Standard bezpieczeństwa online placówek oświatowych

Fundacja Odkrywców Innowacji 2015

DZIAŁANIA NA RZECZ BEZPIECZNEGO KORZYSTANIA Z INTERNETU

Standard bezpieczeństwa online placówek oświatowych

DZIAŁANIA NA RZECZ BEZPIECZNEGO KORZYSTANIA Z INTERNETU

www.bezpiecznyinternet.edu.pl

Publikacja powstała w ramach projektu pt.: *„Działania na rzecz bezpiecznego korzystania z internetu”*
© Copyright Fundacja Odkrywców Innowacji

Publikacja została opracowana przez Zespół Ekspertów:

NASK — Naukowej i Akademickiej Sieci Komputerowej - Instytutu Badawczego

Wyższa Szkoła Pedagogiczna im. Janusza Korczaka w Warszawie — Wyższej Szkoły Pedagogicznej im. Janusza Korczaka w Warszawie

Redakcja: Joanna Lizut
Skład Zespołu Eksperckiego:
Marcin Bochenek, Urszula Brochwicz, Michał Chrzanowski, Tomasz Jordan Kruk, Joanna Lizut, Zuzanna Polak, Krzysztof Silicki, Agnieszka Wrońska

Recenzja:
dr hab. Mirosław Grewiński, prof. WSP im. Janusza Korczaka w Warszawie; dr Bogdan Skrzypczak

Projekt objęty honorowym patronatem:

MINISTER EDUKACJI NARODOWEJ

RZECZNIK PRAW DZIECKA
Marek Michalak

UKE Urząd Komunikacji Elektronicznej

ORE Ośrodek Rozwoju Edukacji

FUNDACJA ODKRYWCÓW INNOWACJI

Ministerstwo Administracji i Cyfryzacji

fundacja drabina rozwoju

Zadanie publiczne „Działania na rzecz bezpiecznego korzystania z Internetu”
współfinansowane przez Ministerstwo Administracji i Cyfryzacji

SPIS TREŚCI

Przedmowa 5

Wprowadzenie 6

Definicja standardu przyjęta w dokumencie 8

Cel wprowadzenia standardu 9

Użytkownicy standardu 10

Dział I. Profilaktyka
Zapobieganie wystąpieniu cyberproblemów 11

Model działań profilaktycznych 11

Działania diagnostyczne 12

Działania informacyjne 12

Działania szkoleniowe i edukacyjne 13

Działania wychowawcze 13

Model profilaktyczny: zalecenia dotyczące przygotowania bezpiecznej i efektywnej infrastruktury internetowej placówki 14

Trzy poziomy bezpieczeństwa infrastruktury IT 15

Poziom minimalny 16

Poziom podwyższony 18

Poziom profesjonalny 19

Dział II. Interwencja
Reagowanie w przypadku wystąpienia cyberproblemów 21

Model działań interwencyjnych 21

Działania wobec aktu/zdarzenia 22

Ustalenie okoliczności zdarzenia, analiza zdarzenia oraz zebranie i zabezpieczenie dowodów 23

Identyfikacja sprawcy/sprawców 24

Monitoring pointerwencyjny 24

Działania wobec uczestników zdarzenia 25

Działania wobec instytucji/organizacji/służb pomocowych i współpracujących – policja, sąd rodzinny, służby społeczne 26

Obowiązki szkoły i placówek oświatowych w zakresie współpracy z policją i sądem rodzinnym 26

Współpraca ze służbami społecznymi i placówkami specjalistycznymi 28

Współpraca z dostawcami usług internetowych i operatorami sieci telekomunikacyjnych 30

Zastosowanie modelu działań interwencyjnych - procedury reagowania wobec wybranych rodzajów zagrożeń 30

Procedura interwencyjna: Cyberprzemoc 30

Procedura interwencyjna: Niebezpieczne kontakty online 34

Procedura interwencyjna: Nielegalne i szkodliwe treści 37

Procedura interwencyjna: Seksting 40

Procedura interwencyjna: Nadmierne korzystanie z Internetu/nowoczesnych technologii 43

Dział III.
Technologiczne zagrożenia w cyberprzestrzeni 45

Co trzeba wiedzieć o Internecie aby czuć się bezpiecznie? 46

Dostawcy usług 46

Jak funkcjonuje Internet? 47

Model reagowania, środki zaradcze i dobre praktyki 48

Zakończenie 53

Załączniki 54

Bibliografia 110

O projekcie 112

Przedmowa

Niniejsza publikacja stanowi efekt prac Zespołu Ekspertów Naukowej i Akademickiej Sieci Komputerowej oraz Wyższej Szkoły Pedagogicznej im. Janusza Korczaka w Warszawie, które były realizowane w ramach projektu *„Działania na rzecz bezpiecznego korzystania z internetu”*. Dokument jest propozycją standardu bezpieczeństwa online dla placówek oświatowych i umożliwiać ma prawidłowe ukierunkowanie działań profilaktycznych i naprawczych w odniesieniu do cyberproblemów. Zaproponowane w standardzie modele prewencji i interwencji wypełniają lukę pomiędzy nauką i praktyką aktualnego funkcjonowania placówek, a ich implementacja pozwoli na podniesienie poziomu bezpieczeństwa członków społeczności szkolnej.

Materiał ten wpisuje się w pełni w plany i zalecenia przyjmowane zarówno na poziomie krajowym, jak i w ramach Unii Europejskiej dotyczące roli i znaczenia nowoczesnych technologii. Autorzy przygotowując to opracowanie opierali się zarówno na swoim eksperckim doświadczeniu, ale też na bogatej literaturze przedmiotu.

Wnioski, procedury i zalecenia sformułowane w tym dokumencie stanowić mają podstawę konkretnych działań zarówno z zakresu profilaktyki, jak i reagowania. Propozycje poszczególnych schematów działania stanowią autorskie rozwiązania ekspertów przygotowujących ten dokument. Zaproponowane w standardzie modele wskazują niezbędne aktywności, które należy uwzględnić w planowaniu, wdrażaniu oraz monitorowaniu zadań edukacyjnych i prac technicznych w placówkach. Ponadto mogą służyć do budowania programów profilaktycznych, tworzenia reguł i oceny funkcjonowania placówek w zakresie bezpiecznego korzystania z Internetu. Pośrednio, standard powinien wpłynąć także na nowe określenie rozwoju zawodowego nauczycieli, w którym powinny pojawić się także elementy związane z zagadnieniami bezpieczeństwa w sieci. Standard można też wykorzystać do samodoskonalenia i podnoszenia umiejętności wykorzystywania technologii cyfrowych.

Lista potencjalnych zagrożeń online i przedstawiony opis bazują na przeprowadzonej przez autorów na poczet tego dokumentu analizie stanu bezpieczeństwa Internetu. Autorzy uważają, iż w przyszłości mogą pojawić się nowe, dziś jeszcze nie występujące zagrożenia, ważne jest stałe przeprowadzanie weryfikacji poziomu bezpieczeństwa, szkolenia pracowników i edukacja uczniów. Przygotowane procedury działania mają charakter uniwersalny i będzie można je zastosować do ewentualnych działań także w przyszłości.

Publikacja standardów stanowi ważny, pierwszy krok w ich rozpowszechnianiu. Kolejne, niezbędne działania, które wprowadzą standardy do praktyki działania oraz umocują je w systemie oświaty, powinny obejmować szkolenia i działania edukacyjne przeznaczone dla szerokiego grona odbiorców pracujących w obszarze oświaty. Powszechne zastosowanie standardów bezpośrednio wpłynie na bezpieczeństwo społeczności szkolnych, przede wszystkim dzieci i młodzieży, ale także kadry oświatowej i rodziców.

Wprowadzenie

Internet stał się trwałym elementem funkcjonowania placówek oświatowych. Wykorzystywany jest przede wszystkim w procesie nauczania, ale coraz częściej także jako element działania i funkcjonowania organizacyjnego oraz administracyjnego placówki. Do niedawna traktowany jako nowość, dziś jawi się nie tylko jako stały, ale także niezbędny element funkcjonowania szkoły. Gwałtowna ekspansja sieci, coraz większa jej obecność w edukacji i w procesach komunikowania, w naturalny sposób nie szły w parze z tworzeniem zasad, procedur i norm postępowania. Należy zauważyć, iż rozwojowi sieci towarzyszy pojawienie się w Internecie niebezpiecznych zjawisk i przestępczości. Możemy mówić o przenoszeniu się negatywnych zjawisk ze świata realnego do sieci, jaki i o tworzeniu się całkiem nowych kategorii zjawisk niekorzystnych i przestępstw. Mamy do czynienia zarówno z zagrożeniami o charakterze technicznym, jak i społecznym. Te pierwsze to między innymi wykradanie danych, blokowanie dostępu, wszelkiego rodzaju szkodliwe programy komputerowe, takie jak niszczące zasoby lub przejmujące kontrolę nad komputerami użytkowników. Zagrożenia o charakterze społecznym wiążą się przede wszystkim z pojawianiem się w sieci niebezpiecznych i nielegalnych treści. Mówimy tu między innymi o: cyberprzemocy, groomingu, sekstingu, hejtingu, pornografii dziecięcej, treściach rasistowskich i zachęcaniu do samobójstw.

Na potrzeby tego standardu dokonano podziału zagrożeń online na dwie podstawowe grupy:

- **zagrożenia o charakterze społeczno – wychowawczym**
- **zagrożenia technologiczne**

W powstających opracowaniach, jak i w praktyce działania, stosuje się także inne podziały. Warto także zauważyć, iż niektóre z opisywanych zjawisk występują łącznie. Podział ten służy jasnemu sprecyzowaniu natury poszczególnych zagrożeń, ale też w praktyce działania, lepszemu przygotowaniu się placówki do reagowania w przypadku ich wystąpienia.

Szczegółowo omówione zostały najczęściej występujące zagrożenia. To właśnie z tymi problemami muszą radzić sobie placówki oświatowe. Niezależnie od zaprezentowanej w dokumencie listy mogą pojawić się także inne niebezpieczeństwa. Procedura reagowania w takich sytuacjach winna być wzorowana na modelach zaprezentowanych w standardzie.

ZAGROŻENIA O CHARAKTERZE SPOŁECZNO – WYCHOWAWCZYM:

- **szkodliwe i nielegalne treści** – prezentujące przemoc, obrażenia fizyczne, śmierć (ofiary wypadków, okrucieństwo wobec ludzi i zwierząt), nawołujące do autodestrukcji (samookaleczeń, samobójstw, zażywania szkodliwych substancji itp.), zachęcające do nietolerancji, wrogości czy nienawiści, pornografia dziecięca;
- **niebezpieczne kontakty, uwodzenie w internecie (child grooming)**;
- **seksting, prowokacyjne zachowania i aktywność seksualna** jako źródło dochodu osób nieletnich;
- **agresja elektroniczna** – różnego rodzaju działania agresywne realizowane za pomocą współczesnych technologii komunikacyjnych mające na celu dyskredytowanie jednej czy wielu osób (szczególną formą agresji elektronicznej jest cyberprzemoc rówieśnicza);
- **nadużywanie internetu** – rozumiane jako nadmierne i/lub dysfunkcyjne używanie internetu związane z czasem, jak i intensywnością korzystania z sieci oraz potrzebą korzystania z sieci z jednoczesną utratą kontroli nad planowanym czasem aktywności online. Wiąże się to często z zaniedbywaniem innych aspektów życia.

ZAGROŻENIA TECHNOLOGICZNE W CYBERPRZESTRZENI, TAKIE JAK:

- **szkodliwe oprogramowanie (malware)** takie jak: wirusy, konie trojańskie, ransomware itp.,
- **zagrożenie poprzez surfowanie (drive by download)** - ściąganie szkodliwego oprogramowania poprzez kontakt z zarażonymi serwisami WWW,
- **BOTnety**, czyli sieci atakujących komputerów, przejętych przez cyberprzestępców,
- **ataki typu blokowanie usług (DoS)**,
- **ataki socjotechniczne (phishing)**,
- **włamania na strony internetowe lub do wewnętrznych systemów komputerowych**.

Zagadnienia związane z cyberproblemami i wyjaśnienie stosowanych pojęć zostały szczegółowo przedstawione w słowniku najważniejszych zagrożeń (patrz: Załącznik nr 1) oraz w słowniku najważniejszych pojęć związanych z użytkowaniem sieci (patrz: Załącznik nr 2).

Ponadto w części związanej z technologiami IT znalazły się zagadnienia dotyczące użytkowania prywatnych urządzeń mobilnych na terenie placówki (z ang. BYOD – *Bring Your Own Device*) oraz wykorzystania infrastruktury w placówce do nielegalnej lub szkodliwej działalności.

Dostrzeżenie niebezpieczeństw, jakie niesie internet i właściwe radzenie sobie z nimi, jest dzisiaj koniecznością. To zadanie jest szczególnie ważne w momencie, kiedy polska szkoła wchodzi w pełni w cyfrową rzeczywistość, a w procesie dydaktycznym odchodzi się od tradycyjnych podręczników na rzecz elektronicznych. Rzeczywistości i problemów placówki oświatowej nie można rozważać w oderwaniu od powszechnej obecności Internetu w naszym życiu. Pracownik szkoły korzysta z Internetu także w domu, podobnie uczeń. Taka sytuacja powoduje, iż zjawiska bezpieczeństwa online w szkole nie można rozpatrywać w oderwaniu od problematyki korzystania z sieci przez krąg osób związanych z placówką oświatową. Należy zdawać sobie sprawę, iż stworzenie całościowego programu, systemu zaleceń lub też standardu bezpieczeństwa w sieci, nie jest do końca możliwe.

Wychodząc naprzeciw potrzebie opisania problemów, stworzenia procedur działania i reagowania wobec niebezpiecznych zjawisk, proponujemy wprowadzenie standardu bezpieczeństwa online dla placówek oświatowych.

Definicja standardu przyjęta w dokumencie

Zgodnie z obowiązującymi definicjami standard określa pożądane, powszechne cechy np. tworzonego produktu. Zejście poniżej standardu w ekonomii traktowane jest jako proces deprecjonujący wartość. W przedstawianym dokumencie przyjmujemy takie rozumienie standardu, a istotną jego część stanowią konkretne procedury działań, które zgodnie z tymi definicjami można uznać za normy. Standard nie jest przypadkowym zbiorem, czy spisem zasad i procedur. Wprowadzone elementy stanowią spójną całość. Nie oznacza to jednak braku możliwości wykorzystania jedynie niektórych elementów standardu w praktyce działania placówki oświatowej. Taka decyzja uwarunkowana może być specyfiką funkcjonowania placówki lub wcześniej działającymi regułami.

Proponowany tutaj standard jest autorskim opracowaniem, ale powstał z uwzględnienieniem obowiązujących reguł, zasad i przepisów. Ponieważ dokument ten ma charakter standardu przeznaczonego do praktycznej implementacji autorzy, nie omawiają innych, obowiązujących w placówkach oświatowych, dokumentów. Wiele z nich opisuje znacznie szerszą problematykę, a nie odnosi się (jak prezentowany standard), do jednego acz niezwykle ważnego zagadnienia. Dokument wpisuje się w zasady Podstawy Programowej Kształcenia Ogólnego określające działalność edukacyjną szkoły. Podstawa wskazuje, iż działalność ta określona jest poprzez:

- szkolny zestaw programów nauczania,
- program wychowawczy szkoły, zawierający działania i treści o charakterze wychowawczym,
- program profilaktyki przystosowany do potrzeb rozwojowych uczniów oraz potrzeb środowiska obejmujący treści i działania o charakterze wychowawczym (Dz.U.2012.977).

Szczegółowe rozwiązania proponowane w niniejszym dokumencie są koherentne z przyjętymi i obowiązującymi dokumentami w placówkach oświatowych.

Dokument ten odzwierciedla przyjęte przez autorów, dziś powszechnie akceptowane, podejście do problematyki zagrożeń. Oznacza ono uznanie istnienia społeczności szkolnej, której częściami są uczniowie, nauczyciele i rodzice. Utrzymuje także pozytywną filozofię rozwiązywania problemów (wyjaśnianie, poprawianie) i nie wprowadzanie modelu represyjnego (karanie). Nie oznacza jednak pobłażania czy lekceważenia roli sprawców czynów szkodliwych lub przestępczych.

Podstawą standardu jest kompleksowe podejście do omawianej problematyki. Wyrazem takiego właśnie sposobu postępowania jest rozpoczęcie procesu zapewnienia bezpieczeństwa online w placówce od podjęcia zakrojonych na szeroką skalę działań diagnostycznych (uwzględniających zasoby i możliwości działania szkoły). Standard obejmuje także etapy takie jak: działania o charakterze informacyjnym, profilaktykę, reagowanie po wystąpieniu incydentu oraz działania wychowawcze. Każdy z nich stanowi nieodzowną część łańcucha postępowania. Autorzy wskazują jednak na kluczową rolę działań o charakterze profilaktycznym. Zaproponowane rozwiązania winny być realizowane w ramach Szkolnego Programu Profilaktyki. Zgodnie z Podstawą Programową Kształcenia Ogólnego taki program każda placówka opracowuje indywidualnie. Zawarta tu propozycja dotycząca zagadnień bezpieczeństwa online może być częścią takiego programu.

Pisząc o dostosowaniu działań profilaktycznych do konkretnej sytuacji autorzy mieli na uwadze podział na profilaktykę pierwszorzędową i drugorzędową, obecny w licznych opracowaniach naukowych poświęconych temu zaganieniu. Społeczność szkolna jest zróżnicowana, a w praktyce działania mamy do czynienia także z osobami wymagającymi szczególnego traktowania. Oznacza to, że w ramach opisywanych tu działań, bazując na profilaktyce pierwszorzędowej, staramy się dotrzeć do wszystkich członków społeczności szkolnej z podstawowymi komunikatami, treściami i opisami procedur oraz zasad. W sytuacjach wymagających szczególnej troski zalecamy stosowanie metod profilaktyki drugorzędowej.

Cel wprowadzenia standardu

Celem niniejszego standardu jest podniesienie poziomu bezpieczeństwa online placówek oświatowych. Cel ten należy rozumieć kompleksowo. Przede wszystkim jako podniesienie poziomu bezpieczeństwa uczniów i nauczycieli (czy też szerzej pracowników placówki), ale też zwiększenie poziomu bezpieczeństwa infrastruktury technicznej istniejącej w danej placówce. Przy wprowadzaniu standardu przyjęto szereg założeń wynikających z zasad, jakimi powinny kierować się placówki oświatowe, jak i z doświadczeń związanych z funkcjonowaniem cyfrowego świata.

Podstawowe zasady:

1. **Główny nacisk działań mających podnieść poziom bezpieczeństwa online powinien być skierowany na profilaktykę.** Zapobieganie niebezpiecznym zjawiskom jest podstawą skutecznego działania.

2. **Podejmowane aktywności nie powinny mieć charakteru represyjnego**. Działania placówki powinny być nastawione na kształtowanie poprawnych postaw i oddziaływania wychowawcze. Wychodząc z takich przesłanek, nie należy jednak doprowadzać do bezkarności sprawcy (czy też sprawców) naruszającego reguły, zasady czy przepisy prawne.

3. **Bezpieczeństwo w placówkach oświatowych jest zależne przede wszystkim od ludzi: ich wiedzy, umiejętności, zaangażowania i podejmowania odpowiednich decyzji.** Dotyczy to zarówno zagrożeń o charakterze społecznym jak i technicznym. Pamiętając o konieczności ciągłego doskonalenia rozwiązań o charakterze technicznym, o wprowadzaniu zabezpieczeń zmniejszających poziom potencjalnego ryzyka zwracamy jedocześnie uwagę na kluczową rolę działań poszczególnych osób. Najsłabszym ogniwem bezpieczeństwa każdego systemu jest człowiek. Dlatego istotnym elementem w procesie budowania standardu jest podkreślenie roli edukacji, budowania kompetencji oraz zdolności rozumienia cyfrowej rzeczywistości.

