenie

Profesjonalną opieką należy otoczyć także świadków zdarzenia uczestniczących w ustalaniu przebiegu zajścia. Osoby podejmujące działania interwencyjne muszą mieć świadomość skutków, jakie działania te niosą nie tylko dla ofiar, ale i świadków zdarzeń.

1. Ważne jest, by w wyniku interwencji nie narazić ich na zemstę i groźby ze strony sprawcy. Osoba, której uczeń zaufał, informując o jakimkolwiek akcie przemocy, a więc także cyberprzemocy, ma obowiązek postępować tak, by swoim zachowaniem i działaniem nie narazić świadka zgłaszającego problem.
2. Postępowanie interwencyjne wymaga od wyjaśniającego sprawę dyskrecji i poufnego postępowania. Występowaniu w roli świadka często towarzyszą dramatyczne przeżycia – uczniowie boją się, że sami również mogą się stać obiektem prześladowań, obawiają się etykiety „donosiciela". Pedagog powinien wzbudzić swoim zachowaniem zaufanie i poczucie bezpieczeństwa u takiego ucznia oraz wykazać dla niego zrozumienie i empatię.

3. Niedopuszczalne jest stosowanie konfrontacji świadka ze sprawcą jako metody wyjaśniania sprawy czy ostentacyjne wywoływanie go z lekcji celem złożenia zeznań, ze względu na bezpieczeństwo i nienarażanie go na odwet ze strony agresora. Zaniedbanie tego rodzaju podstawowych zasad bezpieczeństwa może sprawić, że następnym razem uczeń nie podejmie działań na rzecz obrony słabszych i pokrzywdzonych i nie zgłosi zagrażającego zdarzenia.

JAK SIĘ ZACHOWAĆ WOBEC ŚWIADKA ZGŁASZAJĄCEGO CYBERPRZEMOC?

1. Powiedz, że dobrze zrobił, zgłaszając fakt przemocy.
2. Powiedz, że wymagało to od niego wiele odwagi.
3. Zapewnij o swojej dyskrecji.
4. Nie ujawniaj jego danych, jeśli nie jest to konieczne (np. gdy sprawa została zgłoszona na policję).
5. Pod żadnym pozorem nie konfrontuj go ze sprawcą.
6. Zadbaj o jego bezpieczeństwo, nie upubliczniając jego udziału w sprawie.

Sporządzenie dokumentacji z zajścia

1. Pedagog szkolny jest zobowiązany do sporządzenia notatki służbowej z rozmów ze sprawcą, poszkodowanym, ich rodzicami oraz świadkami zdarzenia. Dokument powinien zawierać datę i miejsce rozmowy, personalia osób biorących w niej udział i opis ustalonego przebiegu wydarzeń.
2. Jeśli rozmowa przebiegała w obecności świadka (np. wychowawcy), powinien on podpisać notatkę po jej sporządzeniu.
3. Jeśli zostały zabezpieczone dowody cyberprzemocy, należy je również włączyć do dokumentacji pedagogicznej (wydruki, opis itp.).

Współpraca szkoły z policją i sądem rodzinnym

Praca wychowawcza i profilaktyczna szkoły polega między innymi na utrzymywaniu kontaktów z przedstawicielami organów ścigania oraz z sądem rodzinnym. Większość przypadków cyberprzemocy nie wymaga powiadamiania sądu rodzinnego czy policji i powinna być rozwiązywana przy użyciu dostępnych szkole środków wychowawczych. Istnieją jednak sytuacje, gdy konieczne staje się zgłoszenie sprawy do sądu rodzinnego, a mianowicie:

1) jeśli rodzice sprawcy cyberprzemocy odmawiają współpracy lub nie stawiają się do szkoły, a uczeń nie zaniechał dotychczasowego postępowania, dyrektor szkoły powinien pisemnie powiadomić o zaistniałej sytuacji sąd rodzinny, szczególnie jeśli do szkoły napływają informacje o innych przejawach demoralizacji dziecka;
2) gdy szkoła wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje regulaminowe wobec ucznia, spotkania z pedagogiem itp.), a ich zastosowanie nie przynosi pożądanych rezultatów, dyrektor powinien zwrócić się do sądu rodzinnego z wnioskiem o podjęcie odpowiednich środków wynikających z ustawy o postępowaniu z nieletnimi.

W 2004 r. Rada Ministrów przyjęła Krajowy Program Zapobiegania Niedostosowaniu Społecznemu i Przestępczości wśród Dzieci i Młodzieży, który zawiera między innymi moduł współpracy szkół z policją. Zostały w nim przybliżone zadania szkoły w tym zakresie i możliwości jej współpracy z policją, gdy uczeń przejawia zachowania świadczące o demoralizacji bądź popełnieniu czynu karalnego.

Poważne przypadki cyberprzemocy przebiegające z naruszeniem prawa (np. groźby karalne, propozycje seksualne, publikowanie nielegalnych treści itp.) powinny zostać bezwzględnie zgłoszone na policję. Zgłoszenia dokonuje dyrektor szkoły.