STANDARD WPROWADZA:

- **modele profilaktyczne - działania o charakterze prewencyjnym.** Skierowane zarówno do nauczycieli, uczniów, ich rodziców i opiekunów. Oznaczają między innymi: stworzenie procedur zarządzania problematyką cyfrową w szkole, ustanowienie szkolnego lidera w tej dziedzinie, edukację w zakresie bezpieczeństwa online oraz szeroko zakrojoną akcję informacyjną. Wzmocnieniem tych procesów jest wprowadzenie działań o charakterze profilaktycznym dotyczących tematyki związanej z edukacją medialną.

- **modele interwencyjne - reagowanie w sytuacjach kryzysowych**. Dotyczą zarówno reagowania na zagrożenia o charakterze społecznym jak i technologicznym. Modele te uwzględniają zarówno elementy społeczne, psychologiczne, techniczne jak i prawne. Oparte zostały na wiedzy, doświadczeniu i najlepszych praktykach.

Ponadto w dokumencie znajduje się wyciąg z podstawowych aktów prawnych dotyczących zagrożeń online i problematyki bezpieczeństwa w placówkach oświatowych.

Użytkownicy standardu

Kluczowym elementem do osiągnięcia sukcesu w działaniach na rzecz bezpieczeństwa online jest klarowne zdefiniowanie grup odbiorców niniejszego standardu. Dokument ten odnosi się do potrzeb oraz problemów całej społeczności szkolnej (społeczności placówki oświatowej) to znaczy: nauczycieli, uczniów i rodziców. **Pojęcie „społeczności szkolnej" jest kluczowe gdyż pokazuje współzależność trzech grup: nauczycieli, uczniów i rodziców.** W praktyce użytkownikami standardu będą głównie nauczyciele, ale również uczniowie i rodzice będą odnosili się do norm w nim zawartych. Beneficjentami wprowadzenia standardu będzie cała szkolna społeczność. Nauczyciele i pracownicy placówki oświatowej wprowadzają standard w życie na co dzień implementując zaproponowane w nim działania. Bezpośrednimi odbiorcami tych działań są uczniowie, a w konsekwencji także rodzice. Rolą placówki powinno być, posługując się proponowanymi założeniami, jak najszersze angażowanie rodziców w prowadzone działania. Nowoczesność sieci, trudność w rozdzielaniu obszarów działania, powodują zatarcie granic pomiędzy światem szkoły i domu. Dlatego właśnie ten aspekt współpracy jest tak kluczowy dla osiągnięcia sukcesu.

Dział I. Profilaktyka – Zapobieganie wystąpieniu cyberproblemów

W przedstawionym standardzie przyjęto założenie, iż w placówkach oświatowych należy położyć szczególny nacisk na zapobieganie występowaniu niepożądanych zjawisk związanych z funkcjonowaniem placówki online. Działania prewencyjne pozwalają uniknąć wielu problemów, w tym tych najpoważniejszych, związanych z krzywdą konkretnych osób. Z punktu widzenia funkcjonowania placówki oświatowej oznaczają one także oszczędność, ponieważ działania, które podejmowane są po wystąpieniu niekorzystnych zjawisk, są kosztowne i czasochłonne. Proponowane w standardzie podejście do zagadnień profilaktyki bazuje na zaplanowanych i konsekwentnie wdrażanych działaniach oraz procedurach. W procesach tych autorzy uwzględnili rolę i potrzeby całej społeczności szkolnej, zarówno uczniów, nauczycieli i rodziców.

Model działań profilaktycznych

Proponowany model działań profilaktycznych powinien obejmować: działania diagnostyczne, działania informacyjne, działania szkoleniowe i edukacyjne oraz działania wychowawcze (Rys. 1).

Rys.1 Typy działań profilaktycznych

Źródło: opracowanie Marcin Bochenek

Działania diagnostyczne

Pierwszym elementem działań o charakterze diagnostycznym powinno być przygotowanie wstępnej oceny stanu bezpieczeństwa online placówki. Badanie takie powinno odpowiedzieć na pytania dotyczące poziomu wiedzy, przebytych szkoleń, istniejących procedur i sposobów działania, a także przeprowadzonych działań o charakterze informacyjnym i edukacyjnym. Inicjatorem i organizatorem takiego procesu winien być dyrektor placówki. To badanie powinno przyczynić się także do wyłonienia lidera bezpieczeństwa online. **Do zadań lidera bezpieczeństwa online należy:**

- koordynowanie zagadnień bezpieczeństwa online (techniczne, społeczne, wychowawcze zagrożenia płynące z sieci),
- realizacja zadań wynikających z wprowadzonego standardu bezpieczeństwa online,
- raportowanie w sprawach bezpieczeństwa online do dyrektora,
- działania w Zespole ds. Bezpieczeństwa Online.

ZESPÓŁ DS. BEZPIECZEŃSTWA ONLINE

W placówce należy powołać zespół, w skład którego powinien wejść pedagog/psycholog, dyrektor, w przypadku szkoły również wychowawca klasy (po ustaleniu osób uczestniczących w zdarzeniu) oraz lider bezpieczeństwa online, jeśli taka funkcja została w placówce powołana. Do prac zespołu warto włączać osoby posiadające umiejętności techniczne/informatyczne szczególnie przydatne przy zbieraniu i kompletowaniu materiałów dokumentujących zdarzenie. Zadaniem Zespołu jest włączenie się w opracowanie i realizację szkolnego programu profilaktyki bezpieczeństwa online oraz w działania interwencyjne opisane w Dziale II.

Działania informacyjne

Placówka powinna prowadzić stałe, zaplanowane działania informacyjne skierowane do wszystkich członków społeczności. Zaleca się by tematyka bezpieczeństwa online wprowadzona była do kalendarza placówki i omawiana na spotkaniu Rady Pedagogicznej przed rozpoczęciem roku szkolnego. Przypomniane powinny zostać procedury i zasady postepowania. Wskazane jest, aby w trakcie roku szkolnego tematyka ta była poruszana przez Radę jeszcze dwukrotnie. Uczniowie powinni zapoznawać się z tymi zagadnieniami nie tylko podczas lekcji informatyki, ale także w trakcie lekcji wychowawczych co najmniej raz podczas semestru.

Bezpieczeństwo online powinno być także omawiane przynajmniej raz w semestrze w trakcie zebrań z rodzicami. Opiekunowie odgrywają zasadniczą rolę w funkcjonowaniu dziecka na terenie placówki oświatowej. Osobą przekazującą wiedzę jest wychowawca lub szkolny lider bezpieczeństwa online. W takim charakterze może wystąpić także zewnętrzny gość/ekspert np. z policji. Wszyscy nauczyciele powinni korzystać ze wspólnej prezentacji, jednolitego materiału omawiającego zagrożenia i sposoby przeciwdziałania. Jeśli wymagać będzie tego sytuacja (ze względu na wydarzenia, incydenty w danej placówce lub konieczność poinformowania o zjawisku, problemie czy zagrożeniu) to częstotliwość zajęć powinna być zwiększona. Decyzję wówczas podejmuje Dyrektor placówki.

W widocznym i dostępnym miejscu w placówce wywieszona powinna być informacja skierowana do uczniów, wskazująca, co należy zrobić, gdy jest się ofiarą lub świadkiem niepożądanego zjawiska w sieci. W miejscu dostępnym dla nauczycieli i pracowników placówki wskazane jest aby znalazła się informacja przedstawiająca procedury reagowania w przypadku wystąpienia zagrożeń. Działania informacyjne mogą być realizowane poprzez dystrybucję plakatów, ulotek, organizację konkursów.

Działania szkoleniowe i edukacyjne

W ślad za działaniami informacyjnymi powinny iść działania szkoleniowe i edukacyjne. Także i ta aktywność kierowana jest zarówno do pracowników placówki, uczniów oraz rodziców. Tematyka zajęć powinna dotyczyć informacji o zagrożeniach i metodach przeciwdziałania, jak i zagadnienia szeroko rozumianej edukacji medialnej. Wskazane jest, aby szkolenie z zagadnień dotyczących bezpieczeństwa dla pracowników placówki odbywało się co najmniej raz w roku, obejmując informacje o występujących zagrożeniach i metodach przeciwdziałania, z uwzględnieniem najnowszej wiedzy i zmieniających się trendów. Za zorganizowanie szkolenia odpowiedzialny jest szkolny lider bezpieczeństwa online. W trakcie kursu powinny zostać omówione zagadnienia edukacji medialnej, a w szczególności specyfiki przekazu, jego rozumienia, źródeł informacji, weryfikacji wiedzy dostępnej online oraz nowoczesnych sposobów i technik komunikowania. Ma to na celu budowanie i rozwijanie kompetencji informacyjnych rozumianych jako zbiór umiejętności pozwalających w sposób odpowiedzialny rozumieć, pozyskiwać, przetwarzać i publikować informacje za pomocą dostępnych dziś narzędzi i technologii.

W przypadku uczniów należy zadbać by tematyka bezpieczeństwa online była poruszana na lekcjach informatyki, w trakcie godzin wychowawczych, a także w czasie zajęć z innych przedmiotów. Szczegółowe rozwiązania powinny być przyjmowane w trakcie poprzedzającej rozpoczęcie roku szkolnego Rady Pedagogicznej. Wskazane jest, aby wszyscy nauczyciele poruszający te zagadnienia, posługiwali się jednolitymi/spójnymi materiałami informacyjnymi i prezentacjami. Za ich przygotowanie odpowiada szkolny lider lub/i są to zadania Zespołu ds. Bezpieczeństwa Online.

Działania wychowawcze

Obok wcześniej wymienionych obszarów istotną rolę odgrywają także działania o charakterze wychowawczym. Ten moduł odnosi się do sfery profilaktycznej, jak i do działań prowadzonych już po zaistnieniu zdarzenia naruszającego bezpieczeństwo. Adresatem tej aktywności są uczniowie danej placówki. Działania wychowawcze mają na celu kształtowanie postaw lub ich zmianę. Te pierwsze mają na celu przypomnienie uniwersalnych zasad postępowania odnoszących się nie tylko do aktywności w świecie cyberprzestrzeni, ale do całej płaszczyzny relacji społecznych.

Działania wychowawcze mają na celu utrwalić prawidłowe postawy u uczniów i wskazać na te sposoby działania, komunikowania i reagowania, które pozwalają uniknąć/zabezpieczyć się przed konfliktami i problemami. Nauczyciel – wychowawca (ewentualnie wspólnie z pedagogiem szkolnym) w trakcie zajęć przedstawia konsekwencje przykładowo podejmowanych niepożądanych działań oraz zasady unikania problemów związanych z korzystaniem z sieci. Główny nacisk powinien być położony na sferę psychologiczną tak, by uczeń rozumiał konsekwencje podejmowanych aktywności. Tego typu zajęcia o charakterze profilaktycznym powinny odbywać się raz w semestrze w trakcie godziny wychowawczej.

Rys.2 Model profilaktyczny

Źródło: opracowanie Marcin Bochenek

Model profilaktyczny: zalecenia dotyczące przygotowania bezpiecznej i efektywnej infrastruktury internetowej placówki

Szkoła czy inna placówka oświatowa, podłączając swoją infrastrukturę do sieci dostawcy usług (sieci Internet) występuje w dwóch rolach:

- z jednej strony jest klientem dostawcy dostępu do Internetu, dostawcy hostingu, dostawcy rozwiązań chmurowych,
- z drugiej strony oferuje usługi lokalnego Internetu dla personelu placówki, nauczycieli czy uczniów.

Placówka oświatowa powinna zadbać, by infrastruktura komputerowa oraz sieciowa służąca dostępowi do sieci, a także same systemy komputerowe i aplikacje wykorzystywane na terenie placówki, zapewniały odpowiedni poziom bezpieczeństwa.

Trzy poziomy bezpieczeństwa infrastruktury IT

Niniejszy standard wyróżnia trzy zalecane poziomy bezpieczeństwa infrastruktury IT przy dostępie do Internetu realizowanym w placówce:

- **poziom minimalny** – zakładający, że nawet przy poważnych ograniczeniach budżetowych w placówce musi być zagwarantowany pewien standard organizacyjno-techniczny (zapewniający, że infrastruktura IT spełnia określone, minimalne techniczne wymogi bezpieczeństwa, bez spełnienia których w ogóle nie powinna być oddawana do użytku), a także, że istnieją odpowiednie zasoby organizacyjne – chociażby dotyczące opieki nad infrastrukturą,

- **poziom podwyższony** – przyjmujący, że w placówce, w której wykorzystuje się aplikacje i systemy informatyczne dostępne dla użytkowników sieci lokalnej, a także realizowany jest dostęp do Internetu, poziom minimalny bezpieczeństwa jest niewystarczający, należy więc zastosować dodatkowe mechanizmy zalecane na poziomie podwyższonym,

- **poziom profesjonalny** – właściwy dla infrastruktury IT w placówce, której celem jest wykorzystywanie nowoczesnych rozwiązań informatycznych stacjonarnych, jak i mobilnych oraz używanie infrastruktury do pogłębionej edukacji informatycznej, posiadającej rozbudowany intranet (sieć wewnętrzna wraz z wieloma serwisami przeznaczonymi do użytku pracowników i uczniowi, którą w praktyce można porównać z nowoczesnymi sieciami przedsiębiorstw).

Rys.3 Trzypoziomowy model bezpieczeństwa infrastruktury IT

* stosowane przez firmy/przedsiębiorstwa lub przeznaczone dla firm/przedsiębiorstw

Źródło: opracowanie Krzysztof Silicki

Poziom minimalny

Nawet przy poważnych ograniczeniach budżetowych infrastruktura IT w szkole powinna zapewniać minimalne wymogi ochrony przed cyber - zagrożeniami. Często bowiem systemy komputerowe i sieci zainstalowane są bez zwracania uwagi na zasady bezpieczeństwa. Na dodatek pozbawione opieki w trakcie użytkowania stają się zaprzeczeniem początkowej idei: nie służą ich właścicielom tylko padają łupem cyberprzestępców.

MINIMUM BEZPIECZEŃSTWA

W ramach zapewniania minimalnego poziomu bezpieczeństwa oraz właściwej opieki nad infrastrukturą, zaleca się:

- Ustanowić administratora dbającego o prawidłowe funkcjonowanie infrastruktury komputerowej, bezpieczeństwo oraz o spełnianie przez placówkę minimalnych wymagań standardu. Osoba ta może być pracownikiem placówki, bądź pochodzić z zewnątrz.
- Jeśli administrator pochodzi z zewnątrz, w placówce należy ustanowić rolę opiekuna infrastruktury, który nadzorował by zgodność placówki ze standardem oraz pracę administratora.
- Jeśli występuje brak możliwości powołania opiekuna lub administratora należy rozważyć zasadność udostępniania Internetu w szkole, bowiem infrastruktura pozostająca bez opieki przyniesie więcej zagrożeń i problemów niż korzyści z samego udostępniania Internetu.
- Odpowiednio przygotować sprzęt wykorzystywany przy dostępie do Internetu (lista zaleceń poniżej).

Sprzęt wykorzystywany przy dostępie do Internetu powinien spełniać określone wymagania bezpieczeństwa. Poniżej wymieniono **minimalne wymagania standardowe odnośnie sprzętu i jego konfiguracji:**

- **Lokalne urządzenie dostępowe (router) zapewniające mechanizm ochrony danych oparty o standard szyfrowania WPA2; sieć bezprzewodowa (WiFi) dostępna tylko na hasło** (przy czym należy stosować dwa rodzaje haseł: jedno dla pracowników szkoły, drugie gościnne, z których mogą także korzystać uczniowie - ograniczony dostęp do Internetu, restrykcje czasowe, ilości przesyłanych bajtów, włączony filtr rodzinny). Hasła powinny być zmieniane cyklicznie (co trzy miesiące).
- Dodatkowo zaleca się **zastosowanie przy dostępie WiFi tzw. strony startowej**, która pojawia się zawsze w trakcie dostępu do sieci przez przeglądarkę internetową (nawiązanie połączenia z urządzeniem dostępowym, typowo routerem WiFi). **Na stronie startowej powinny znaleźć się informacje o zasadach bezpiecznego korzystania z Internetu** (regulamin oraz wyciąg najważniejszych elementów higieny bezpieczeństwa korzystania z Internetu). Strona taka może służyć także do identyfikacji użytkowników (czasowe hasła dostępu indywidualne lub grupowe np.:dla uczniów tej samej klasy), jako że należy unikać oferowania anonimowego dostępu do sieci.

- Należy **aktywować oraz zadbać o właściwe skonfigurowanie usługi filtrowania szkodliwych treści.** Usługę tzw. filtra rodzinnego można zapewnić na różne sposoby. Przykładowo, poprzez odpowiednią konfigurację urządzenia dostępowego (routera) i zastosowanie ogólnodostępnego oprogramowania (np. DansGuardian),bądź poprzez wykupienie odpowiedniego pakietu usługi filtrowania u operatora (jeśli taka usługa istnieje). Inną możliwością jest stosowanie rozwiązania opartego na przekierowaniu ruchu internetowego przez urządzenia pośredniczące (np. typu proxy), które pozwalają na filtrowanie treści (np. wykorzystując usługę OpenDNS).

- **Na routerze powinna zostać włączona usługa przegrody firewall.** Konfiguracja tej usługi powinna odzwierciedlać przyjętą w placówce politykę bezpieczeństwa określającą między innymi zasady i zakres dostępu do zasobów znajdujących się w systemach informatycznych.

- **Strona WWW szkoły** (jeśli istnieje), w przypadku ograniczeń zasobów administracyjnych **powinna zostać posadowiona na serwerze hostingowym operatora zapewniającego odpowiedni poziom bezpieczeństwa.** Nie zwalnia to jednak personelu szkoły z obowiązku monitorowania prawidłowego działania strony i jej zawartości. Zdarzają się przypadki, że strona WWW szkoły pada ofiarą cyberprzestępców (np.: zostaje podmieniona), a szkoła tego nie zauważa, gdyż rzadko dokonuje modyfikacji treści na stronie.

- **Na komputerach szkolnych powinny być zainstalowane programy antywirusowe.** Jeśli nie ma środków na rozwiązania komercyjne, należy stosować pakiety darmowe. W tym przypadku należy zweryfikować dany program oraz jego producenta poprzez zasięgnięcie opini o jego reputacji (oceny o programie w Internecie, weryfikacja danych teleadresowych, istnienie kontaktu telefonicznego itp.). Zdarza się często, że programy podające się za systemy antywirusowe, w rzeczywistości są szkodliwym oprogramowaniem (malware), które zaraża komputery. Pakiety antywirusowe muszą być cyklicznie aktualizowane, należy zadbać więc o dokonywanie się automatycznych aktualizacji.

- **Korzystanie z usług chmurowych jest dopuszczalne pod warunkiem spełnienia określonych wymagań**, takich jak: weryfikacja dostawcy, zapoznanie się z regulaminem usługi, zapoznanie się zasadami zapewniania prywatności danych (nieudostępnianie ich innym podmiotom przez dostawcę usługi chmurowej, zapewnienie wiarygodnych mechanizmów poufności danych - szyfrowania), odzyskiwanie danych po awarii usługi, a także istnienie funkcji bezpowrotnego kasowania plików w przypadku zamiaru zakończenia korzystania z usługi.

- **W placówce powinien powstać uproszczony dokument polityki bezpieczeństwa oraz regulamin korzystania z sieci komputerowej i dostępu do Internetu.**

Poziom podwyższony

Podwyższony poziom bezpieczeństwa jest poziomem zalecanym dla każdej placówki oświatowej. Poziom minimalny można stosować jedynie, jeśli występują poważne ograniczenia budżetowe lub infrastruktura IT placówki jest bardzo ograniczona.

Na poziomie podwyższonym bezwzględnie powinien być ustanowiony administrator odpowiedzialny za opiekę techniczną nad infrastrukturą IT oraz za bezpieczeństwo teleinformatyczne.

Poniżej wymieniono **minimalne wymagania standardowe odnośnie sprzętu i jego konfiguracji oraz architektury sieci dla tego poziomu:**

- Urządzenie dostępowe (router) klasy firmowej (enterprise)[1], renomowanego dostawcy.
- Stosowanie zasad separacji funkcjonalnej i związanej z nią segmentacji sieci.
- System uwierzytelniania użytkowników (np.: LDAP, Active Directory).
- System ochrony i kontroli dostępu - firewall (system filtrowania niepożądanych treści).
- System antywirusowy na stacjach roboczych pracowników.
- Dla identyfikacji użytkowników zaleca się korzystanie z systemu uwierzytelniania lub wprowadzenie strony logowania, zezwalającej na dostęp do sieci wifi w oparciu o standard szyfrowania WPA 2.
- Przy tym poziomie bezpieczeństwa mogą być prowadzone przez placówkę różne serwisy dostępne przez Internet, takie jak e-dziennik, jednak przy zachowaniu wszystkich standardowych zaleceń bezpieczeństwa (osoba administrująca, bezpieczne środowisko i konfiguracja serwisu). Dodatkowo muszą być stosowane odpowiednie mechanizmy bezpieczeństwa przy dostępie użytkowników do serwisu (szyfrowane połączenie z serwerem poprzez protokół https), a także należy zabezpieczyć logi z serwera i aplikacji – co wynika między innymi z przepisów o ochronie danych osobowych (dla serwisów, w których przechowywane są dane osobowe).
- **Na poziomie podwyższonym placówka powinna posiadać politykę bezpieczeństwa w postaci dokumentu zatwierdzonego przez kierownictwo instytucji oraz regulamin korzystania z systemów i sieci komputerowych.**

1 Stosowane przez firmy/przedsiębiorstwa lub przeznaczone dla firm/przedsiębiorstw

Poziom profesjonalny

Na tym poziomie zakłada się, że w placówce funkcjonuje profesjonalnie utrzymywany intranet. Wdrożone są wewnętrze systemy informatyczne służące do pracy wszystkim pracownikom placówki. Dodatkowo różnym grupom użytkowników (np.: nauczycielom, wychowawcom, uczniom, rodzicom) mogą być oferowane usługi webowe.

Na poziomie profesjonalnym obowiązują wszystkie zalecenia właściwe dla poziomu pośredniego oraz dodatkowo:

- **System antywirusowy (AV) odpowiedzialny za kontrolę ruchu na styku z siecią Internet.**

  Na tym poziomie bezpieczeństwa użytkownicy są chronieni przed szkodliwym oprogramowaniem (wirusami) w dwóch miejscach: na styku z Internetem oraz na stacjach roboczych. Zapewnia to większą pewność, że zabezpieczenia nie będą omijane.

- **System wykrywania prób włamania (IDS/IPS).**

  Systemy IDS *(Intrusion Detection)*/IPS *(Intrusion Prevention System)* pozwalają na wykrywanie prób ataków, np. włamań do systemów wewnętrznych. Stanowią one najczęściej standardową część systemu firewall, który jest obowiązkowym elementem infrastruktury internetowej placówki. Dla uaktywnienia funkcji IDS/IPS wymagana jest jego dodatkowa konfiguracja.

- **Cykliczne wykonywanie przeglądów bezpieczeństwa (audyty techniczne).**

  Zapewnienie profesjonalnego poziomu bezpieczeństwa wymaga przeprowadzania cyklicznych badań odporności infrastruktury IT na znane zagrożenia. Audyty techniczne są standardowym elementem wypełniającym niniejsze zalecenie. Powinny być przeprowadzane zgodnie z założeniami polityki bezpieczeństwa danej placówki, ale nie rzadziej niż: raz do roku przez personel wewnętrzny, co dwa lata w postaci audytu zewnętrznego oraz każdorazowo po zaistnieniu poważnego incydentu naruszającego bezpieczeństwo. Audyty wewnętrzne mogą być przeprowadzane przez osoby zajmujące się administrowaniem systemów, przy wykorzystaniu automatycznych bądź półautomatycznych narzędzi testowania, komercyjnych, bądź open source (np. openvas, nessus). Audyty zewnętrzne mogą zostać zlecone wykwalifikowanym zewnętrznym pentesterom lub firmom specjalistycznym. Wyniki audytu powinny być uzupełnione o wypływające z testu wnioski, co do koniecznych działań i neleży je przedstawić kierownictwu placówki.

- **Ustanowiona polityka w zakresie BYOD**

  Umożliwienie użytkownikom danej instytucji dostępu do Internetu za pośrednictwem prywatnych mobilnych urządzeń końcowych, jak smartfony czy tablety na terenie placówki, zwana jest koncepcją BYOD (od *Bring Your Own Device*). Jest wyjątkowo złożonym zagadnieniem. Z punktu widzenia bezpieczeństwa technicznego klasyczne rozwiązanie, w którym do zasobów instytucji sięga się jedynie za pośrednictwem urządzeń własnych instytucji jest rozwiązaniem wygodniejszym. Dopuszczenie z kolei urządzeń użytkowników z punktu widzenia bezpieczeństwa teleinformatycznego i zarządzania technicznego jest bez wątpienia poważnym wyzwaniem. Trudno jednak abstrahować od faktu, że dziś coraz więcej pracowników i uczniów posiada, praktycznie bez przerwy przy sobie, urządzenia mobilne służące między innymi do dostępu do zasobów internetowych i intranetowych. Umożliwienie wpinania urządzeń własnych typu smartfon/tablet/laptop użytkowników w sieć instytucji wymaga dużych przygotowań i nakładów na infrastrukturę oraz zwiększonej

obsługi bieżącej rozwiązań teleinformatycznych wdrożonych w danej jednostce oświatowej. Stąd jedynie poziom profesjonalny daje szansę poniesienia stosownych nakładów oraz wytworzenia odpowiednich rozwiązań formalno-operacyjnych. Na poziomach słabszych nie powinno się jej rozpatrywać. Koncepcja BYOD została rozwinięta w osobnym załączniku do niniejszego dokumentu (patrz: Załącznik nr 9).

Rys. 4 Model profilaktyczny - aspekt techniczny

Źródło: opracowanie Krzysztof Silicki

Dział II. Interwencja
Reagowanie w przypadku wystąpienia cyberproblemów

Zaproponowane w poprzednim rozdziale działania koncentrują się na zapobieganiu zjawiskom i zachowaniom niepożądanym w cyberprzestrzeni. Ich głównym celem jest zbudowanie świadomości użytkownika sieci i umiejętności identyfikowania zagrożeń. Na kompleksową znajomość tych zagadnień składają nie tylko informacje i kwalifikacje pozwalające skutecznie uniknąć cyberproblemów, ale także wskazujące jak prawidłowo reagować w przypadku ich wystąpienia. Równoważną częścią modelu bezpieczeństwa online w placówce oświatowej są modele interwencyjne, których zastosowanie pozwala skutecznie reagować na niebezpieczne zjawiska oraz eliminować lub ograniczać negatywne skutki niepożądanych zachowań w sieci.

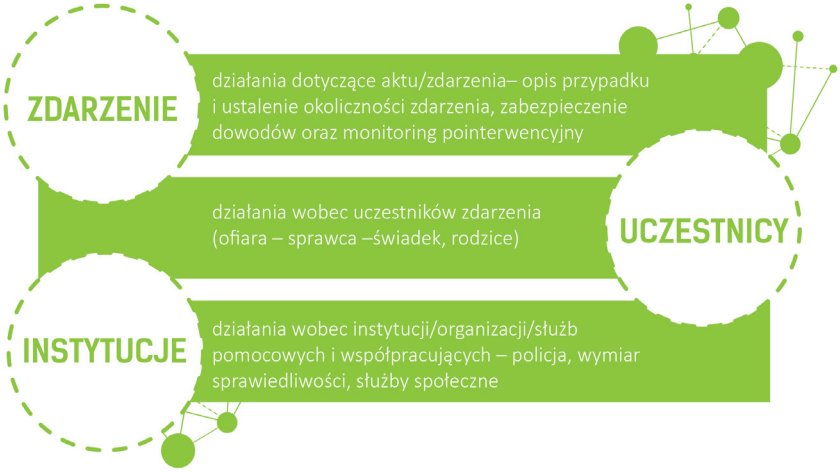
Model działań interwencyjnych

Przedstawiony poniżej model zawiera propozycje postępowania szkół i placówek oświatowych w sytuacji wystąpienia incydentu związanego z zagrożeniem w sferze online lub podejrzenia wystąpienia takiego incydentu z udziałem ucznia. Schemat działania stanowi zbiór wskazówek i zaleceń dotyczących sposobu reagowania pracowników placówek oświatowych na ujawnione zdarzenia związane z naruszeniem bezpieczeństwa w Internecie. Procedura została opracowana na podstawie literatury przedmiotu, przy wykorzystaniu dobrych praktyk zebranych przez placówki oświatowe oraz odpowiednich przepisów prawa.[2] Placówka może skorzystać z przygotowanej propozycji lub ją dopasować do własnych potrzeb i możliwości.

MODEL INTERWENCYJNY ZAWIERA NASTĘPUJĄCE ELEMENTY:

- działania wobec aktu/zdarzenia – opis przypadku, ustalenie okoliczności zdarzenia, zabezpieczenie dowodów oraz monitoring pointerwencyjny,
- działania wobec uczestników zdarzenia (ofiara – sprawca –świadek, rodzice),
- działania wobec instytucji/ organizacji/służb pomocowych i współpracujących – policja, wymiar sprawiedliwości, służby społeczne.

Rys.5 Model interwencyjny - aspekt społeczny



Źródło: opracowanie Agnieszka Wrońska, Zuzanna Polak

2 Ustawa z dnia 26 października 1982 roku o postępowaniu w sprawach nieletnich oraz odpowiednie rozporządzenia do ustawy.

Przedstawiony model zawiera grupę elementów, które w zależności od rodzaju zdarzenia powinny obejmować odpowiadające im kolejne etapy rozwiązywania sytuacji ryzyka, których propozycje znajdują się w dalszej części dokumentu.

Działania wobec aktu/zdarzenia

Działania wobec aktu/zdarzenia dotyczą pozyskania informacji na temat incydentu, przyjęcia zgłoszenia, ustalenia okoliczności zdarzenia, pełnej jego analizy wraz z zebraniem i zabezpieczeniem dowodów oraz prowadzeniem dokumentacji i monitoringu pointerwencyjnego.

Pozyskanie informacji i przyjęcie zgłoszenia

Informacja o zdarzeniu stanowi punkt wyjścia do podjęcia interwencji. Należy przyjąć założenie, że informacja może być dostarczona przez różne osoby i w różny sposób. Poinformować mogą zarówno osoby poszkodowane, inni uczniowie oraz osoby dorosłe – rodzice i pracownicy placówki. Ważnym elementem jest zatem stworzenie możliwości bezpiecznego i skutecznego systemu komunikowania o zdarzeniu. Niezbędnym elementem jest publicznie dostępna informacja komu i w jaki sposób można przekazać zgłoszenie w celu dalszego procedowania sprawy (patrz: Zespół ds. Bezpieczeństwa Online). Zgłoszenia mogą odbywać się w sposób bezpośredni – każdemu pracownikowi szkoły, który zobowiązany jest do przekazania jej wychowawcy oraz pośredni np.: za pomocą anonimowych punktów zgłoszeń np. skrzynki.*

Skrzynka *- zastosowanie „skrzynek" pozwala na anonimowe zgłoszenie zdarzenia, co pozwala na ujawnienie aktu bez konieczności bezpośredniego angażowania się. Ma to szczególne znaczenie w przypadkach zgłaszania cyberprzemocy, gdy świadkowie obawiają się stygmatyzacji lub/i stania się ofiarą. Koniecznym warunkiem korzystania ze „skrzynek" jest poprzedzenie ich wprowadzania działaniami informacyjno - edukacyjnymi wskazującymi skuteczności i celowość ich stosowania oraz zmniejszenie ryzyka niewłaściwego wykorzystania.*

Zastosowanie tej metody zgłaszania jest opcjonalne i zależne od uwarunkowań konkretnej placówki.

ZADANIA ZESPOŁU DS. BEZPIECZEŃSTWA ONLINE

Zadania zespołu powinny koncentrować się nie tylko na ustaleniu okoliczności zdarzenia, przerwaniu aktu oraz dokumentacji zdarzenia, ale przede wszystkim na udzieleniu wsparcia ofierze oraz wyciągnięciu konsekwencji wobec sprawcy przemocy. Zadania i procedury tej grupy muszą być znane wszystkim członkom społeczności szkolnej. Ustalenia zespołu oraz planowane przez niego podjęcie kolejnych działań musi przebiegać w ścisłej współpracy z rodzicami/opiekunami prawnymi osoby małoletniej zaangażowanej w zdarzenie. Obowiązkiem jest sporządzenie dokumentacji z zebranego i analizowanego materiału. Standard nie narzuca placówkom formy prowadzenia dokumentacji, ale rekomendowane jest, aby dokumentacja miała prostą formę oraz zawierała następujące elementy: opis przebiegu zdarzenia, osoby uczestniczące zabezpieczone dowody, zastosowane środki wychowawcze i dyscyplinarne, plan monitoringu zdarzenia (Dokumentacja procedury interwencyjnej zastosowanej w placówce - Załącznik nr 6). Ważnym elementem dokumentu są notatki służbowe członków Zespołu (pedagoga, psychologa, wychowawcy) z rozmów ze sprawcą, poszkodowanym, ich rodzicami oraz świadkami zdarzenia. Powinny zawierać informację o miejscu rozmowy, personalia osób biorących w niej udział oraz opis ustalonego przebiegu wydarzeń. Dokumentacja musi być prowadzona z poszanowaniem prywatności osób uczestniczących w zdarzeniu wraz z zapewnieniem niezbędnej poufności przechowywanych i przetwarzanych danych.

Ustalenie okoliczności zdarzenia, analiza zdarzenia oraz zebranie i zabezpieczenie dowodów

Każde zgłoszenie powinno zostać zarejestrowane, przenalizowane oraz odpowiednio udokumentowane. W analizie zdarzenia powinien znaleźć się dokładny opis zdarzenia, wskazanie osób uczestniczących i/lub podjętych działań w celu identyfikacji sprawcy oraz materiały dokumentujące zdarzenie.

Dowodem mogą być: wiadomości e-mailowe, SMS-y i MMS-y, historia połączeń w telefonie komórkowym, wiadomości nagrane na pocztę głosową telefonu komórkowego, zrzuty ekranu prezentujące wpisy na stronach internetowych, komentarze do wpisów lub zdjęć w serwisach społecznościowych, blogach, zdjęcia, grafiki, treści rozmów prowadzonych przy użyciu komunikatorów lub czatów. Dowody powinny zostać zabezpieczone i opisane (data otrzymania, treść wiadomości, dane nadawcy tj. nazwa użytkownika, adres email, adres strony WWW). Właściwe opisanie dowodów ułatwia dalsze postępowanie, szczególnie w sytuacji naruszenia prawa. Jeśli zebrane dowody wskazują na naruszenie prawa należy niezwłocznie powiadomić Policję i przekazać jej cały zgromadzony materiał dowodowy.

W celu usunięcia z Internetu kompromitujących lub krzywdzących materiałów należy poinformować rodziców/opiekunów prawnych o możliwościach usunięcia materiałów we współpracy z administratorami serwisów internetowych, operatorami telekomunikacyjnymi oraz organizacjami pomocowymi (patrz: Dział prawny)**.**

W JAKI SPOSÓB ZABEZPIECZYĆ MATERIAŁY?

- **zachowywanie wiadomości, e-maili** - w przypadku naruszenia przy użyciu telefonu komórkowego ważne jest, by nie usuwać odpowiednich wiadomości SMS, MMS, historii połączeń, nagrań z poczty głosowej. W przypadku naruszeń za pośrednictwem Internetu należy zachować wszystkie odpowiednie wiadomości e-mail. Zgłaszając sprawę na policję, należy przedstawić wydruki odpowiednich komunikatów z jednoczesnym pokazaniem tzw. nagłówków wiadomości. Należy sprawdzić jak włączyć tę funkcję w danym programie/aplikacji do obsługi poczty.
- **komentarze** - niektóre naruszenia są dokonywane za pośrednictwem komentarzy pod profilem w serwisie społecznościowym, blogiem czy filmem w serwisie video. Treść komentarzy również warto zachować, wraz z pokazaniem autora danego wpisu. Można to zrobić wykonując zrzut ekranu prezentujący serwis oraz konkretny komentarz. Aby zrobić zrzut ekranu, można skorzystać z dedykowanej aplikacji lub systemowo za pomocą klawisza PrintScreen (PrtScn).
- **archiwizowanie treści rozmów w komunikatorach** - korzystając z komunikatorów i czatów, warto uruchomić funkcję archiwizacji – opcję automatycznego zapisywania wszystkich prowadzonych przez użytkownika rozmów (czasami opcja nazywa się „Historią"). Umożliwia ona śledzenie treści poszczególnych rozmów.
- **linki-** o ile to możliwe, a treści nie zostały jeszcze usunięte, istotne jest wskazanie konkretnych adresów URL (linków). Adresy te należy zapisać w edytorze tekstu, a następnie wydrukować.