W placówkach oświatowych wyznaczeni zostali koordynatorzy ds. bezpieczeństwa, którzy integrują działania wszystkich podmiotów szkolnych i współpracują również, obok dyrektora placówki, z policją (Uchwała Rady Ministrów nr 186/2006 w sprawie działalności administracji rządowej przeciwko przemocy w szkołach i placówkach). Pracownicy szkoły wyznaczeni do współpracy z policją, specjaliści ds. nieletnich oraz dzielnicowi powinni wspólnie ustalić wzajemnie zasady kontaktu, by móc na bieżąco wymieniać informacje i rozwiązywać problemy związane z bezpieczeństwem i dobrem uczniów.

W RAMACH OGÓLNEJ WSPÓŁPRACY SZKOŁY Z POLICJĄ MOGĄ BYĆ ORGANIZOWANE:

- spotkania pedagogów szkolnych, nauczycieli, dyrektora szkoły z zaproszonymi specjalistami ds. nieletnich, dotyczące zagrożeń cyberprzemocą w środowisku lokalnym;
- spotkania młodzieży szkolnej z udziałem policjantów, m.in. na temat odpowiedzialności nieletnich za popełniane czyny karalne, zasad bezpieczeństwa oraz sposobów unikania zagrożeń związanych z cyberprzemocą;
- wspólny udział (szkoły i policji) w lokalnych programach profilaktycznych, związanych z zapewnieniem bezpieczeństwa uczniom oraz zapobieganiem przemocy/cyberprzemocy i przestępczości nieletnich.

Obecność policji w szkole

Policja powinna być wzywana do szkoły w sytuacji, gdy ujawnione zostanie naruszenie prawa. W przypadku zagrożenia zdrowia lub życia policję należy wezwać natychmiast. Warto także zaprosić policjanta – specjalistę ds. nieletnich, gdy wyczerpane zostaną środki wychowawcze możliwe do zastosowania przez szkołę. Policja udziela pomocy szkole w rozwiązywaniu trudnych problemów, mogących mieć podłoże przestępcze.

Każda wizyta policjanta w szkole dotycząca uczniów powinna być wcześniej zasygnalizowana dyrektorowi lub uzgodniona z innym pracownikiem szkoły (koordynatorem ds. bezpieczeństwa).

Tekst został pierwotnie opublikowany w książce „Jak reagować na cyberprzemoc. Poradnik dla szkół", FDN 2008

W celu uzyskania porady dotyczącej możliwości dalszych działań w stosunku do sytuacji cyberprzemocy, metod zabezpieczania dowodów i wskazówek dotyczących bezpośredniej pomocy specjalistycznej zachęcamy do kontaktu z zespołem pomocy w sytuacjach zagrożenia bezpieczeństwa online **Helpline.org.pl**. Oferta ta skierowana jest zarówno do dzieci, młodzieży, rodziców, jak i profesjonalistów. Kontakt możliwy jest pod bezpłatnym numerem telefonu **800 100 100** oraz poprzez czat, od poniedziałku do piątku w godz. 12.00-18.00, jak również poprzez formularz *Zadaj nam pytanie* na stronie **www.helpline.org.pl** i e-mail **helpline@helpline.org.pl**.

PRZESTĘPSTWA ŚCIGANE NA WNIOSEK POSZKODOWANEGO:

- groźby – art. 190 kk
- naruszenie wizerunku – art. 23 i art. 24 kc
- naruszenie czci – art. 23 i art. 24 kc oraz art. 216 kk
- nękanie – art. 190a § 1 kk
- podszywanie – art. 190a § 2 kk
- wulgaryzmy – art. 140 i art. 141 kw

Uwodzenie

Łatwość komunikacji w internecie, dostęp do licznego grona potencjalnych znajomych – to niezaprzeczalne zalety internetu, ale jednocześnie ryzyko natrafienia na osobę o złych intencjach.

Specyficzną formą takich relacji jest grooming – proces uwodzenia dziecka w internecie przez osobę dorosłą w celu spotkania, wykorzystania seksualnego lub np. zaangażowania w produkcję pornografii. Polega na „oswajaniu" dziecka, przywiązywaniu go do sprawcy, który stopniowo zdobywa jego zaufanie, poruszając początkowo neutralne tematy i deklarując np. wspólne zainteresowania. Jednocześnie w celu ukrycia swojego działania przed bliskimi dziecka, przekonuje je do dochowania „wspólnej tajemnicy". Docelowo – nakłania do spotkania, prostytucji lub produkcji pornografii.

Warto przypomnieć, że według polskiego prawa kontakty seksualne z osobą poniżej 15 roku życia są przestępstwem. Dodatkowo, od 2010 roku Kodeks karny uwzględnia pojęcie „uwodzenia dzieci w internecie". By doszło do przestępstwa, nie jest więc konieczny bezpośredni kontakt ofiary i sprawcy. Ścigane jest już nawiązywanie kontaktu z osobą małoletnią w celu wykorzystania jej seksualnie lub produkcji pornografii.

Więcej informacji na temat regulacji prawnych dotyczących problemu wykorzystania seksualnego dziecka jest dostępnych na stronach FDN: ***dzieckowsieci.fdn.pl/wykorzystywanie-seksualne.***

Do nawiązania kontaktu w internecie z kimś nieznanym wcześniej przyznaje się blisko 70 proc. uczestników badania EU NET ADB. Ponad 30 proc. młodych ludzi spotkało się twarzą w twarz z osobą znaną jedynie z internetu. 9 proc. spośród nich deklaruje, że spotkanie to było dla nich nie-

pokojące. Według badania Ogólnopolska Diagnoza Problemu wobec Dzieci (FDN 2012), 5 proc. nastolatków w wieku 11-17 lat deklaruje, że zawarło w internecie znajomość, w ramach której próbowano ich skłonić do zachowań o charakterze seksualnym (6,5 proc. dziewcząt oraz 3,8 proc. chłopców).