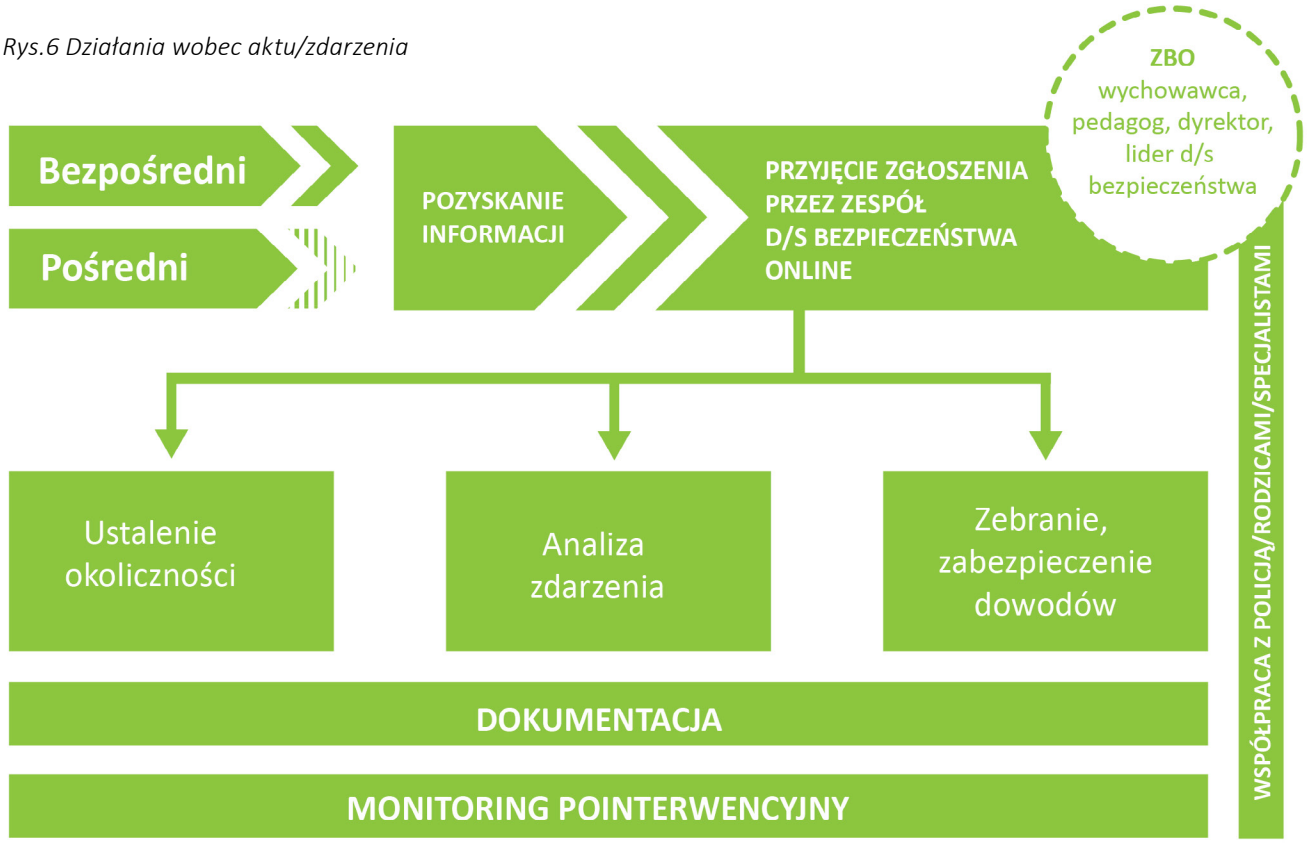
Identyfikacja sprawcy/sprawców

Wbrew przekonaniom wielu młodych internatów o anonimowości, w sieci istnieje wiele sposobów identyfikacji osób naruszających bezpieczeństwo w Internecie czy łamiących prawo. Nie zawsze jest to proces łatwy czy możliwy w ramach posiadanych kompetencji w szkołach i placówkach oświatowych. Niektórzy sprawcy posługują się „skradzioną tożsamością" wykorzystując urządzenia, konta pocztowe czy profile w serwisach społecznościowych innych osób, korzystają z bramek internetowych, kart prepaid lub jednorazowo zakładanych profili czy kont e-mailowych. Sprawcy cyberprzestępstw niejednokrotnie wykorzystują zaawansowane technologie i metody utrudniające ustalenie ich tożsamości. Wsparcie w takich sytuacjach można otrzymać od policji czy administratorów serwisów internetowych (patrz: Współpraca z policją). W przypadku cyberprzemocy w identyfikacji sprawcy może pomóc również ofiara/osoba pokrzywdzona, która może znać sprawcę oraz potrafi wytypować potencjalnych agresorów posiadających motyw, np. osobiście skonfliktowanych oraz świadkowie, którzy mogą posiadać informacje na temat autora obraźliwych wpisów czy przesyłanych zdjęć.

Monitoring pointerwencyjny

Niezwykle istotnym elementem procedury interwencyjnej jest systematyczne prowadzenie monitoringu zdarzenia po jego przerwaniu i zastosowaniu środków naprawczych. W praktyce oznacza to przede wszystkim regularne pozyskiwanie informacji na temat sytuacji, potrzeb uczestników incydentu oraz reagowania na ewentualne pojawienie się odroczonych skutków, a także możliwość oceny prawidłowości podjętych działań.

Rys.6 Działania wobec aktu/zdarzenia



Źródło: opracowanie Agnieszka Wrońska, Zuzanna Polak

Działania wobec uczestników zdarzenia

Działania wobec uczestników zdarzenia z zakresu naruszenia bezpieczeństwa w cyberprzestrzeni, powinny być dedykowane zarówno osobom poszkodowanym (ofiarom), sprawcom oraz świadkom zdarzenia (z uwagi na zróżnicowany charakter incydentu). Niektóre formy dotyczyć mogą pracy wyłącznie z ofiarami, inne wymagać będą zastosowania różnych działań wychowawczych i/lub dyscyplinarnych wobec sprawcy (patrz: Procedury reagowania na wybrane zagrożenia). Należy pamiętać, że podejmowane działania dotyczą w większości przypadków osób nieletnich, więc stroną uczestniczącą jest także rodzic/opiekun prawny.

Zasadnym jest, by podejmowane przez placówkę działania były zaplanowane, stopniowe, dostosowane do sytuacji oraz przebiegały w proponowanej kolejności:

1. Rozmowa uczestnika zdarzenia z przedstawicielami Zespołu ds. Bezpieczeństwa Online (wychowawca/pedagog/psycholog) odpowiednia do charakteru zdarzenia oraz roli uczestnika (ofiara/sprawca/świadek).

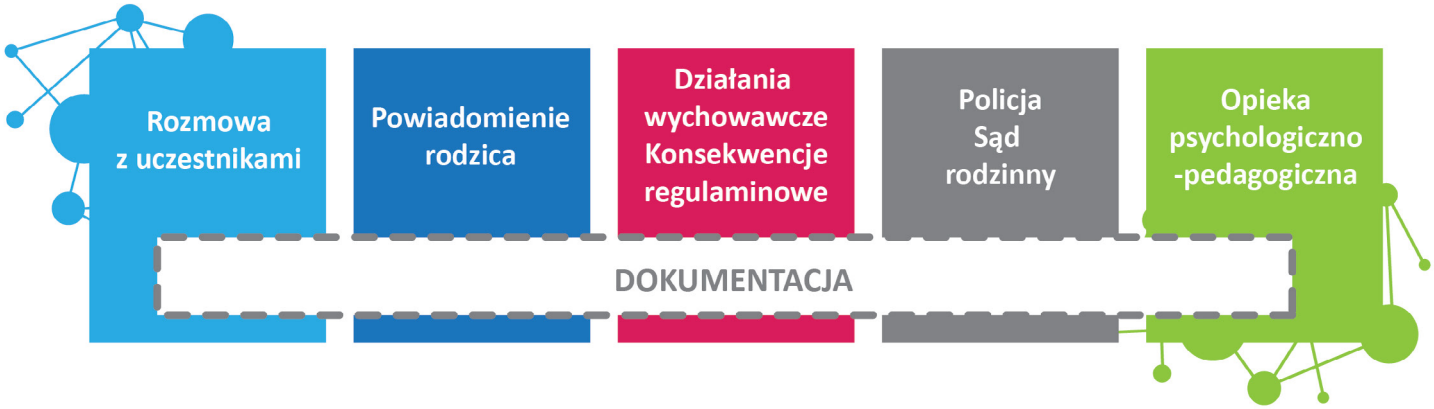
2. Powiadomienie rodziców/opiekunów prawnych uczestników zdarzenia oraz informowanie ich o podejmowanych działaniach i ewentualnych konsekwencjach regulaminowych oraz przedstawienie propozycji wsparcia.

3. Prowadzenie działań wychowawczych i zastosowanie konsekwencji regulaminowych wobec znanego sprawcy (objętego opieką danej placówki).

4. Powiadomienie policji/sądu rodzinnego w przypadku naruszenia prawa (patrz: Współpraca z policją).

5. Otoczenie wsparciem i opieką psychologiczno-pedagogiczną uczestników zdarzenia.

Rys.7 Działania wobec uczestników



Źródło: opracowanie Agnieszka Wrońska, Zuzanna Polak

Działania wobec instytucji/organizacji/służb pomocowych i współpracujących – policja, sąd rodzinny, służby społeczne

Większość sytuacji może znaleźć pozytywne rozwiązanie dzięki metodom i środkom wychowawczym stosowanym w placówkach oświatowych. Niekiedy jednak nieodzowne jest wsparcie instytucjonalne ze strony policji i sądu rodzinnego czy specjalistycznych placówek. W razie pozyskania informacji o cyberprzestępstwie i zidentyfikowaniu jego sprawcy, działania szkoły będą uzależnione od wieku sprawcy oraz charakteru popełnionego czynu.[3]

Obowiązki szkoły i placówek oświatowych w zakresie współpracy z policją i sądem rodzinnym

Na instytucjach publicznych, takich jak szkoła i inne placówki oświatowe, spoczywa szczególny obowiązek współpracy z policją oraz sądem rodzinnym. Szkoła i placówki oświatowe, przez osobę dyrektora, są zobligowane do zawiadomienia policji lub sądu rodzinnego o popełnieniu przez nieletniego czynu karalnego o którym dowiedziały się w związku ze swoją działalnością (*art. 4 § 2 upn*).[4] Ponadto spoczywa na nich obowiązek podjęcia niezbędnych czynności, aby nie dopuścić do zatarcia jego śladów oraz zabezpieczenia dowodów (*art. 4 § 3 upn*). Obowiązek powiadomienia policji przez dyrektora nie dotyczy czynów ściganych przez organy na wniosek pokrzywdzonego oraz z oskarżenia prywatnego, gdy sam pokrzywdzony występuje w charakterze oskarżyciela. W sieci internetowej najczęściej będą popełniane takie przestępstwa jak wskazane na liście poniżej.

Rys.8 Przestępstwa zgłaszane przez dyrektora placówki i na wniosek pokrzywdzonego

Źródło: opracowanie Urszula Brochwicz, Agnieszka Wrońska

3 W sytuacji gdy sprawcą jest nieletni, tj. osoba w wieku od 13 do 17 lat, zastosowanie będą mieć przepisy ustawy z dnia 26 października 1982 roku o postępowaniu w sprawach nieletnich (dalej upn) W razie zaś, gdy sprawca ukończył 17 lat, ponosić będzie odpowiedzialność karną na podstawie ustawy z dnia 6 czerwca 1997 roku Kodeks karny (dalej: kk) i będą mieć do niego zastosowanie przepisy kpk.
4 Ustawa z dnia 26 października 1982 roku o postępowaniu w sprawach nieletnich oraz odpowiednie rozporządzenia do ustawy.

W razie wystąpienia przez pokrzywdzonego ze skargą lub oskarżeniem, współpraca placówki oświatowej z policją oraz sądem rodzinnym może polegać w szczególności, na udzielaniu informacji i pomocy przy przeprowadzaniu czynności postępowania w szkole, przekazaniu dokumentów oraz udostępnieniu danych ucznia.

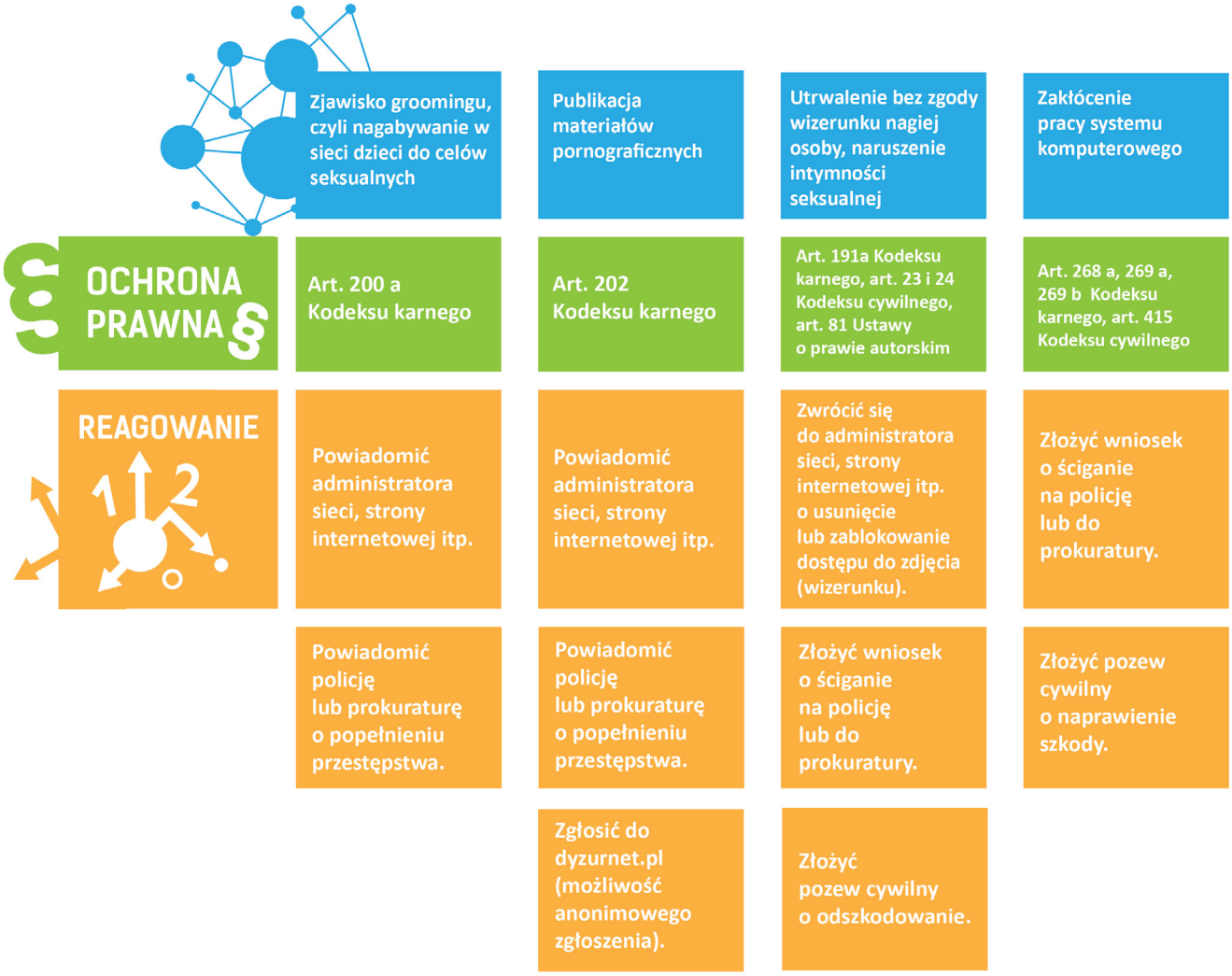
Pozostałe osoby, w tym uczniowie oraz nauczyciele mają, w razie uzyskania informacji o czynie karalnym, społeczny obowiązek zawiadomienia policji oraz sądu rodzinnego. Ponadto taki obowiązek poinformowania, a także przeciwdziałania, ciąży na każdym, kto stwierdzi istnienie okoliczności świadczących o demoralizacji nieletniego, w szczególności: naruszania zasad współżycia społecznego, systematyczne uchylanie się od obowiązku szkolnego lub kształcenia zawodowego, używanie alkoholu lub innych środków w celu wprowadzenia się w stan odurzenia, uprawianie nierządu, włóczęgostwa, udziału w grupach przestępczych (*art. 4 § 1 upn*).

Placówka oświatowa powinna powiadomić sąd rodzinny w sytuacjach, gdy pomimo zastosowanej procedury i dostępnych środków wychowawczych podopieczny placówki kontynuuje działania naruszające bezpieczeństwo, dodatkowo gdy rodzice/opiekunowie prawni odmawiają współpracy z placówką, oraz szczególnie w sytuacji, gdy placówce oświatowej znane są inne przejawy demoralizacji.

Rys.9 Czyny zabronione i działania szkodliwe - sposoby reagowania

Źródło: opracowanie Urszula Brochwicz, Agnieszka Wrońska

Rys.10 Czyny zabronione i działania szkodliwe - sposoby reagowania



Źródło: opracowanie Urszula Brochwicz, Agnieszka Wrońska

Współpraca ze służbami społecznymi i placówkami specjalistycznymi

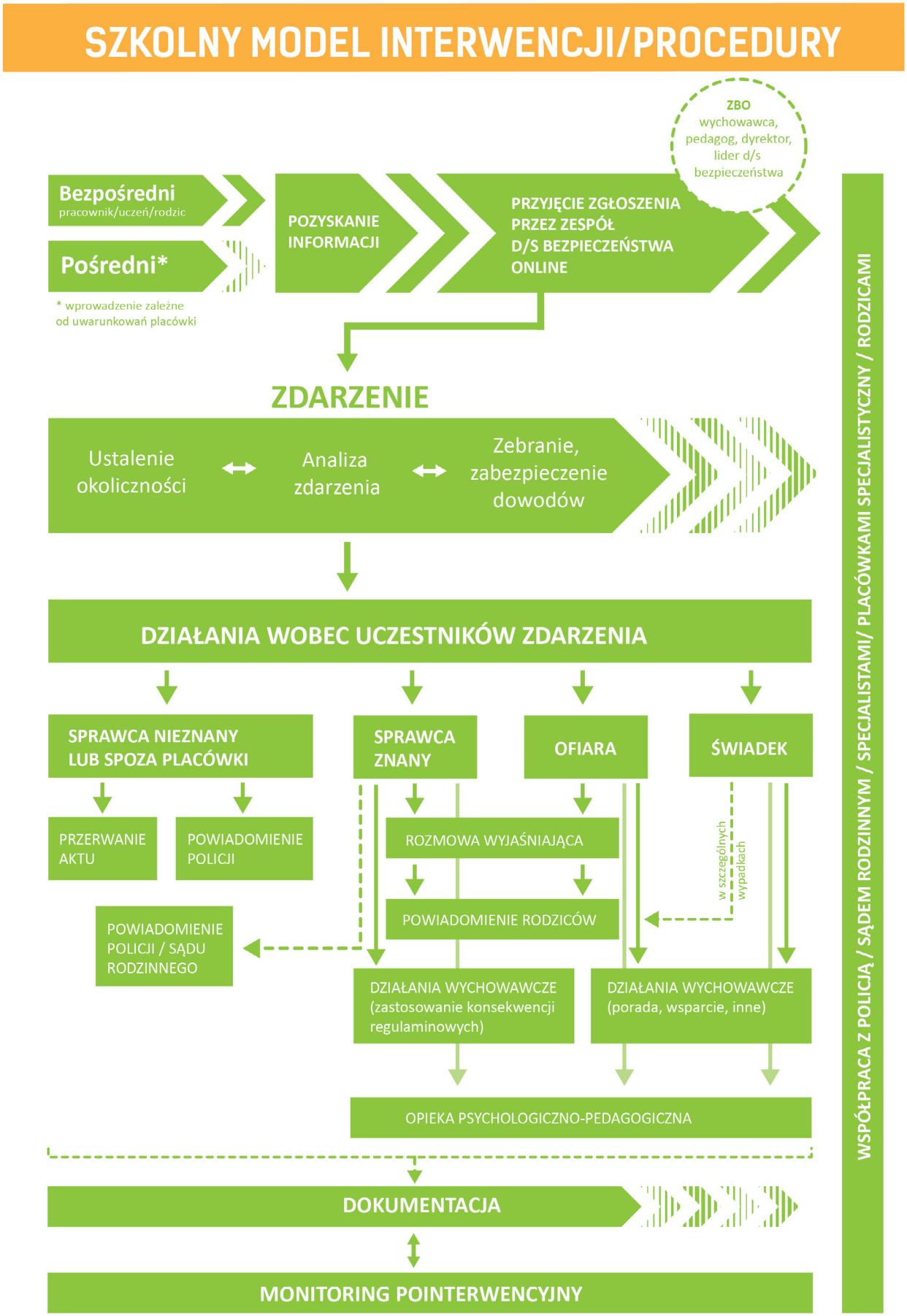
W przypadku zaistnienia potrzeby kontynuowania działań pomocowych i uczestnictwa w programach terapeutycznych placówka, we współpracy z rodzicami i za ich zgodą, kieruje podopiecznych na odpowiednie zajęcia.

Współpraca placówek oświatowych ze specjalistycznymi placówkami świadczącymi usługi na rzecz dzieci i młodzieży jest opisana m.in. w Rozporządzeniu Ministra Edukacji Narodowej z dnia 1 lutego 2013 r. w sprawie szczegółowych zasad działania publicznych poradni psychologiczno-pedagogicznych, w tym publicznych poradni specjalistycznych.

W razie ustanowienia kuratora sądowego (zawodowego lub społecznego) dla uczestnika zdarzenia, dyrektor placówki oświatowej powinien na bieżąco informować kuratora o niepokojących zdarzeniach z udziałem jego podopiecznego.

Gdy uczestnik zdarzenia lub jego rodzina korzystają z pomocy społecznej w ramach np. pomocy oferowanej przez Powiatowe Centra Pomocy Rodzinie (PCPR), wskazana jest współpraca dyrektora placówki oświatowej z PCPR mająca na celu wspieranie rodzin przeżywających trudności.

Rys.11 Model działań interwencyjnych



Źródło: opracowani Agnieszka Wrońska, Zuzanna Polak

Współpraca z dostawcami usług internetowych i operatorami sieci telekomunikacyjnych

Współpraca placówki oświatowej z dostawcami usług internetowych w zakresie przerwania aktu (np. usunięcie krzywdzących i ośmieszających materiałów) nie jest regulowana przepisami prawnymi i w większości przypadków jest przykładem zrozumienia problemu oraz chęci współpracy administratorów konkretnych stron, serwisów czy portali internetowych. W przypadku polskich serwisów internetowych, poinformowanie o cyberprzestępstwie administratora, zobowiązuje go do usunięcia bezprawnych treści z sieci *(art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną)*. Administrator nie jest zobowiązany do udostępnienia danych, które pozwolą na identyfikację sprawcy. Dane, takie jak np. imię i nazwisko użytkownika portalu lub nr IP, objęte są tajemnicą telekomunikacyjną. Policja może przyjąć od osoby pokrzywdzonej skargę o cyberprzestępstwie. Następnie policja przesyła ją do sądu, który może zobowiązać operatora sieci komórkowej, administratora portalu internetowego czy dostawcę usługi internetowej do ujawienia danych sprawcy. Do zobowiązania takich podmiotów do ujawnienia danych sprawcy, uprawniony jest także prokurator *(art. 180 ust. 1a pkt 2 ustawy z dnia 16 lipca 2004 roku Prawo telekomunikacyjne, art. 488 § 1 oraz 218 § 1 ustawy z dnia 6 czerwca 1997 roku Kodeks postępowania karnego).*

Zastosowanie modelu działań interwencyjnych – procedury reagowania wobec wybranych rodzajów zagrożeń

Procedura interwencyjna: Cyberprzemoc

1. Działania wobec zdarzenia

- **Pozyskanie informacji i przyjęcie zgłoszenia**

  W przypadku atakowania dziecka za pośrednictwem internetu osobą zgłaszającą problem może być rodzic/opiekun prawny, opiekun pracowni informatycznej w placówce lub zaniepokojony rówieśnik ofiary (świadek). Ze względu na potencjalne bardzo negatywne skutki cyberprzemocy dla ofiary, należy dążyć do jak najszybszego przerwania aktu.

- **Ustalenie okoliczności zdarzenia, analiza zdarzenia oraz zebranie i zabezpieczenie dowodów**

  Członek ZBO dysponujący odpowiednią wiedzą techniczną powinien służyć wsparciem rodzicom/opiekunom prawnym w kwestii zabezpieczenia odpowiednich materiałów na prywatnym komputerze ofiary (zrzuty ekranu, zapisy rozmów, wiadomości email oraz w komunikatorach) lub zabezpieczyć je na urządzeniu należącym do placówki.

  Niektóre przypadki cyberprzemocy są skomplikowane (spirala agresji - cyberprzemoc w odpowiedzi na wcześniejszy incydent lub konflikty w świecie rzeczywistym), więc ustalenie okoliczności zdarzenia oraz ofiary/sprawcy może być trudne. Należy dążyć do jak najbardziej dokładnej analizy sytuacji.

- **Identyfikacja sprawcy/sprawców**

  Identyfikacja sprawcy cyberprzemocy jest niezwykle istotna i warunkuje dalsze postępowanie placówki. W przypadku sprawcy będącego podopiecznym placówki można zastosować konsekwencje przewidziane regulaminem.

2. Działania wobec uczestników zdarzenia

Rozmowa uczestników zdarzenia z przedstawicielami Zespołu ds. Bezpieczeństwa Online (wychowawca/pedagog/psycholog) odpowiednia do charakteru zdarzenia oraz roli uczestnika (ofiara/sprawca/świadek)

- **Działania wobec ofiary cyberprzemocy**

  W efekcie rozmowy z wychowawcą/pedagogiem lub innym wyznaczonym członkiem ZBO ofiara powinna otrzymać komunikat, że placówka jest w stanie efektywnie reagować na cyberprzemoc oraz wspierać ucznia w trudnych sytuacjach. Ponadto podopieczny powinien otrzymać poradę, jak ma się zachować, aby zapewnić sobie poczucie bezpieczeństwa i nie doprowadzić do eskalacji prześladowania. Nie należy również stosować metody konfrontacyjnej ofiary ze sprawcą.

- **Działania wobec sprawcy cyberprzemocy, będącego podopiecznym placówki**

  W efekcie rozmowy z wybranym członkiem ZBO sprawca powinien otrzymać komunikat o braku akceptacji jakichkolwiek form przemocy oraz informację o konsekwencjach regulaminowych, które zostaną wobec niego zastosowane. Ponadto winny powinien zaprzestać dalszego stosowania form cyberprzemocy, usunąć krzywdzące materiały z sieci oraz określić sposoby zadośćuczynienia wobec ofiary. W przypadku, gdy w akcie cyberprzemocy brała udział grupa sprawców należy procedurę potraktować indywidualnie dostosowując rozmowę oraz środki dyscyplinarne do zaistniałego przewinienia zgodną z wewnętrznymi przepisami szkoły. Sprawcę również należy objąć opieką psychologiczno-pedagogiczną, której celem jest zmiana postawy i postępowania ucznia, jednocześnie zapobiegając jego demoralizacji.

- **Ochrona świadków**

  Podejmując działania interwencyjne wobec cybeprzemocy należy pamiętać o roli, jaką w tym procesie odgrywa świadek zdarzenia i następstwach jakich może doświadczyć. Ważne jest, by zapewnić mu poczucie bezpieczeństwa i by w wyniku interwencji nie narazić go na działania przemocowe ze strony sprawcy. Niedopuszczalne jest konfrontowanie świadka ze sprawcą czy ostentacyjne eksponowanie jego roli. Brak dbałości o podstawowe zasady bezpieczeństwa może sprawić, że przy kolejnym lub innym akcie przemocy świadek cyberprzemocy nie zgłosi zdarzenia, nie będzie chciał uczestniczyć w procesie wyjaśniania, nie podejmie żadnych działań na rzecz obrony słabszych i pokrzywdzonych.

Należy pamiętać o:

- **Powiadomieniu rodziców/opiekunów prawnych, uczestników zdarzenia oraz informowaniu ich o podejmowanych działaniach oraz przedstawieniu propozycji wsparcia.**
- **Powiadomieniu policji/sądu rodzinnego w przypadku naruszenia prawa (patrz: Współpraca z policją).**
- **Otoczeniu wsparciem i opieką psychologiczno-pedagogiczną uczestników zdarzenia.**

3. Działania wobec instytucji/organizacji/służb pomocowych i współpracujących – policja, sąd rodzinny, służby społeczne

- **Obowiązki szkoły i placówek oświatowych w zakresie współpracy z policją i sądem rodzinnym**

  Cyberprzemoc może wypełniać znamiona różnych przestępstw, ale są one ścigane na wniosek pokrzywdzonego. W przypadku, gdy rodzice/opiekunowie prawni zdecydują się na zgłoszenie sprawy do policji, szkoła może służyć wsparciem, np. kontaktując rodziców z odpowiednią jednostką.

  Placówka oświatowa powinna powiadomić sąd rodzinny w sytuacjach, gdy pomimo zastosowanej procedury i dostępnych środków wychowawczych, sprawca (podopieczny placówki) kontynuuje działania naruszające bezpieczeństwo, dodatkowo gdy rodzice/opiekunowie prawni odmawiają współpracy z placówką oraz szczególnie w sytuacji gdy placówce oświatowej znane są inne przejawy demoralizacji.

- **Współpraca ze służbami społecznymi i placówkami specjalistycznymi**

  Jeżeli zachodzi taka potrzeba, zaleca się skorzystać ze specjalistycznej formy opieki psychologicznej (w porozumieniu z rodzicami/opiekunami prawnymi) oferowanej przez poradnie specjalistyczne.

- **Współpraca z dostawcami usług internetowych i operatorami sieci telekomunikacyjnych**

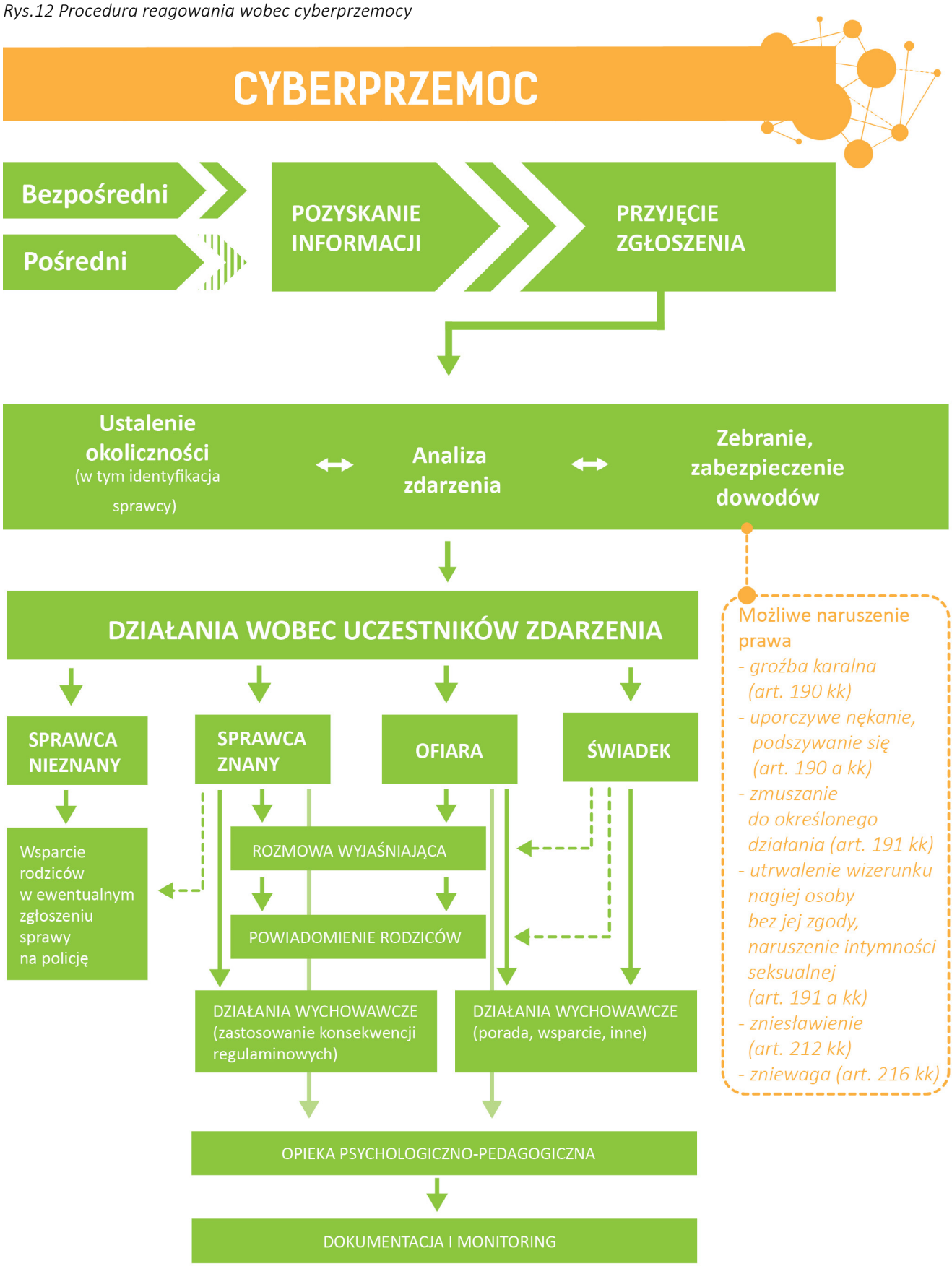
  Współpraca z ww. podmiotami nie jest konieczna – niezbędne ustalenia zostaną poczynione przez policję. Przypadkiem szczególnym będzie sytuacja rozpowszechnienia kompromitujących ofiarę materiałów w sieci (patrz procedura: Nielegalne i szkodliwe treści).

4. Dokumentacja i monitoring pointerwencyjny

Dokumentacja dotycząca cyberprzemocy powinna zawierać takie elementy jak: opis przebiegu zdarzenia, osoby uczestniczące zabezpieczone dowody, zastosowane środki wychowawcze i dyscyplinarne, plan monitoringu zdarzenia oraz notatki służbowe członków zespołu (Załącznik nr 6. Dokumentacja procedury interwencyjnej zastosowanej w placówce). Z uwagi na specyfikę problemu (ochrona świadków, ochrona sprawców przed wiktymizacją) rekomenduje się prowadzenie dokumentacji z poszanowaniem prywatności uczestników oraz z zapewnieniem poufności przechowywanych i przetwarzanych danych.

Monitoring powinien być prowadzony systematycznie po przerwaniu aktu i zastosowaniu środków naprawczych.

Rys.12 Procedura reagowania wobec cyberprzemocy



Źródło: opracowanie Agnieszka Wrońska, Zuzanna Polak

Procedura interwencyjna: Niebezpieczne kontakty online

1. Działania wobec zdarzenia

- **Pozyskanie informacji i przyjęcie zgłoszenia**

  W przypadku uwodzenia dziecka przez Internet osobą zgłaszającą problem może być rodzic/opiekun prawny, opiekun pracowni informatycznej w placówce lub zaniepokojony rówieśnik ofiary. Ze względu na możliwe konsekwencje incydentu (spotkanie z uwodzicielem w świecie rzeczywistym, wykorzystanie seksualne dziecka w świecie rzeczywistym lub przymuszenie go do odbycia aktywności seksualnej w czasie rozmowy internetowej z użyciem kamerki internetowej oraz nagranie materiału dla celów szantażu) należy działać niezwykle szybko.

- **Ustalenie okoliczności zdarzenia, analiza zdarzenia oraz zebranie i zabezpieczenie dowodów**

  Członek ZBO dysponujący odpowiednią wiedzą techniczną powinien służyć wsparciem rodzicom/opiekunom prawnym w kwestii zabezpieczenia odpowiednich materiałów na prywatnym komputerze ofiary (zrzuty ekranu, zapisy rozmów, wiadomości email oraz w komunikatorach) lub zabezpieczyć je na urządzeniu należącym do placówki.

- **Identyfikacja sprawcy/sprawców**

  Identyfikacja sprawcy w przypadku uwodzenia przez Internet w większości przypadków wykracza poza kompetencje i możliwości placówki, która powinna sprawę przekazać policji (patrz: Współpraca z policją).

2. Działania wobec uczestników zdarzenia

Rozmowa uczestnika zdarzenia z przedstawicielami Zespołu ds. Bezpieczeństwa Online (wychowawca/pedagog/psycholog) w zależności od charakteru zdarzenia oraz roli uczestnika (ofiara/świadek). Otoczenie wsparciem i opieką psychologiczno-pedagogiczną uczestników zdarzenia.

Małoletni powinien zostać otoczony szczególną opieką psychologiczno-pedagogiczną. Należy zapewnić mu komfort psychiczny, upewnić się, że kontakt z osobą uwodzącą został przerwany oraz przeanalizować sytuację rodzinną. Zdarza się, że dziecko podejmuje kontakt z nieznajomymi w sieci z powodów konfliktów rodzinnych lub braku poczucia odpowiedniego wsparcia wśród bliskich.

Zaleca się skorzystać ze specjalistycznej formy opieki psychologicznej w porozumieniu z rodzicami/opiekunami prawnymi.

Jeżeli zgłaszającym był rówieśnik należy również objąć go opieką, pozytywnie wzmacniając jego reakcję na sytuację.

Należy pamiętać o:

- **Powiadomieniu rodziców/opiekunów prawnych uczestników zdarzenia oraz informowaniu ich o podejmowanych działaniach oraz przedstawieniu propozycji wsparcia.**

- **Powiadomieniu policji/sądu rodzinnego w przypadku naruszenia prawa (patrz: Współpraca z policją).**

W przypadku ujawnienia sytuacji próby uwiedzenia małoletniego poniżej lat 15 przez osobę dorosłą należy w porozumieniu z rodzicami NIEZWŁOCZNIE powiadomić policję.

3. Działania wobec instytucji/organizacji/służb pomocowych i współpracujących – policja, sąd rodzinny, służby społeczne

- **Obowiązki szkoły i placówek oświatowych w zakresie współpracy z policją i sądem rodzinnym**

  Próba uwiedzenia dziecka poniżej 15 r.ż. przez internet jest przestępstwem ściganym z urzędu[5], dlatego też dyrektor placówki jest zobowiązany do zgłoszenia incydentu na policję.

- **Współpraca ze służbami społecznymi i placówkami specjalistycznymi**

  Zaleca się skorzystać ze specjalistycznej formy opieki psychologicznej w porozumieniu z rodzicami/opiekunami prawnymi oferowanej przez poradnie specjalistyczne.

- **Współpraca z dostawcami usług internetowych i operatorami sieci telekomunikacyjnych**

Współpraca z ww. podmiotami nie jest konieczna – konieczne ustalenia zostaną poczynione przez policję. Przypadkiem szczególnym będzie sytuacja rozpowszechnienia kompromitujących ofiarę materiałów w sieci (patrz procedura interwencyjna: Nielegalne i szkodliwe treści).

4. Dokumentacja i monitoring pointerwencyjny

Dokumentacja dotycząca incydentów związanych z niebezpiecznymi kontaktami online powinna zawierać takie elementy jak: opis przebiegu zdarzenia, osoby uczestniczące, zabezpieczone dowody, zastosowane środki wychowawcze, plan monitoringu zdarzenia oraz notatki służbowe członków zespołu (Dokumentacja - Załącznik nr 6. Dokumentacja procedury interwencyjnej zastosowanej w placówce). Rekomenduje się prowadzenie dokumentacji z poszanowaniem prywatności uczestników oraz z zapewnieniem poufności przechowywanych i przetwarzanych danych.

Monitoring powinien być prowadzony systematycznie po przerwaniu aktu i zastosowaniu środków naprawczych.