W przypadku gdy w szkole ujawniono proceder uwiedzenia, często niezbędne jest wsparcie psychiczne ofiary. Warto zadbać, by nie doszło do jej wtórnej wiktymizacji – ofiara została już skrzywdzona przez sprawcę, od wrażliwości i empatii osób zajmujących się sprawą zależy, czy nie dozna dodatkowych krzywd wynikających np. z próby ustalenia okoliczności zdarzenia.

*Więcej informacji na temat problemu uwodzenia dzieci w internecie jest dostępnych w broszurze „**Zapobieganie wykorzystywaniu seksualnemu dzieci w Internecie**” (dzieckowsieci.fdn.pl/materialy-do-pobrania-przeglad).*

PROCEDURA REAGOWANIA NA ZGŁOSZENIA DOTYCZĄCE NIEBEZPIECZNYCH KONTAKTÓW/GROOMINGU W SZKOLE

1. **Ujawnienie przypadku uwodzenia.** Informacja o niebezpiecznych kontaktach podejmowanych przez ucznia/uczennicę może dotrzeć do nauczyciela/pedagoga z różnych źródeł. Zdarzenie może być zgłoszone przez osobę nawiązującą niebezpieczny kontakt, jej rodziców, świadków lub innych nauczycieli.
2. **Rozmowa z uczniem.** Zebranie informacji na temat sytuacji uwodzenia, jego formy, miejsca wystąpienia, czasu trwania, sprawcy i ofiary.
3. **Ustalenie okoliczności zdarzenia.**
   - Poinformowanie o fakcie przemocy wychowawcę klasy, pedagoga/psychologa szkolnego i dyrektora.
   - Zabezpieczenie dostępnych dowodów i zebranie informacji na temat zagrożenia bezpieczeństwa dziecka, jego formy, częstotliwości i miejsca wystąpienia (niezależnie od okoliczności zdarzenia i znalezionych dowodów, osoby te powinny być poinformowane o tym, co miało miejsce).
   - Ustalenie okoliczności zdarzenia: identyfikacja sprawcy i ofiary zdarzenia.
4. **Powiadomienie rodziców ucznia/uczennicy o zdarzeniu i zapoznanie, w miarę możliwości, z materiałem dowodowym;** podjęcie współpracy z rodzicami w celu udzielenia wsparcia dziecku.
5. **Zapewnienie na terenie szkoły wsparcia psychologicznego krzywdzonemu dziecku bądź polecenie specjalistycznej placówki.**
6. **Wsparcie informacyjne.** W celu uzyskania porady dotyczącej możliwości dalszych działań w stosunku do sytuacji uwodzenia dziecka w sieci, informacji dotyczącej zabezpieczania dowodów, wskazówek dotyczących bezpośredniej pomocy specjalistycznej, zachęcamy do kontaktu z zespołem pomocy w sytuacjach zagrożenia bezpieczeństwa online **Helpline.org.pl**. Oferta skierowana jest do dzieci i młodzieży, rodziców, jak i profesjonalistów. Kontakt możliwy jest pod bezpłatnym numerem telefonu **800 100 100** oraz przez czat, od poniedziałku do piątku w godz. 12.00-18.00, jak również poprzez formularz: *Zadaj nam pytanie* na stronie **www.helpline.org.pl** i e-mail: **helpline@helpline.org.pl**.
7. **Podjęcie interwencji prawnej.** Interwencja prawna przeprowadzona przez szkołę możliwa jest w przypadku naruszenia prawa:
   - naruszenie wizerunku (publikowanie wizerunku nagiej osoby małoletniej – rozpowszechnienie pornografii z udziałem małoletniego) – art. 202 § 3 kk, w przypadku groomingu interwencja jest możliwa na podstawie art. 200a kk.

   W sytuacji podejrzenia groomingu zaleca się konsultację z organami ścigania i ewentualne zawiadomienie dotyczące podejrzenia popełnienia przestępstwa.
8. **Dokumentacja zgłoszenia** (opis sytuacji – okoliczności, dowody, osoby biorące udział w zdarzeniu, podjęte działania; ustalenia z poszczególnymi uczniami).
9. **Monitorowanie sytuacji** (kontakt z poszkodowanym dzieckiem i jego rodzicami, upewnienie się, czy nie jest potrzebne udzielenie dalszego wsparcia).

Nadmierne korzystanie z internetu

Potoczne pojęcie „uzależnienie od internetu” jest podważane przez wielu naukowców, zastrzegających termin „uzależnienie” dla uzależnień fizjologicznych (od alkoholu, nikotyny, narkotyków). Lepiej więc w kontekście dysfunkcyjnych zachowań związanych z internetem mówić o jego nadużywaniu. Chociaż do nadużywania internetu dochodzi najczęściej poza szkołą, to nauczyciele mogą być pierwszymi osobami, które dostrzegą zagrożenie – zmieniające się zachowanie ucznia, wycofanie się z kontaktów z rówieśnikami, pojawiające się problemy w nauce. Z tego też powodu szkoła powinna zareagować – oczywiście w porozumieniu z rodzicami.