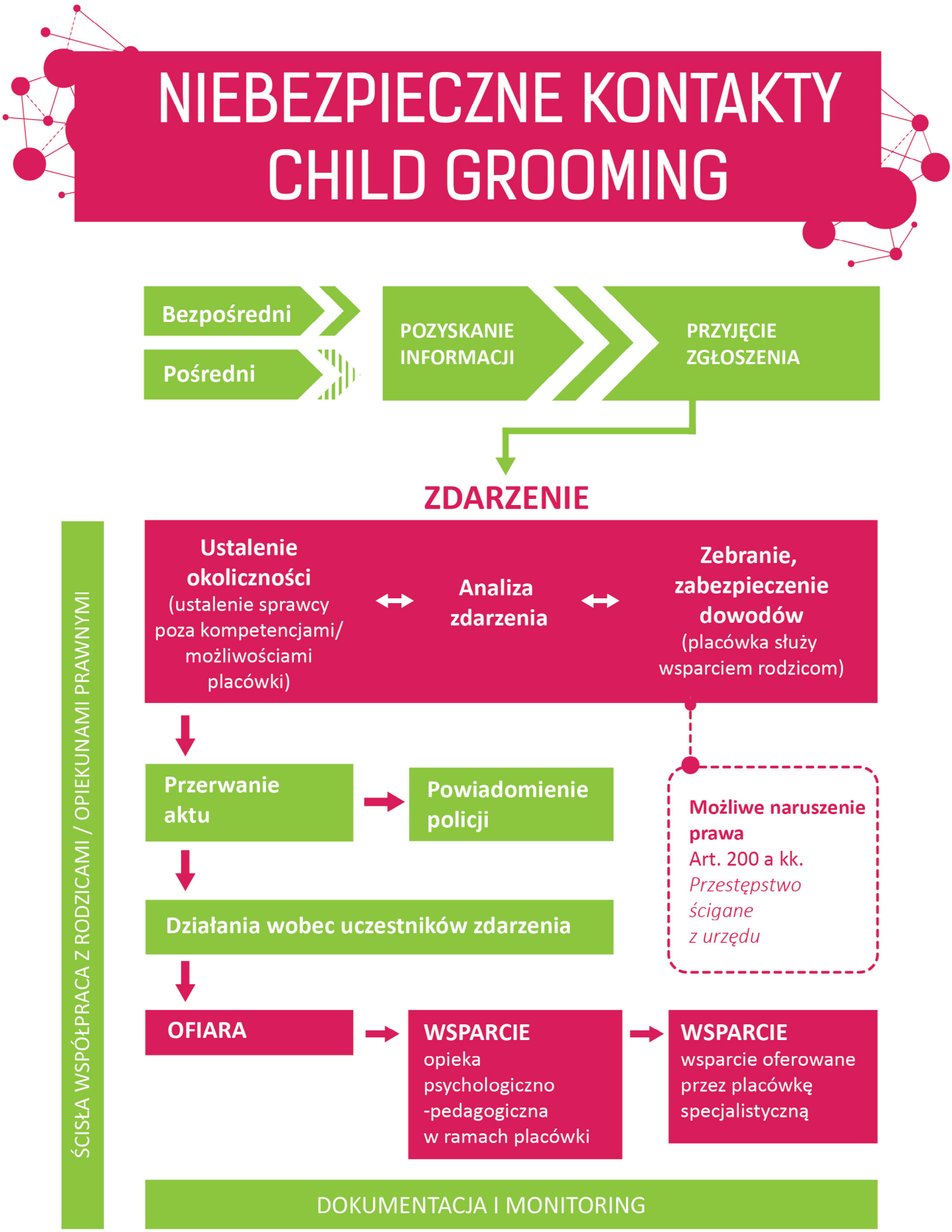
WAŻNE:

W przypadku ujawnienia innego niebezpiecznego kontaktu (werbunek do sekty lub innej grupy o potencjalnie zagrażających poglądach lub promującej niebezpieczne zachowania), procedura działań powinna przede wszystkim skupić się na ofierze i zapewnieniu jej pomocy psychologicznej. Niebezpieczne kontakty różnego rodzaju są często nawiązywane w przypadku, gdy dziecko przeżywa różnego rodzaju problemy psychiczne czy rodzinne w świecie offline.

Zaobserwowanie jakiegokolwiek antyzdrowotnego zachowania (samookaleczenia, restrykcyjna dieta, używanie substancji psychoaktywnych) powinno zwrócić uwagę pracownika placówki również na świat online. Tego typu zachowania mogą łączyć się z przynależnością ucznia do jakiejś niebezpiecznej społeczności działającej w internecie. Rodzice/opiekunowie prawni również powinni zostać poinformowani o takiej możliwości.

5 Art. 200a Kodeksu karnego

Rys.13 Procedura reagowania wobec incydentów związanych z niebezpiecznymi kontaktami online



Źródło: opracowanie Agnieszka Wrońska, Zuzanna Polak

Procedura interwencyjna: Nielegalne i szkodliwe treści

1. Działania wobec zdarzenia

- **Pozyskanie informacji i przyjęcie zgłoszenia**

  W przypadku kontaktu dziecka z treściami o charakterze pornograficznym (również z udziałem małoletniego – tzw. pornografią dziecięcą) osobą zgłaszającą problem może być rodzic/opiekun prawny, opiekun pracowni informatycznej w placówce lub zaniepokojony rówieśnik ofiary. Należy pamiętać, że kontakt z tego typu treściami mógł zostać wymuszony na dziecku w procesie uwodzenia, jako forma „oswojenia" dziecka z tego rodzaju seksualnością.

- **Ustalenie okoliczności zdarzenia, analiza zdarzenia oraz zebranie i zabezpieczenie dowodów**

  Członek ZBO dysponujący odpowiednią wiedzą techniczną powinien służyć wsparciem rodzicom/opiekunom prawnym, w kwestii zabezpieczenia odpowiednich materiałów na prywatnym komputerze ofiary (zrzuty ekranu, zapisy rozmów, wiadomości email oraz w komunikatorach) lub zabezpieczyć je na urządzeniu należącym do placówki. W przypadku trudności w zanalizowaniu materiału, o pomoc można zwrócić się również do zespołu Dyżurnet.pl, przyjmującego zgłoszenia na temat nielegalnych i szkodliwych treści w sieci.

- **Identyfikacja sprawcy/sprawców**

  Należy rozdzielić osobę sprawcy, który wytworzył materiały, od osoby, która zaprezentowała małoletniemu treści. O ile to możliwe, warto dotrzeć do tej drugiej osoby. Może zdarzyć się, że treści pokazują sobie nawzajem rówieśnicy. W takiej sytuacji należy poinformować rodziców wszystkich małoletnich zaangażowanych w zdarzenie.

2. Działania wobec uczestników zdarzenia

Rozmowa uczestnika zdarzenia z przedstawicielami Zespołu ds. Bezpieczeństwa Online (wychowawca/pedagog/psycholog) odpowiednia do charakteru zdarzenia, roli uczestnika (ofiara/świadek) oraz otoczenie wsparciem i opieką psychologiczno-pedagogiczną uczestników zdarzenia.

Małoletni powinien zostać otoczony szczególną opieką psychologiczno-pedagogiczną. Należy zapewnić mu komfort psychiczny, sprawdzić w jaki sposób dziecko dotarło do treści i dalej postępować zgodnie z ustaleniami.

W uzasadnionych przypadkach zaleca się skorzystać ze specjalistycznej formy opieki psychologicznej w porozumieniu z rodzicami/opiekunami prawnymi. Kontakt dziecka z materiałami nielegalnymi może mieć znaczący wpływ na jego psychikę.

Należy pamiętać o:

- **Powiadomieniu rodziców/opiekunów prawnych uczestników zdarzenia oraz informowaniu ich o podejmowanych działaniach oraz przedstawieniu propozycji wsparcia.**

- **Powiadomieniu policji/sądu rodzinnego w przypadku naruszenia prawa (patrz: Współpraca z policją).**

W przypadku ujawnienia sytuacji próby uwiedzenia małoletniego poniżej lat 15 przez osobę dorosłą lub rozpowszechniania materiałów pornograficznych z udziałem nieletniego, należy w porozumieniu z rodzicami/opiekunami prawnymi, NIEZWŁOCZNIE powiadomić policję.

3. Działania wobec instytucji/organizacji/służb pomocowych i współpracujących – policja, sąd rodzinny, służby społeczne

- **Obowiązki szkoły i placówek oświatowych w zakresie współpracy z policją i sądem rodzinnym**

  Rozpowszechnianie materiałów pornograficznych z udziałem osób nieletnich jest przestępstwem ściganym z urzędu[6], dlatego też dyrektor placówki jest zobowiązany do zgłoszenia incydentu na policję.

- **Współpraca ze służbami społecznymi i placówkami specjalistycznymi**

  W uzasadnionych przypadkach zaleca się skorzystać ze specjalistycznej formy opieki psychologicznej (w porozumieniu z rodzicami/opiekunami prawnymi) oferowanej przez poradnie specjalistyczne.

- **Współpraca z dostawcami usług internetowych i operatorami sieci telekomunikacyjnych**

  Współpraca z ww. podmiotami nie jest konieczna – konieczne ustalenia zostaną poczynione przez policję. Przypadkiem szczególnym będzie sytuacja rozpowszechnienia kompromitujących ofiarę materiałów w sieci (patrz procedura: Nielegalne i szkodliwe treści).

4. Dokumentacja i monitoring pointerwencyjny

Dokumentacja dotycząca incydentów związanych z kontaktem z nielegalnymi i szkodliwymi treściami w internecie powinna zawierać takie elementy jak: opis przebiegu zdarzenia, wskazanie osób uczestniczących w zdarzeniu, zabezpieczone dowody, zastosowane środki wychowawcze, plan monitoringu zdarzenia oraz notatki służbowe członków zespołu (Dokumentacja - Załącznik nr 6. Procedury interwencji zastosowaniej w placówce). Rekomenduje się prowadzenie dokumentacji z poszanowaniem prywatności uczestników oraz z zapewnieniem poufności przechowywanych i przetwarzanych danych.

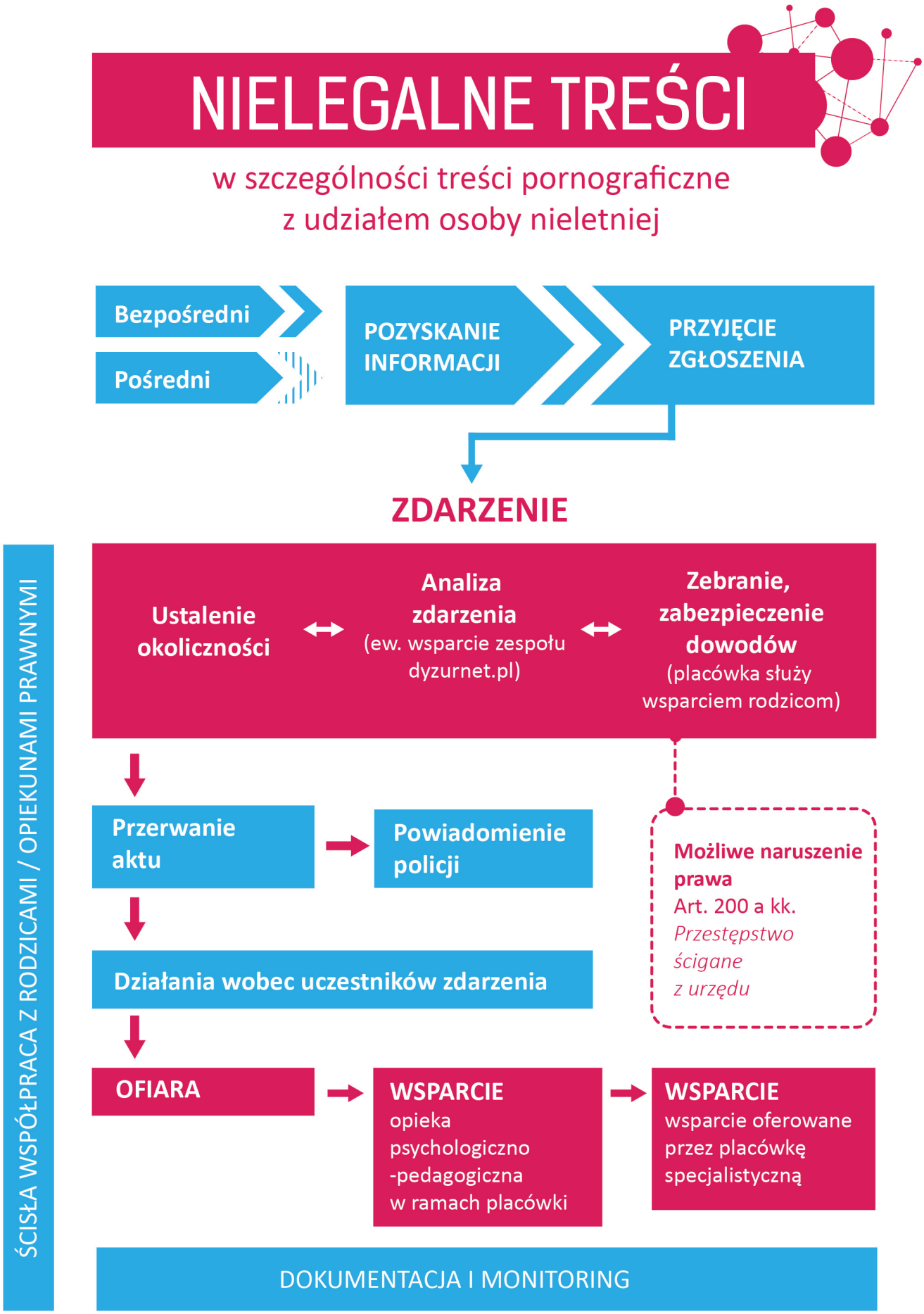
Monitoring powinien być prowadzony systematycznie po przerwaniu aktu i zastosowaniu środków naprawczych.

WAŻNE:

W przypadku kontaktu dziecka z innymi treściami szkodliwymi np. pornografią osób dorosłych, materiałami prezentującymi przemoc czy zachowania szkodliwe dla zdrowia, należy również dokładnie zbadać sposób, w jaki nastąpił kontakt dziecka z nimi. Poszukiwanie tego typu treści w sieci, lub podsuwanie ich dziecku przez innych, może być oznaką niepokojących incydentów ze świata rzeczywistego. Np. kontakty z osobami handlującymi narkotykami czy proces rekrutacji do sekty lub innej niebezpiecznej grupy.

6 Art. 202 kodeksu karnego.

Rys.14 Procedura reagowania wobec incydentów związanych z kontaktem z nielegalnymi i szkodliwymi treściami



Źródło: opracowanie Agnieszka Wrońska, Zuzanna Polak

Procedura interwencyjna: Seksting

1. Działania wobec zdarzenia

- **Pozyskanie informacji i przyjęcie zgłoszenia**

  W przypadku sekstingu osobą zgłaszającą problem może być rodzic/opiekun prawny lub zaniepokojony rówieśnik ofiary. Pracownik placówki może również sam dokonać przypadkowego wykrycia sprawy. Ze względu na możliwe konsekwencje incydentu (rozpowszechnienie w Internecie materiałów erotycznych prezentujących dziecko), ale biorąc pod uwagę delikatny charakter sprawy, należy działać sprawnie i z zachowaniem dyskrecji.

- **Ustalenie okoliczności zdarzenia, analiza zdarzenia oraz zebranie i zabezpieczenie dowodów**

  Zjawisko sekstingu może przyjmować różne formy i w zależności od nich, różny zasięg i następstwa. Procedura interwencyjna będzie wyglądała nieco inaczej w każdym przypadku.

  Przypadek 1.

  Wymiana materiałów o charakterze seksualnym następuje tylko w ramach związku między dwojgiem rówieśników. Materiały nie uległy rozprzestrzenieniu dalej.

  Przypadek 2.

  Materiały o charakterze seksualnym zostały rozesłane większej liczbie osób, jednak nie dochodzi do działań cyberprzemocowych na tym tle. Młodzież traktuje materiał jako formę wyrażenia siebie.

  Przypadek 3.

  Materiały zostały rozesłane większej liczbie osób w celu upokorzenia osoby na nich zaprezentowanej – lub zostają rozpowszechnione omyłkowo, jednak są zastosowane jako narzędzie cyberprzemocy.

- **Identyfikacja sprawcy/sprawców**

  W zależności formy incydentu sekstingu, jego zasięgu i następstw, identyfikacja sprawcy będzie miała charakter indywidualny. Identyfikacja sprawcy będzie miała większe znaczenie w przypadku sytuacji naruszenia prawa. W innych przypadkach, większy nacisk należy położyć na działania wychowawcze oraz opiekę psychologiczno-pedagogiczną wobec osoby uwiecznionej na materiałach.

2. Działania wobec uczestników zdarzenia

Rozmowa uczestników zdarzenia z przedstawicielami Zespołu ds. Bezpieczeństwa Online (wychowawca/pedagog/psycholog) odpowiednia do charakteru zdarzenia, roli uczestnika (ofiara/świadek) oraz otoczenie wsparciem i opieką psychologiczno-pedagogiczną uczestników zdarzenia.

Małoletni powinni zostać otoczeni szczególną i dyskretną opieką psychologiczno-pedagogiczną.

Przypadek 1.

Dalsze działania poza zapewnieniem wsparcia i opieki psychologiczno-pedagogicznej nie są konieczne, jednak istotne jest pouczenie uczestników zdarzenia, że dalsze rozpowszechnianie materiałów może być nielegalne i będzie miało inne konsekwencje.

Przypadek 2.

Niektóre z tego typu materiałów mogą zostać uznane za pornograficzne, w takim wypadku na dyrektorze placówki ciąży obowiązek zgłoszenia incydentu na policję. Rozpowszechnianie materiałów pornograficznych z udziałem nieletnich jest przestępstwem ściganym z urzędu[7], dlatego też dyrektor placówki jest zobowiązany do zgłoszenia incydentu na policję.

Wszelkie działania wobec osób uczestniczących w incydencie powinny być podejmowane w porozumieniu z ich rodzicami/opiekunami prawnymi.

Przypadek 3.

Niektóre z tego typu materiałów mogą zostać uznane za pornograficzne (patrz: Przypadek 2).

W sytuacji zaistnienia znamion cyberprzemocy, należy dodatkowo zastosować procedurę: Cyberprzemoc.

Należy pamiętać o:

- **Powiadomieniu rodziców/opiekunów prawnych uczestników zdarzenia oraz informowaniu ich o podejmowanych działaniach i przedstawieniu propozycji wsparcia.**

  Decyzję o ewentualnym poinformowaniu opiekunów powinna być podejmowana przez pedagoga/psychologa, biorącego pod uwagę dobro małoletnich, w zależności od charakteru sytuacji.

- **Powiadomieniu policji/sądu rodzinnego w przypadku naruszenia prawa (patrz: Współpraca z policją) .**

W przypadku ujawnienia sytuacji rozpowszechniania materiałów pornograficznych z udziałem osoby nieletniej należy w porozumieniu z rodzicami/opiekunami prawnymi NIEZWŁOCZNIE powiadomić policję.

3. Działania wobec instytucji/organizacji/służb pomocowych i współpracujących – policja, sąd rodzinny, służby społeczne

- **Obowiązki szkoły i placówek oświatowych w zakresie współpracy z policją i sądem rodzinnym**

Rozpowszechnianie materiałów prezentujących seksualne wykorzystywanie nieletnich jest przestępstwem ściganym z urzędu[8], toteż dyrektor placówki jest zobowiązany do zgłoszenia incydentu na policję.

- **Współpraca ze służbami społecznymi i placówkami specjalistycznymi**

- **Współpraca z dostawcami usług internetowych i operatorami sieci telekomunikacyjnych**

Współpraca z ww. podmiotami nie jest konieczna - niezbędne ustalenia zostaną poczynione przez policję. Przypadkiem szczególnym będzie sytuacja rozpowszechnienia kompromitujących ofiarę materiałów w sieci (patrz: Nielegalne i szkodliwe treści.)

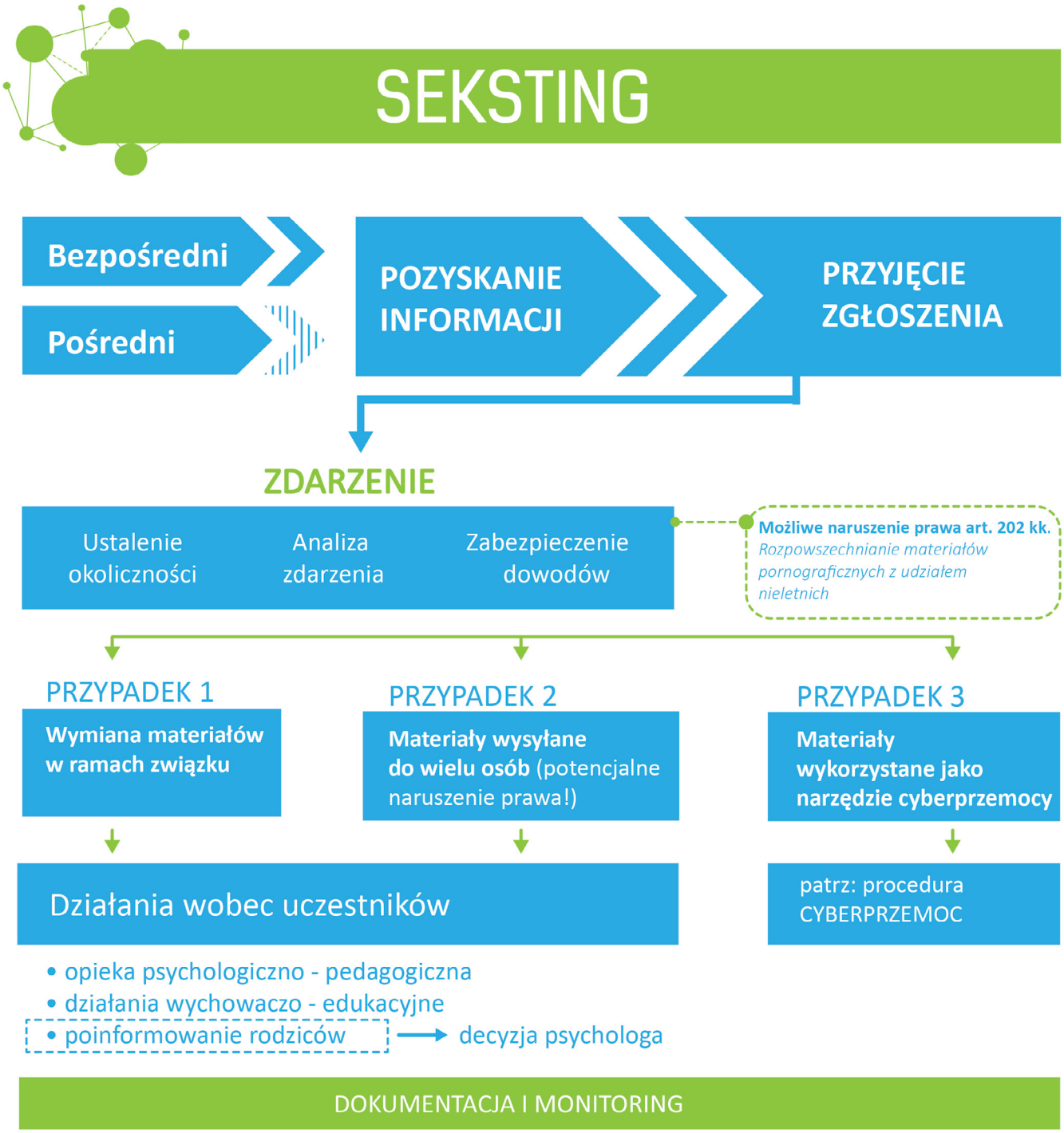
7 Art. 202 kodeksu karnego.
8 ibidem

4. Dokumentacja i monitoring pointerwencyjny

Dokumentacja dotycząca sekstingu powinna zawierać takie elementy jak: opis przebiegu zdarzenia, osoby uczestniczące w zdarzeniu, zabezpieczone dowody, zastosowane środki wychowawcze i dyscyplinarne, plan monitoringu zdarzenia oraz notatki służbowe członków zespołu (Załącznik nr 6. Dokumentacja procedury interwencyjnej zastosowanej w placówce). Rekomenduje się prowadzenie dokumentacji z poszanowaniem prywatności uczestników oraz z zapewnieniem poufności przechowywanych i przetwarzanych danych.

Monitoring powinien być prowadzony systematycznie po przerwaniu aktu i zastosowaniu środków naprawczych.

Rys.15 Procedura reagowania wobec sekstingu



Źródło: opracowanie Agnieszka Wrońska, Zuzanna Polak

Procedura interwencyjna: Nadmierne korzystanie z internetu/nowoczesnych technologii

1. Działania wobec zdarzenia

- **Pozyskanie informacji i przyjęcie zgłoszenia**

  W przypadku nadmiernego korzystania dziecka z Internetu/gier osobą zgłaszającą problem może być rodzic/opiekun prawny, opiekun pracowni informatycznej w placówce lub zaniepokojony rówieśnik ofiary.

- **Ustalenie okoliczności zdarzenia, analiza zdarzenia oraz zebranie i zabezpieczenie dowodów**

  Należy przede wszystkim zbadać jakie obszary aktywności dziecka zostały naruszone ze względu na nadmierne korzystanie z nowoczesnych technologii i czy sytuacja wymaga zaangażowania placówki specjalistycznej. W początkowych etapach uzależnienia wystarczające może być wsparcie rodzinne oraz psychologa/pedagoga szkolnego.

- **Identyfikacja sprawcy/sprawców**

  Nie dotyczy.

2. Działania wobec uczestników zdarzenia

Rozmowa uczestnika zdarzenia z przedstawicielami Zespołu ds. Bezpieczeństwa Online (wychowawca/pedagog/psycholog) odpowiednia do charakteru zdarzenia, roli uczestnika (ofiara/świadek) oraz otoczenie wsparciem i opieką psychologiczno-pedagogiczną uczestników zdarzenia.

Małoletni powinien zostać otoczony szczególną opieką psychologiczno-pedagogiczną. Należy zapewnić mu komfort psychiczny, upewnić się jak poważna jest sytuacja. Zdarza się, że dziecko angażuje się w nadmierne korzystanie z Internetu/gier/nowoczesnych technologii z powodów konfliktów rodzinnych lub rówieśniczych w świecie rzeczywistym.

Należy pamiętać o:

- **Powiadomieniu rodziców/opiekunów prawnych uczestników zdarzenia oraz informowaniu ich o podejmowanych działaniach oraz przedstawieniu propozycji wsparcia.**

  Wszelkie działania oraz zastosowanie metod terapeutycznych powinny być uzgadnianie z rodzicami/opiekunami prawnymi.

- **Powiadomieniu policji/sądu rodzinnego w przypadku naruszenia prawa (patrz: Współpraca z policją)**

  Nie ma konieczności zawiadamiania policji, ale w przypadku braku współpracy ze strony rodziców należy rozważyć zgłoszenie sprawy do sądu rodzinnego. Szczególnie w sytuacji gdy placówce oświatowej znane są inne przejawy demoralizacji.

3. Działania wobec instytucji/organizacji/służb pomocowych i współpracujących – policja, sąd rodzinny, służby społeczne

- **Obowiązki szkoły i placówek oświatowych w zakresie współpracy z policją i sądem rodzinnym**
- **Współpraca ze służbami społecznymi i placówkami specjalistycznymi**

  W uzasadnionych przypadkach konieczne może być skierowanie małoletniego do placówki specjalistycznej oferującej program terapeutyczny z zakresu przeciwdziałania uzależnieniom.
- **Współpraca z dostawcami usług internetowych i operatorami sieci telekomunikacyjnych**

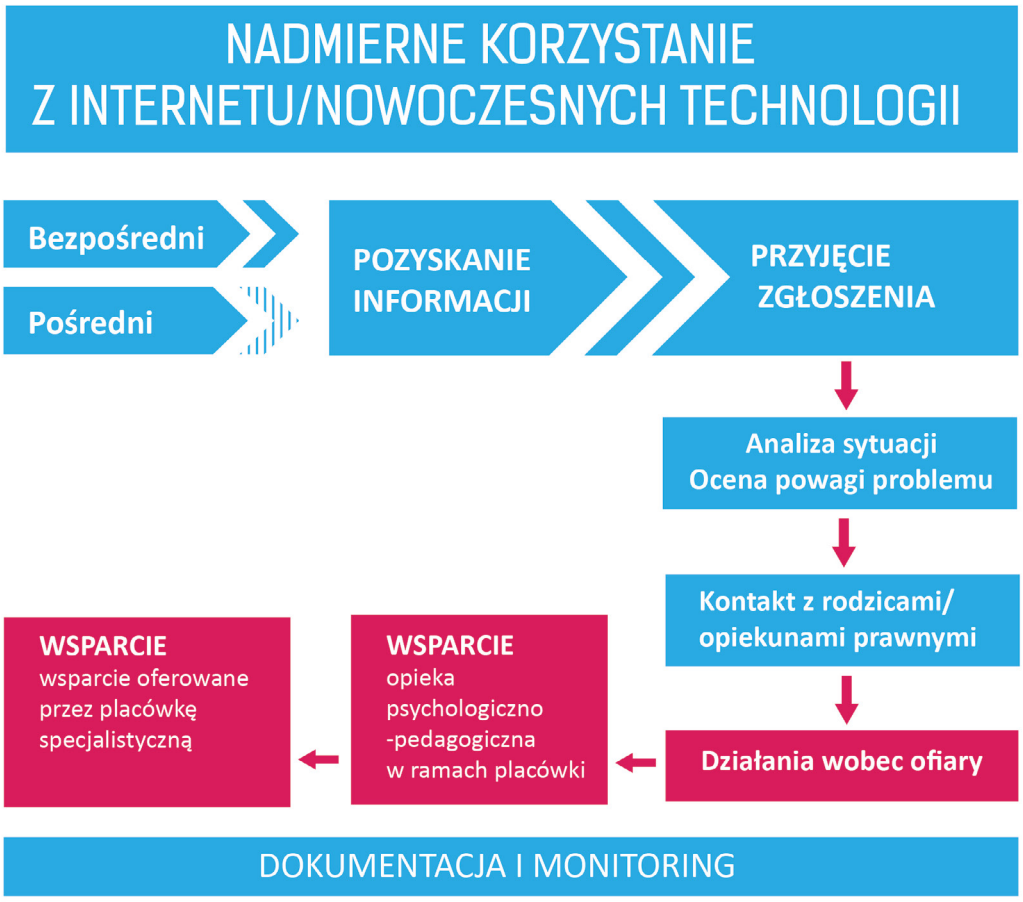
  Nie dotyczy

4. Dokumentacja i monitoring pointerwencyjny

Dokumentacja dotycząca incydentów związanych z niebezpiecznymi kontaktami online powinna zawierać takie elementy jak: opis przebiegu zdarzenia, wykaz osób uczestniczących w zdarzeniu, zabezpieczone dowody, zastosowane środki wychowawcze i dyscyplinarne, plan monitoringu zdarzenia oraz notatki służbowe członków zespołu (Załącznik nr 6. Dokumentacja procedury interwencyjnej zastosowanej w placówce). Rekomenduje się prowadzenie dokumentacji z poszanowaniem prywatności uczestników oraz z zapewnieniem poufności przechowywanych i przetwarzanych danych.

Monitoring powinien być prowadzony systematycznie po przerwaniu aktu i zastosowaniu środków naprawczych.

Rys.16 Procedura reagowania wobec nadmiernego korzystania z internetu



Źródło: opracowanie Agnieszka Wrońska, Zuzanna Polak

Dział III. Technologiczne zagrożenia w cyberprzestrzeni

Od czasu pierwszego incydentu związanego z rozpowszechnieniem się w roku 1988 wirusa Morris Worm przy pomocy sieci Internet, stało się jasne, że środowisko sieci komputerowych będzie obszarem zagrożeń dla bezpieczeństwa danych, systemów oraz użytkowników korzystających z nowoczesnych technologii komunikacyjnych.

Zadając sobie pytanie, dlaczego i w jakim stopniu należy poświęcać czas oraz budżet na kwestie związane z bezpieczeństwem teleinformatycznym, **należy na bieżąco uświadamiać sobie, jakim zagrożeniom podlega każda infrastruktura komputerowa** – szczególnie, jeśli ma kontakt z internetem.

Katalog typów zagrożeń internetowych jest dość szeroki i stale się powiększa. Zagrożenia znane od lat, takie jak wirusy komputerowe, są coraz bardziej zaawansowane technicznie i trudniejsze do wykrycia a dodatkowo, wraz z rozwojem technologii wciąż powstają nowe formy zagrożeń (np. ataki na płatności mobilne). Dlatego niezwykle istotne jest stałe podnoszenie wiedzy na temat zagrożeń w cyberprzestrzeni i metod im przeciwdziałania. W związku z tym, **każda instytucja powinna zapewnić użytkownikom cykliczne szkolenia na temat zagrożeń bezpieczeństwa i dobrych praktyk ochrony informacji.**

Każdy system oparty na przetwarzaniu komputerowym, niezależnie od tego, czy jest to komputer PC lub laptop z systemem Windows czy Linux, serwer sieciowy, router, tablet, smartfon, konsola do gier a nawet tzw. SmartTV, jest i będzie podatny nie tylko na awarie, ale także na wiele zagrożeń i ataków. Przynoszą one szereg przykrych konsekwencji jak np.: utrata wizerunku z powodu wycieku danych z instytucji, utrata środków finansowych przy płatnościach przez internet, strata efektów pracy poprzez utratę gromadzonych danych. Niekiedy może to doprowadzić do zainteresowania instytucją ze strony organów ścigania z powodu nielegalnych działań prowadzonych przez jej legalnych użytkowników albo intruzów „korzystających" z sieci tej instytucji.

Kolejne, nowe podatności wykrywane są każdego dnia. Tak więc, jeśli system komputerowy nie jest aktualizowany (aktualizacji muszą podlegać systemy operacyjne oraz aplikacje, nawet przeglądarki internetowe i programy do edycji tekstu) – jego odporność na infekcję szkodliwym oprogramowaniem maleje każdego dnia. **Bardzo istotną kwestią jest więc systematyczne aktualizowanie oprogramowania.**

W literaturze przedmiotu coraz częściej mówi się o **higienie bezpieczeństwa IT.** Na wzór przestrzegania podstawowych zasad higieny w życiu codziennym, termin ten określa stosowanie się do określonych zaleceń bezpieczeństwa w cyberprzestrzeni, przekazywanych użytkownikom sieci i systemów komputerowych za pomocą regulaminów, szkoleń przedstawiających najlepsze praktyki czy kampanii uświadamiających.

Na potrzeby opracowania przyjęto następującą definicję standardu dla części technicznej:

Standard wdrożenia oraz utrzymania infrastruktury i usług teleinformatycznych dla zapewnienia odpowiedniego poziomu bezpieczeństwa IT w placówce oświatowej.

Co trzeba wiedzieć o Internecie aby czuć się bezpiecznie?

Internet jest przestrzenią, w której różne podmioty oferują bogaty katalog usług. Ogólnie można podzielić te podmioty na dostawców dostępu do Internetu (obszar ten jest regulowany ustawą prawo telekomunikacyjne), dostawców treści (obszar będący domeną ustawy o świadczeniu usług drogą elektroniczną). Wyróżnia się także dostawców hostingu oferujących przestrzeń przetwarzania dla serwerów i aplikacji swoich klientów (także w postaci tzw. usług chmurowych). W wielu przypadkach te same podmioty mogą być jednocześnie dostawcami różnego typu usług.

Dostawcy usług

1. Dostawca Internetu

Dostęp do Internetu jest usługą, która jest oferowana przez rozmaite podmioty takie jak: operatorzy telekomunikacyjni, wyspecjalizowani dostawcy Internetu (ISP – Internet Service Provider), operatorzy sieci kablowych, lokalni dostawcy bezprzewodowego Internetu i inni. Jest istotne aby mieć świadomość, iż wszystkie te podmioty muszą zgłosić działalność telekomunikacyjną w Polsce i podlegają rygorom Prawa Telekomunikacyjnego (także w obszarze stosowania zasad bezpieczeństwa). Zawierając umowę na dostawę Internetu, **należy sprawdzić, czy dany podmiot znajduje się w rejestrze Urzędu Komunikacji Elektronicznej**[9], gdyż znane są przypadki, iż dostęp do Internetu jest oferowany przez kogoś, kto nie jest do tego uprawniony i nie zapewnia odpowiednich parametrów jakości czy bezpieczeństwa.

2. Dostawca treści

Do tej grupy można zaliczyć serwisy społecznościowe, sklepy internetowe, portale, serwisy chmurowe oraz inne formy usług udostępniane użytkownikom za pośrednictwem Internetu. Dostawcy treści mogą być zlokalizowani gdziekolwiek na świecie i podlegają prawu lokalnemu, w miejscu gdzie usługodawca zarejestrował działalność. Część przedsiębiorców rejestruje działalność w Polsce, inne firmy mają tylko przedstawicielstwa handlowe w naszym kraju, a jeszcze inne w ogóle nie mają związku z geograficzną lokalizacją w danym kraju. Dodatkowo infrastruktura techniczna tych usługodawców może być rozproszona po całym świecie. Takie aspekty mają znaczenie w przypadku, kiedy w danym serwisie zajdzie jakieś zdarzenie naruszające bezpieczeństwo. **Korzystając z usług dostawców treści należy dokładne przestudiować regulaminy korzystania z usługi a także warunków umownych danej usługi**. W Polsce świadczenie usług wykorzystujących komunikację internetową podlega ustawie o świadczeniu usług drogą elektroniczną.[10]

9 Rejestr przedsiębiorców telekomunikacyjnych: http://www.uke.gov.pl/marta/?p=2
10 Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

3. Dostawcy kolokacji, hostingu lub rozwiązań chmurowych

Wśród dostawców wykorzystujących Internet jako medium dostępowe można wyróżnić także podmioty oferujące usługi polegające na powierzeniu lub posadowieniu zasobów informatycznych klienta w infrastrukturze dostawcy. Możemy tu mówić o usłudze kolokacji (gdzie sprzęt klienta (np. serwer z aplikacją) pracuje w wyspecjalizowanej serwerowni dostawcy), usłudze hostingu (kiedy to dostawca wydzierżawia wirtualne przestrzenie komputerowe, na których klient instaluje/tworzy własne aplikacje (np. strony internetowe), czy też coraz bardziej popularne usługi chmurowe (klient ma do dyspozycji, przez Internet, praktycznie dowolne usługi przetwarzania (np. archiwizacja danych, aplikacje biurowe itp.) zrealizowane w rozproszonej geograficznie infrastrukturze usługodawcy. W przypadku korzystania z tego typu usług należy zadbać o uzyskanie takich warunków umownych z usługodawcą, które będą zapewniać odpowiedni poziom usług, a także gwarancję bezpieczeństwa (samej usługi oraz powierzanych danych).

Jak funkcjonuje Internet?

Przywołując powyższy podział na dostawców internetu (operatorów) oraz dostawców treści (serwisy internetowe) można w uproszczeniu przedstawić infrastrukturę internetową jako połączone ze sobą sieci różnych operatorów na całym świecie, które składają się z linii (kablowych lub bezprzewodowych), urządzeń przekazujących pakiety (routery, przełączniki), serwerów (np. serwery nazw, serwery pocztowe) i innych elementów, takich jak systemy zarządzania czy systemy bezpieczeństwa.

Z kolei w warstwie usług internetowych dotyczących treści, (np. e-sklepy, portale aukcyjne, serwisy bankowości elektronicznej), infrastruktura dostawców tych usług składa się (w pewnym uproszczeniu) z serwerów z odpowiednimi aplikacjami, które są podłączone do sieci operatorów Internetu i dzięki temu są dostępne dla użytkowników.

Każdy komputer (ale także innego typu urządzenia) w Internecie ma swój adres, zwany adresem IP a także (zwykle) skojarzoną z tym adresem nazwę domenową. W szczególności jeśli jest to serwer jakiejś usługi. Użytkownicy, nawigując w sieci, posługują się właśnie nazwami domenowymi (lub ich fragmentami – wyszukując je w wyszukiwarkach internetowych).