Czas spędzany w internecie nie jest jedynym kryterium rozpoznania tego problemu. By mówić o nadużywaniu internetu, powinny być spełnione dwa kryteria:

1. czas i intensywność korzystania z sieci wymyka się spod kontroli, użytkownik spędza w internecie więcej czasu niż zamierzał, odczuwa nieodpartą potrzebę korzystania z sieci;
2. korzystanie z internetu prowadzi do zaniedbywania innych aspektów życia, rodzi problemy na różnych płaszczyznach, powoduje cierpienie – uzależnionego lub osób z jego otoczenia.

Według badania EU NET ADB kryteria, które pozwalają mówić o nadużywaniu internetu, spełnia 1,3 proc. młodzieży. Osoby wykazujące tylko część symptomów – zagrożone nadużywaniem – to 12,1 proc. W sumie to 13,4 proc. osób dysfunkcyjnie korzystających z sieci. Nadużywanie internetu jest bardziej powszechne wśród chłopców niż dziewcząt (odpowiednio 1,8 i 0,8 proc.).

Pojęcie nadużywania sieci może dotyczyć różnych obszarów: gier internetowych, portali społecznościowych i komunikatorów, pornografii i cyberseksu, hazardu online. Zazwyczaj u podłoża nadużywania internetu leżą złożone czynniki. Tak jak w przypadku innych uzależnień, ucieczka w internet może być rodzajem niekonstruktywnej strategii radzenia sobie ze stresem, chęcią oderwania się od niepowodzeń, odrzucenia przez grupę rówieśniczą, konfliktów w rodzinie. To jednocześnie błędne koło – nadmierne zaangażowanie się w aktywność w internecie rodzi kolejne problemy, nie rozwiązując poprzednich. Podkreślane są również czynniki osobowościowe korelujące z nadmiernym używaniem internetu:

- depresja;
- introwersja, neurotyzm, nadmierna wrażliwość, nieśmiałość;
- współwystępowanie innych nałogów;
- niska samoocena, przeżywanie niepewności, niskie poczucie sprawstwa;
- negatywne strategie radzenia sobie ze stresem.

*Więcej informacji na temat nadużywania internetu znajduje się w broszurze „**Nadmierne korzystanie z komputera i Internetu przez młodzież i dzieci**", dostępnej na stronie: dzieckowsieci.fdn.pl/nadmierne-korzystanie lub dzieckowsieci.fdn.pl/materialy-do-pobrania-przeglad.*

PROCEDURA REAGOWANIA NA ZGŁOSZENIA DOTYCZĄCE NADUŻYWANIA INTERNETU

1. **Ujawnienie przypadku nadużywania internetu.** Informacja o nadmiernym korzystaniu z sieci lub komputera może dotrzeć do nauczyciela/pedagoga z różnych źródeł: może być zgłoszona przez ucznia, rodziców, innych nauczycieli.
2. **Rozmowa z uczniem.** Zebranie informacji na temat podejrzeń o nadużywaniu internetu, jego formy oraz częstotliwości.
3. **Kontakt z rodzicami.** Poinformowanie opiekunów o obserwacjach dotyczących dziecka.
4. **Zapewnienie wsparcia psychologicznego dziecku na terenie szkoły bądź polecenie specjalistycznej placówki.**
5. **Wsparcie informacyjne** dotyczące możliwości dalszych działań w sytuacji nadużywania internetu, informacje dotyczące bezpośredniej pomocy specjalistycznej. Przekazanie kontaktu do zespołu pomocy w sytuacjach zagrożenia bezpieczeństwa online **Helpline.org.pl**. Kontakt z zespołem jest możliwy pod bezpłatnym numerem telefonu **800 100 100** oraz poprzez czat, od poniedziałku do piątku w godz. 12.00-18.00, jak również poprzez formularz: *Zadaj nam pytanie* na stronie **www.helpline.org.pl** i e-mail: **helpline@helpline.org.pl**.
6. **Podjęcie interwencji prawnej.**
   Większość sytuacji związanych z nadużywaniem internetu bądź komputera nie wymaga powiadamiania sądu rodzinnego. Zgłoszenie sprawy do sądu rodzinnego jest jednak wskazane:
   - jeśli rodzice dziecka odmawiają współpracy i nie kontaktują się ze szkołą, a uczeń nie zaprzestaje działań, które są dla niego krzywdzące i skutkują niewywiązywaniem się z obowiązku szkolnego. W takiej sytuacji dyrektor szkoły powinien zwrócić się do sądu rodzinnego z wnioskiem o podjęcie odpowiednich środków wynikających z ustawy o postępowaniu z nieletnimi.
7. **Dokumentacja zgłoszenia** (opis podjętych przez szkołę działań, np. kontakt z rodzicami, rozmowa z uczniem, zaproponowanie pomocy psychologicznej poza szkołą).
8. **Monitorowanie sytuacji** (kontakt z poszkodowanym dzieckiem i jego rodzicami, upewnienie się, czy nie jest np. potrzebne dalsze wsparcie; sprawdzanie, jak realizuje obowiązek szkolny, czy bierze udział we wszystkich zajęciach).

Niebezpieczne treści

Pojęcie niebezpieczne (szkodliwe) treści jest określeniem szerszym niż treści nielegalne. Polskie prawo za nielegalne uznaje materiały zawierające pornografię dziecięcą, pornografię związaną z prezentowaniem przemocy lub posługiwaniem się zwierzęciem, propagowanie faszystowskiego lub innego totalitarnego ustroju, szerzenie nienawiści wobec jednostki lub grupy społecznej ze względu na jej pochodzenie, kulturę, wyznanie lub ze względu na jej bezwyznaniowość. Lista materiałów uznawanych za szkodliwe jest dłuższa, obejmuje te, które mogą wywrzeć negatywny wpływ na niedojrzałą psychikę młodych ludzi. Do treści szkodliwych zalicza się: materiały promujące samookaleczanie, samobójstwa, skrajne odchudzanie, rozpowszechniające nienawiść, promujące zażywanie narkotyków.

Do kontaktu z treściami szkodliwymi przyznaje się 22 proc. gimnazjalistów (TNS 2013). 16,9 proc. ogółu deklaruje, że trafiła na nie przypadkiem, 4,6 proc. przyznaje, że poszukiwała ich świadomie. Z kolei 67 proc. uczestników badania EU NET ADB twierdzi, że miało w internecie kontakt z pornografią, u 1/3 z nich wywołało to zaniepokojenie. Najczęściej młodzi ludzie trafiają na strony związane z szerzeniem nienawiści i agresywnymi atakami słownymi. Kolejne pozycje to strony promujące zachowania autodestrukcyjne: skrajne odchudzanie (28,6 proc.), narkotyki (24,1 proc.), samookaleczenia (22,3 proc.) oraz samobójstwa (15,6 proc.).

Uczniowie dostęp do treści nielegalnych lub szkodliwych mogą uzyskać albo za pomocą szkolnego komputera (np. w trakcie lekcji), albo prywatnych urządzeń. Nawet najlepsze filtry zainstalowane w szkolnej infrastrukturze nie są w stanie zapewnić 100-procentowej skuteczności blokowania niepożądanych treści. W tej sytuacji znaczenia nabiera ograniczenie skali, w jakiej materiały zostaną rozpowszechnione wśród uczniów.

W przypadku kontaktu z treściami nielegalnymi w internecie, należy je zgłosić do Dyżurnet.pl – punktu kontaktowego, którego celem jest reagowanie na treści wymierzone w bezpieczeństwo dzieci i młodzieży. Zgłoszenia można dokonać anonimowo.

PROCEDURA REAGOWANIA NA ZGŁOSZENIA DOTYCZĄCE SZKODLIWYCH TREŚCI W SZKOLE

1. **Ujawnienie przypadku pojawienia się szkodliwych treści w szkole.** Informacja o kontakcie uczniów ze szkodliwymi treściami może dotrzeć do nauczyciela/pedagoga z różnych źródeł: od samych uczniów, ich rodziców lub innych nauczycieli.
2. **Ustalenie okoliczności zdarzenia.**
   - **Poinformowanie o fakcie rozpowszechniania szkodliwych treści** wychowawcy klasy, pedagoga/psychologa szkolnego i dyrektora.
   - **Zabezpieczenie dowodów.** Zebranie informacji na temat szkodliwych treści, miejsca ich wystąpienia oraz ewentualnych sprawców. Wydrukowanie i zapisanie w formie zrzutów ekranu wszystkich dowodów rozpowszechniania niewskazanych obrazów w sieci; zachowanie SMS-ów. Jeśli treści są nielegalne, nieodpowiednio zabezpieczone lub niezgodne z regulaminem danej strony – kontakt z administratorem strony.
   - **Ustalenie okoliczności zdarzenia: identyfikacja sprawcy zdarzenia** (osoby, która rozpowszechniała szkodliwe treści)**, ustalenie, kim są świadkowie zdarzenia.**
     Klasyfikacja szkodliwych treści: pornograficzne promujące nienawiść, rasizm, ksenofobię, przemoc; promujące zachowania antyspołeczne lub autodestrukcyjne; psychomanipulacja.
   - **Współpraca z pracownikiem/nauczycielem zarządzającym dostępem do sieci w szkole.** Pomoc w zabezpieczeniu dowodów, konfiguracji zabezpieczeń sieci szkolnej blokujących dostęp do szkodliwych materiałów.
3. **Diagnoza potrzeb i działania wobec uczniów zaangażowanych w rozpowszechnianie szkodliwych treści** (edukacja, warsztaty z grupą/klasą lub rozmowa na temat treści, jeżeli np. mają negatywny wpływ na rozwój poznawczy, emocjonalny i są np. psychomanipulacją).
4. **Zdecydowany komunikat ze strony szkoły, że takie materiały nie są w szkole akceptowane.**
5. **Działania wobec sprawcy i osób uczestniczących.** Ustalenie okoliczności zdarzenia; rozmowa/spotkanie uczniów z nauczycielem/pedagogiem na temat przesyłanych treści (jakie emocje budzi prezentowany materiał, do jakich działań ich zachęca i jak wpływa na wyobrażenia na temat otaczającego świata); omówienie konsekwencji zdarzenia dla osób mających kontakt ze szkodliwymi treściami – w tym też konsekwencji wynikających ze złamania regulaminu szkoły.
6. **Rozmowa z uczestnikami zdarzenia (z każdym osobno).** Jeżeli szkodliwe treści rozpowszechnia grupa uczniów, działania interwencyjne warto zacząć od lidera grupy.
7. **Powiadomienie rodziców uczniów o wydarzeniu** i zapoznanie, w miarę możliwości, z materiałem dowodowym. Poinformowanie rodziców o działaniach podjętych przez szkołę wobec ucznia i podjęcie współpracy z rodzicami w celu rozwiązania problemu.
8. **Zapewnienie pomocy psychologiczno-pedagogicznej uczestnikom zdarzenia.**
9. **Wsparcie informacyjne** dotyczące możliwych działań wobec szkodliwych treści, informacja dotycząca formy ich zgłaszania do Dyżurnet.pl (punkt kontaktowy zajmujący się zwalczaniem nielegalnych treści w internecie), zabezpieczania dowodów.
10. **Podjęcie interwencji prawnej.**
    Interwencja prawna przeprowadzona przez szkołę możliwa jest w przypadku naruszenia zakazu rozpowszechniania:
    - pornografii z udziałem małoletniego **– art. 202 § 3 kk**
    - treści propagujących publicznie faszystowski lub inny totalitarny ustrój państwa lub nawołujących do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych **– art. 256 i art. 257 kk.**

    Inne formy interwencji:
    - kontakt z administratorem/moderatorem w sytuacji, gdy treści są nielegalne, nieodpowiednio zabezpieczone lub niezgodne z regulaminem danej strony.
11. **Dokumentacja zgłoszenia.**

Oferta edukacyjna programu „Dziecko w Sieci”

W ramach programu „Dziecko w Sieci” Fundacji Dzieci Niczyje opracowywane są propozycje zajęć edukacyjnych z zakresu bezpieczeństwa dzieci w internecie. Oferta tworzona jest w nawiązaniu do idei blended learningu, łącząc nauczanie tradycyjne (bezpośrednie, oparte na gotowych scenariuszach zajęć lekcyjnych) z nauczaniem przez komputer (kursy e-learning oraz serwisy internetowe dla dzieci **www.sieciaki.pl** i **www.necio.pl**). Scenariusze zajęć oraz kursy e-learning mogą być wykorzystywane podczas zajęć szkolnych, pozaszkolnych lub imprez edukacyjnych. Do ich prowadzenia wymagana jest jedynie podstawowa znajomość internetu.

Zajęcia edukacyjne dla dzieci i młodzieży
Oferta edukacyjna programu „Dziecko w Sieci” została opracowana dla następujących grup wiekowych:
- przedszkola,
- klasy I-III szkół podstawowych,
- klasy IV-VI szkół podstawowych,
- szkoły gimnazjalne,
- szkoły ponadgimnazjalne.

Materiały edukacyjne programu „Dziecko w Sieci” dostępne są na stronie: **dzieckowsieci.fdn.pl**, a zajęcia e-learningowe na platformie: **fdn.pl/kursy**

Oferta edukacyjna dla przedszkoli i klas I-III szkół podstawowych

ZAJĘCIA **„NECIO.PL – ZABAWA W INTERNET”**
Scenariusze zajęć dla dzieci w wieku 4-6 lat, podczas których najmłodsi zapoznają się z Neciem, bohaterem serwisu www.necio.pl, oraz z podstawowymi pojęciami związanymi z komputerem i internetem. Słuchając bajki, ucząc się piosenki, wykonując ćwiczenia, dzieci poznają zasady działania internetu, oswajają się z klawiaturą komputerową, a także dowiadują się, co robić w sytuacji zagrożenia w sieci. Zajęcia mogą być realizowane zarówno w przedszkolach, jak i w klasach zerowych i pierwszych szkoły podstawowej. Podstawowym celem zajęć jest zapoznanie dzieci z internetem oraz uwrażliwienie ich na zagrożenia związane z korzystaniem z sieci.

ZAJĘCIA LEKCYJNE **„OWCE W SIECI”**
Scenariusze zajęć z wykorzystaniem serii 3-minutowych 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, obecny styl życia. Zakończenie każdej bajki zawiera morał, mówiący jak uniknąć zagrożeń.

ZAJĘCIA LEKCYJNE **„SIECIAKI”**
Podczas lekcji dzieci oglądają trzy kreskówki, w których przez pryzmat przygód Sieciaków (grupy dzieci zwalczających w internecie złe Sieciuchy), poznają podstawowe zagrożenia internetowe oraz zasady bezpiecznego korzystania z sieci. Proponowane w scenariuszu formy aktywności dzieci to: burza mózgów, konkursy, ćwiczenia. Scenariusz zajęć jest dostępny w dwóch wersjach: pełnej (dwie jednostki lekcyjne) oraz skróconej (jedna jednostka lekcyjna).

ZAJĘCIA LEKCYJNE **„SIECIAKOWA SZKOŁA”**
Zestaw 12 scenariuszy zajęć (każdy obejmujący dwie lekcje), poświęconych bezpieczeństwu dzieci w internecie, pozwalających na wykorzystanie serwisu Sieciaki.pl jako narzędzia edukacyjnego. Podczas zajęć nauczyciel, odwołując się do wybranych treści z serwisu, omawia m.in.: reguły rejestracji w serwisach internetowych, netykietę, zasady bezpieczeństwa w internecie. Ponadto scenariusze podejmują tematykę: cyberprzemocy, niebezpiecznych treści, uzależnienia od komputera i internetu, wirusów komputerowych, a także zakupów w sieci. W trakcie zajęć wykorzystywane są m.in.: ćwiczenia grupowe i indywidualne, quizy, audycje radiowe, pokazy filmów.

ZAJĘCIA LEKCYJNE **„ZUŹKA I TUNIO POZNAJĄ INTERNET”**
Zajęcia „Zuźka i Tunio poznają Internet”, wykorzystując kreskówki i łamigłówki, zapoznają dzieci z podstawowymi mechanizmami funkcjonowania sieci oraz zasadami bezpiecznego i efektywnego korzystania z internetu. Scenariusz zajęć dostępny jest w dwóch wersjach: pełnej (dwie jednostki lekcyjne) i skróconej (jedna jednostka lekcyjna).

KURS E-LEARNING **„POZNAJ BEZPIECZNY INTERNET”**
Kurs składa się z 8 modułów, w których dzieci poznają podstawowe zasady bezpieczeństwa w internecie. Zadaniem użytkownika kursu jest zdobycie 7 stopni wtajemniczenia i dołączenie do drużyny Sieciaków. Kurs przewidziany jest na trzy jednostki lekcyjne.

Oferta edukacyjna dla klas IV-VI szkół podstawowych

ZAJĘCIA LEKCYJNE **„3... 2... 1... INTERNET!”**
Zajęcia dotyczące szerokiego spektrum zagrożeń internetowych, m.in. przemocy rówieśniczej, kontaktów z obcymi i uzależnienia od komputera. W ich trakcie dzieci oglądają pięć odcinków kreskówki, przedstawiającej przygody grupy uczniów szkoły podstawowej. Każdy z odcinków ma alternatywne zakończenie – bezpieczne i ryzykowne. Wybór należy do uczniów. W trakcie zajęć dzieci biorą udział w ćwiczeniach indywidualnych i grupowych. W prezentacji wykorzystywanej podczas zajęć występuje Krzysztof Hołowczyc, który zapowiada i podsumowuje prezentowane filmy. Zajęcia przewidziane są na dwie jednostki lekcyjne.

ZAJĘCIA LEKCYJNE **„3... 2... 1... INTERNET!” W WERSJI DLA NIESŁYSZĄCYCH**
Z myślą o dzieciach niesłyszących opracowana została specjalna wersja zajęć „3... 2... 1... Internet!” – dubbingowana w Polskim Języku Migowym. Każdej postaci kreskówki towarzyszy tłumacz przekładający jej słowa na język migowy.

KURS E-LEARNING **„3... 2... 1... INTERNET!”**
Kurs, podobnie jak zajęcia lekcyjne, oparty jest na przygodach piątki uczniów szkoły podstawowej. Przez pryzmat losów bohaterów użytkownik zapoznaje się z różnymi formami zagrożeń związanych z internetem. Kurs składa się z siedmiu modułów, w których prezentowanych jest pięć części kreskówki, uzupełnionych wprowadzeniem i podsumowaniem Krzysztofa Hołowczyca. Każda z kreskówek ma alternatywne zakończenie, dzięki czemu użytkownik może natychmiast poznać konsekwencje swoich wyborów.

KURS E-LEARNING **„BEZPIECZNA PRZYGODA Z INTERNETEM”**
Kurs składa się z 7 modułów. W trakcie ich realizacji dzieci poznają zasady bezpieczeństwa w sieci oraz konsekwencje ryzykownych zachowań. Zadaniem użytkownika jest przejście przez 7 komnat, zdobycie 7 dysków wiedzy i dołączenie do drużyny Sieciaków. Kurs przewidziany jest na trzy jednostki lekcyjne.

Oferta edukacyjna dla klas V-VI szkół podstawowych i I gimnazjalnych

ZAJĘCIA **„LEKCJA BEZPIECZEŃSTWA”**
Zajęcia przeznaczone dla dzieci w wieku 11-13 lat. Ich celem jest zapoznanie uczniów z zagrożeniami prywatności w sieci, pokazanie konsekwencji nierozważnych działań online, takich jak: wysyłanie i publikowanie „odważnych” zdjęć oraz lekkomyślne zamieszczanie w sieci innych treści, przyjmowanie do grona „znajomych” osób bliżej nieznanych, niewylogowywanie się z konta, udostępnianie haseł i loginów, ignorowanie ustawień prywatności w portalach społecznościowych itp. Podsumowaniem zajęć są wypracowane zasady bezpiecznego korzystania z sieci. Zajęcia przewidziane na jedną godzinę dydaktyczną (45 minut).

KURS E-LEARNING **„LEKCJA BEZPIECZEŃSTWA”**
Kurs jest przeznaczony dla uczniów w wieku 11-13 lat. Jego treścią są historie dotyczące prywatności w sieci, przytaczane przez uczniów jednego z gimnazjów. Każde zagadnienie podsumowywane jest przez konsultantkę Helpline.org.pl. Celem kursu jest zapoznanie uczniów z zagrożeniami prywatności w sieci, pokazanie konsekwencji nierozważnych działań online oraz wypracowanie zasad bezpiecznego korzystania z internetu, jak również prezentacja możliwych sposobów reagowania w sytuacji zagrożenia prywatności online. Czas trwania: około 25 minut.

ZAJĘCIA LEKCYJNE **„GDZIE JEST MIMI?”**
Scenariusz zajęć przeznaczonych dla uczniów w wieku 11-13 lat, poświęconych cyberprzemocy. Ich celem jest zapoznanie uczniów ze specyfiką cyberprzemocy, pokazanie jej możliwych konsekwencji (zarówno dla ofiar, jak i sprawców) oraz prezentacja metod rozwiązywania sytuacji związanych z cyberprzemocą. Zajęcia mogą być przeprowadzone podczas godziny wychowawczej, lekcji informatyki lub zajęć pozalekcyjnych. Zaplanowano je na jedną godzinę dydaktyczną (45 min).

KURS E-LEARNING **„GDZIE JEST MIMI?”**
Kurs jest przeznaczony dla uczniów w wieku 10-13 lat. Uczestnicy kursu, na podstawie historii uczennicy dotkniętej agresją rówieśniczą w internecie, poznają różne aspekty cyberprzemocy z perspektywy ofiary, świadków oraz sprawcy, dowiadują się też, jak radzić sobie w takich sytuacjach. Czas trwania: około 25 minut.

Oferta edukacyjna dla szkół gimnazjalnych i ponadgimnazjalnych

ZAJĘCIA LEKCYJNE **„STOP CYBERPRZEMOCY!”**
Zajęcia dla szkół gimnazjalnych poświęcone problemowi przemocy rówieśniczej w sieci. Ich celem jest zaprezentowanie uczniom zjawiska cyberprzemocy oraz uwrażliwienie ich na możliwe poważne konsekwencje tego typu działań – zarówno dla ich ofiary, jak i sprawców. Bazą do przeprowadzenia zajęć jest prezentacja krótkiego filmu, przedstawiającego przypadek cyberprzemocy w szkole. W scenariuszu proponowana jest burza mózgów, praca w grupach oraz dyskusja moderowana przez nauczyciela. Zajęcia przewidziane są na dwie jednostki lekcyjne.

ZAJĘCIA LEKCYJNE **„DZIEŃ Z ŻYCIA”**
Zajęcia opracowane z myślą o uczniach szkół gimnazjalnych. Dotyczą problemu nadmiernego korzystania z internetu. Ich celem jest przekazanie wiedzy na temat zagrożeń płynących z nadużywania internetu i komputera (w tym również gier, zarówno online, jak i offline). Uczestnicy mają okazję przyjrzeć się temu, jak sami korzystają z internetu oraz nauczyć się reagować na związane z tym problemem zagrożenia. Zajęcia przewidziane są na jedną godzinę dydaktyczną (45 minut).

KURS E-LEARNING **„ZNAJOMI-NIEZNAJOMI.PL”**

Użytkownik kursu wciela się w rolę administratora serwisu społecznościowego i rozwiązuje problemy, z jakimi zgłaszają się jego użytkownicy. Jest w stałym kontakcie ze swoim szefem, który przekazuje mu polecenia i pomaga w trudnych sytuacjach. Kurs składa się z 10 modułów. W trakcie ich realizacji użytkownik zapoznaje się z najważniejszymi zagrożeniami internetowymi, ze szczególnym uwzględnieniem niebezpieczeństw związanych z serwisami społecznościowymi. Kurs przewidziany jest na trzy jednostki lekcyjne.

ZAJĘCIA LEKCYJNE **„W SIECI”**

Zajęcia poświęcone bezpieczeństwu młodych użytkowników internetu. Przeznaczone są dla uczniów klas II i III szkół gimnazjalnych oraz klas I i II szkół ponadgimnazjalnych. Głównym elementem zajęć jest projekcja talk-show, w którym występują m.in. dwie nastoletnie ofiary niebezpiecznych sytuacji w internecie (cyberprzemocy oraz uwodzenia). Gospodarzem programu jest piosenkarka Ewa Farna. Do przeprowadzenia zajęć potrzebne są dwie (rozwiązanie rekomendowane) lub jedna jednostka lekcyjna.

KURS E-LEARNING **„W SIECI”**

Przeznaczony dla uczniów klas II i III szkół gimnazjalnych oraz klas I i II szkół ponadgimnazjalnych. Składa się z 2 modułów. Uczestnicy kursu w oparciu o talk-show prowadzony przez piosenkarkę Ewę Farną zapoznają się z dwoma przypadkami niebezpiecznych sytuacji, z jakimi mogą mieć do czynienia młodzi ludzie w internecie – cyberprzemocy oraz uwodzenia.

Zajęcia edukacyjne dla rodziców i profesjonalistów

KURS E-LEARNING **„DZIECKO W SIECI”**

Rodzicom i profesjonalistom proponujemy udział w zajęciach e-learningowych „Dziecko w Sieci”, stanowiących kompendium wiedzy o bezpieczeństwie dzieci i młodzieży w internecie. Rodzice znajdą w nim charakterystykę zagrożeń oraz informacje o tym, jak skutecznie im zapobiegać.

Pedagogom szkolnym, nauczycielom, psychologom i innym profesjonalistom pracującym z dziećmi prezentujemy dodatkowo ofertę edukacyjną programu „Dziecko w Sieci”. Kurs jest dostępny na platformie **www.fdn.pl/kursy** – jego ukończenie i zdanie testu sprawdzającego pozwala na otrzymanie stosownego zaświadczenia. Z kursem można się zapoznać na stronie **www.dzieckowsieci.fdn.pl** lub pobrać go ze strony w wersji offline, by korzystać z niego samodzielnie lub prezentować podczas szkoleń i konferencji.