Istotnym więc elementem infrastruktury Internetu jest system rozwiązywania nazw domenowych (DNS – *Domain Name System*), który (mówiąc w uproszczeniu), kojarzy adresy IP z właściwymi nazwami domenowymi. Istotne jest to, iż każda strona ma nazwę, która jest zarejestrowana i jest znana serwerom DNS. W Polsce rejestr domeny krajowej „.pl" jest prowadzony w NASK.[11]

Odbiorców usług dostępu do Internetu, czyli klientów można z kolei podzielić na trzy kategorie:

I. Instytucje podłączające swoje sieci lokalne do sieci operatorów

II. Klienci indywidualni podłączający swoje routery domowe do sieci operatorów

III. Klienci indywidualni korzystający z mobilnego Internetu (w telefonach, smartfonach, tabletach)

11 www.dns.pl

Niezależnie od tego podziału, należy zwrócić uwagę, że **każdy element sieci czy urządzenie komputerowe powinno mieć swojego administratora lub opiekuna.**

Nie można zatem pozwolić, by infrastruktura klienta internetu była pozbawiona opieki technicznej.[12]

Wszelkie systemy komputerowe, te z których zbudowany jest Internet oraz urządzenia i sieci klientów, nie mogą sprawnie działać bez zapewnienia opieki technicznej w postaci osób administrujących danymi systemami. Administratorzy dokonują instalacji systemów, ich konfiguracji, zajmują się wprowadzaniem uaktualnień i nowych wersji oprogramowania, przeglądają dzienniki zdarzeń i wykonują szereg innych prac. Bez stałego i uporządkowanego procesu utrzymania i zarządzania systemy komputerowe po pewnym czasie zaczęłyby pracować wadliwie, przestałyby zapewniać jakikolwiek poziom bezpieczeństwa oraz nie nadążałyby za wymaganiami ich użytkowników.

Jeśli w danej instytucji nie ma odpowiednich zasobów kadrowych, taką opiekę należy powierzyć osobom lub firmom zewnętrznym.

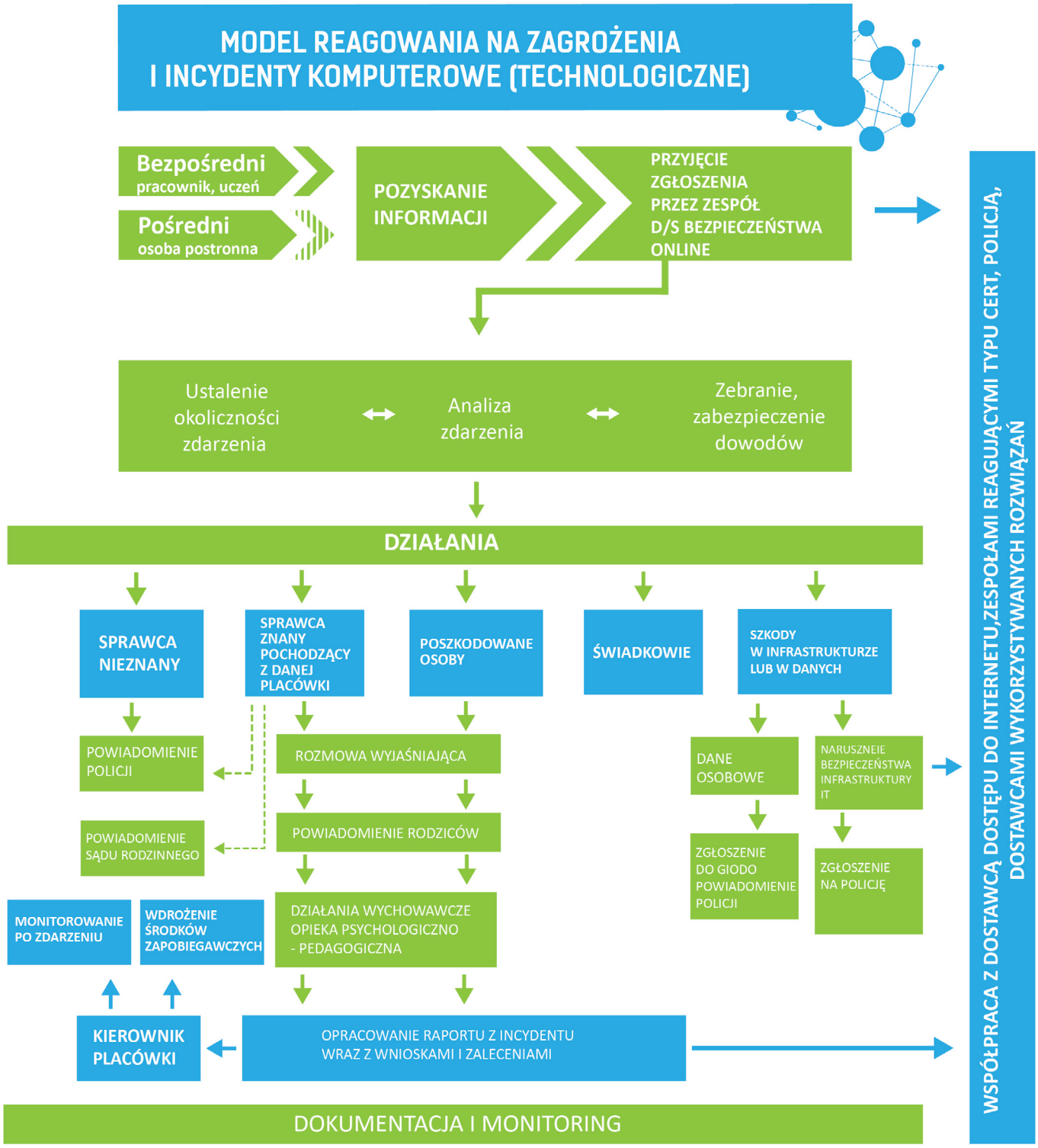
Katalog zagrożeń systematycznie się rozszerza, tak więc kierownictwo placówki powinno cyklicznie (minimum raz do roku) dokonywać przeglądu istotnych zagrożeń w oparciu o raporty wyspecjalizowanych instytucji (np. raporty roczne CERT.GOV.PL http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi) i ich wpływu na bezpieczeństwo infrastruktury oraz użytkowników.

Model reagowania, środki zaradcze i dobre praktyki

W przypadku zagrożeń technicznych, podobnie jak w przypadku społecznych, w chwili wystąpienia incydentów należy podjąć niezwłocznie konkretne działania. Brak szybkiej i skutecznej reakcji może skutkować (i najczęściej skutkuje) dużymi stratami. Zmusza do ponoszenia sporych nakładów finansowych i wysiłku organizacyjnego w celu doprowadzenia do naprawy sytuacji. Należy pamiętać, iż w przypadku wielu tego typu incydentów musimy podejmować bardzo konkretne działania przewidziane przez obowiązujące przepisy. Prezentowany tu model opisuje sposoby postepowania między innymi w takich przypadkach. Sposoby te mogą różnić się jeśli chodzi o konkretną sekwencję kroków. **Podstawowe reguły obowiązują jednak we wszystkich przypadkach: precyzyjne ustalenie co się zdarzyło, niezwłoczna interwencja, konkretne działania oraz podsumowanie całego procesu i wyciągnięcie odpowiednich wniosków.** Tak prowadzona procedura interwencyjna pozwala unikać w przyszłości części zagrożeń dzięki doświadczeniu i wnioskom wyciągniętym z zaistniałych incydentów. Podsumowanie powinno zawierać konkretne rekomendacje na przyszłość, w tym zalecane działania podwyższające poziom bezpieczeństwa i świadomości użytkowników dotyczące tej tematyki. Można więc stwierdzić, że w przedstawionym modelu reagowania zaproponowane zostały mechanizmy wspomagające działania profilaktyczne.

12 Infrastruktura dostawców ma swoich administratorów, zarządzających jej elementami od strony technicznej. Klient powinien mieć kontakt techniczny w postaci telefonu, adresu e-mail do helpdesku dostawcy

Rys.17 Model reagowania na techniczne zagrożenia i incydenty komputerowe



Źródło: opracowanie Agnieszka Wrońska, Zuzanna Polak, Krzysztof Silicki

W związku z istniejąca gamą zagrożeń dla bezpieczeństwa systemów komputerowych, użytkowników i ich danych, środki zaradcze powinny być stosowane w warstwie organizacyjnej, jak i technicznej.

Środki organizacyjne

- **Edukacja: Świadomość podstawowych pojęć związanych z bezpieczeństwem**

  Budowanie świadomości powinno być procesem ciągłym. Szczególnie w placówkach edukacyjnych należy zastosować wszystkie dostępne metody takie jak:

  - włączenie tematyki bezpieczeństwa do programu przedmiotów nie tylko związanych z informatyką lecz wszędzie gdzie propagowane jest korzystanie z Internetu (np. do zdobywania informacji przez uczniów),
  - pogadanki tematyczne realizowane we własnym zakresie,
  - współpraca z ekspertami (zapraszanie do wygłoszenia pogadanek, referatów),
  - wywieszanie plakatów tematycznych,
  - uczestnictwo w kampaniach edukacyjnych (np. bezpiecznymiesiac.pl),
  - współpraca z rodzicami.

  Każdy użytkownik powinien mieć świadomość podstawowych pojęć związanych z bezpieczeństwem takich jak:

  - **Szyfrowanie**

  Zapewnienie poufności przesyłanych (lub składowanych) danych wrażliwych (takich jak loginy, hasła, numery kart płatniczych, dane osobowe) wymaga stosowania mechanizmów takich jak szyfrowanie, które przetwarzają chronione dane na zakodowany ciąg znaków, niemożliwy do zinterpretowania przez potencjalnych intruzów (osoby nie upoważnione do odczytywania naszych danych). Współczesne mechanizmy szyfrowania pozwalają również na zapewnienie innych cech bezpieczeństwa, takich jak integralność danych (ochrona przed nieuprawnioną zmianą komunikatów lub składowanych danych), niezaprzeczalność (przykładowo: pewność, że serwer, z którym nawiązujemy szyfrowane połączenie należy do danej instytucji). Popularną implementacją szyfrowania, jest w codziennej praktyce tzw. „zielona kłódeczka" w pasku adresowym przeglądarki internetowej, która świadczy o tym, że połączenie z serwerem jest szyfrowane.

  - **Aktualizacje**

  Aktualizacjami nazywamy wszelkie czynności ręczne lub zadania realizowane automatycznie prowadzące do wprowadzania (zazwyczaj poprzez Internet) nowych wersji oprogramowania (systemu operacyjnego bądź aplikacji), które usuwają zauważone przez producenta błędy w oprogramowaniu lub podatności na zagrożenia. Wszyscy renomowani producenci oprogramowania zapewniają łaty lub nowe wersje programów, tak często jak jest to niezbędne dla ich prawidłowego działania oraz osiągnięcia odpowiedniego poziomu bezpieczeństwa. Szczególnym przypadkiem są nowe wersje programów antywirusowych, antyspamowych czy wykrywających szkodliwe oprogramowanie, które zapewniają uaktualnianie bazy znanych wirusów czy wzorców spamu.

Użytkownik powinien dbać, aby opcje automatycznych (lub półautomatycznych) mechanizmów aktualizacji były zawsze włączone. Dotyczy to systemu operacyjnego (np. Windows, Android, IOS), wykorzystywanych aplikacji (przeglądarki internetowe, programy do czytania lub edycji plików – np. Acrobat, MS Office) oraz wspomnianych programów podwyższających bezpieczeństwo (np. antywirusowych).

- **Kopie zapasowe**

Kopie zapasowe, podobnie jak aktualizacje , powinny być wykonywane cyklicznie. Można wykonywać duplikaty całej zawartości dysku, bądź tylko określonych zasobów (partycji dysku, katalogów plików, danych kontaktowych itp.) Istotne jest to aby dostosować częstotliwość wykonywania kopii do częstości zmian naszych danych oraz poziomu ich istotności. Wersje zapasowe koniecznie należy przechowywać w innym miejscu niż znajdują się dane oryginalne. Oznacza to, że kopia danych z dysku komputera nie znajduje się na tym samym dysku a na np. nośniku zewnętrznym (pamięć USB, dysk zewnętrzny) bądź w sieci (na serwerze w sieci lokalnej lub serwerach w sieci Internet).

Możliwość odtworzenia danych z kopii zapasowej po wystąpieniu awarii lub zawirusowania komputera (np. wirusem typu ransomware) jest często jedyną szansą na nieutracenie ważnych informacji.

Współczesne systemy operacyjne posiadają specjalne funkcje ułatwiające tworzenie kopii zapasowych i ich odtwarzanie. Użytkownicy zaś powinni nie tylko tworzyć regularnie duplikaty, ale także sprawdzać prawidłowość ich wykonania (poprzez testowe odtworzenie).

- **Systemy bezpiecznego uwierzytelniania**

Bezpieczne uwierzytelnienie polega na zastosowaniu takich mechanizmów przy podawaniu loginu i hasła aby jak najtrudniejsze było ich przechwycenie i nieuprawnione użycie przez inne osoby lub szkodliwe oprogramowanie. Klasyczne hasła zwane są hasłami statycznymi. Ich siła opiera się na doborze odpowiednio długiego ciągu znaków, różnego typu (litery, cyfry, znaki specjalne). Jednak takie hasło, nawet jeśli jest trudne do odgadnięcia, może zostać podsłuchane. Bezpieczniejszym rozwiązaniem, jest stosowanie systemów haseł jednorazowych (stosowanie generatorów haseł jednokrotnych – tzw. tokenów bądź wprowadzanie kodów otrzymanych SMSem w trakcie logowania). Wtedy zabezpieczenie jest dwuelementowe: pierwszy element to zazwyczaj hasło statyczne (np. PIN), a drugi jest dynamicznie generowany na potrzeby danego procesu logowania (np. na stronę bankowości elektronicznej). Przechwycenie jednorazowego hasła dynamicznego nie przyniesie intruzowi korzyści, ponieważ takie hasło nie może być powtórnie użyte. Obecnie serwisy internetowe, dla których bezpieczeństwo użytkowników jest szczególnie istotne, np. systemy bankowości elektronicznej, Google, Facebook i wiele innych dają możliwość stosowania dwuetapowego logowania z użyciem hasła jednorazowego np. przesyłanego SMSem.

- **Bezpieczeństwo w chmurze**

Usługami chmurowymi nazywamy wszelkie usługi internetowe, które polegają na przechowywaniu bądź przetwarzaniu danych użytkownika w rozproszonym środowisku serwerowym usługodawcy (np. Amazon, Microsoft, Apple, usługodawcy krajowi). Mogą to być usługi wykonywania i przechowywania kopii zapasowych w chmurze (np. iCloud, AWS) przechowywanie plików, czy korzystanie z rozmaitych aplikacji bez potrzeby ich lokalnego instalowania (np. edytory tekstów). Przy korzystanie z usług chmurowych należy dokładnie zapoznać się regulaminem usługi aby poznać ofertę, także od strony bezpieczeństwa. Zaleca się korzystać z takich usług przetwarzania w chmurze, które zapewniają szyfrowanie danych składowanych w internecie, szyfrowanie komunikacji pomiędzy użytkownikiem a usługą, kasowanie danych z chmury po zakończeniu korzystania z usługi a także gwarantują nie przekazywanie naszych danych innym podmiotom. W szczególnych przypadkach korzystanie z usług chmurowych może być obwarowane dodatkowymi obostrzeniami, np. jeśli dane określonego typu nie powinny być przechowywane poza granicami kraju – korzystanie z usług chmurowych może stać się niemożliwe, gdyż pojęcie chmury zwykle nie ma odniesienia do granic geograficznych.

ISTNIENIE DOKUMENTÓW FORMALNYCH REGULUJĄCYCH KWESTIE BEZPIECZEŃSTWA INFORMACJI

Zaleca się bezwzględnie aby w placówce istniał podstawowy zestaw dokumentów formalnych, które odnoszą się do tematyki bezpieczeństwa IT.

- Polityka bezpieczeństwa
- Regulamin korzystania z usług infrastruktury komputerowej i sieciowej

Informacje na temat dokumentów regulujących kwestię bezpieczeństwa informacji znajdują się w Załączniku nr 4 i 5.

Środki techniczne

Wymagane jest aby na każdym poziomie zgodności ze standardami bezpieczeństwa w szkole były stosowane odpowiednie środki techniczne dla zapewnienia właściwej ochrony:

- Odpowiednia architektura IT (separacja segmentów przeznaczonych do różnych zastosowań).
- Stosowanie systemów firewall (FW), antywirusowych (AV).
- Stosowanie filtrów treści szkodliwych

  (więcej informacji znajduje się w opisie trójpoziomowego modelu bezpieczeństwa infrastruktury IT).
- Wykonywanie kopii zapasowych.
- Przeprowadzanie automatycznych aktualizacji.

(Patrz: fragment dotyczący podstawowych pojęć związanych z bezpieczeństwem: Model reagowania, środki zaradcze i dobre praktyki)

Zakończenie

Niniejszy standard wprowadza zasady funkcjonowania placówek oświatowych w kontekście zagadnień związanych z użytkowaniem sieci. Możliwość zastosowania przez użytkowników i wdrożenie w placówkach oświatowych standardu pozwala uniknąć wielu zagrożeń cyberprzestrzeni, daje również szansę na odpowiednie przygotowanie pracowników placówek oświatowych do pracy z uczniami i rodzinami w przypadku zaistnienia zdarzenia związanego z niewłaściwym użytkowaniem internetu i urządzeń multimedialnych. Przygotowaniu dokumentu przyświecało przekonanie, iż jego wprowadzenie i stosowanie pozwoli placówkom lepiej chronić najmłodszych użytkowników sieci, którzy są grupą szczególnie narażoną na cyberproblemy. Autorzy standardu uznali, iż zasadnicze znaczenie dla bezpiecznego korzystania z osiągnieć techniki ma poziom wiedzy i umiejętności użytkowników.

W dokumencie zalecano, by zagadnienia związane z korzystaniem z komputera i urządzeń mobilnych postrzegać szeroko, dbając o podnoszenie świadomości wszystkich członków społeczności szkolnej: uczniów, rodziców, nauczycieli. Edukacja i postawienie szczególnego akcentu na działania profilaktyczne zapewne w znacznym stopniu pozwoli na uniknięcie problemów, choć całkowicie ich nie wykluczy. Dlatego tak ważne, by w przypadku ich wystąpienia, pracownicy placówek oświatowych potrafili na nie odpowiednio reagować.

Przedstawione w dokumencie modele interwencji ułatwiają przeprowadzenie odpowiednich działań wobec ofiary i sprawcy. Wskazują także w jaki sposób dokumentować zdarzenia i zabezpieczać dowody. Wprowadzenie standardu nie wymaga szerszych nakładów finansowych. Rekomenduje się odpowiednie inwestycje w infrastrukturę techniczną, choć i w tym przypadku są one związane z podstawową działalnością placówek oświatowych. Zapewnienie korzyści bezpośrednim i pośrednim użytkownikom standardu wymaga natomiast od realizatorów i organizatorów stałej i systematycznej pracy oraz podnoszenia kwalifikacji. Niezbędne jest wyciąganie wniosków z doświadczeń praktycznych i dokonywanie odpowiednich modyfikacji w funkcjonowaniu placówki.

Przyjęcie dokumentu pozwala odpowiednio przygotować się dyrektorom, wychowawcom, nauczycielom na wyzwania jakie przed nimi stoją w związku z coraz szerszym wykorzystaniem internetu i urządzeń multimedialnych.

Załącznik nr 1. Słownik najważniejszych zagrożeń

BOTnety

Jeśli dojdzie do infekcji urządzenia, skutki mogą być różnorakie. Jednym z najmniej dostrzegalnych jest szkodliwe oprogramowanie, które przejmuje sterowanie naszym komputerem i oddaje je w ręce intruzów (zwykle grup przestępczych). Mówimy wtedy, że nasz komputer stał się „zombie" i jest częścią tzw. sieci BOTnet – tysięcy komputerów, które są sterowane z jednego serwera (tzw. C&C). Użytkownik może odczuć spowolnienie pracy swego komputera w czasie, kiedy bez jego wiedzy jego sprzęt, sterowany przez cyberprzestępców, może dokonywać wielu nielegalnych operacji (np. rozsyłać spam albo atakować inne komputery). Oprócz tego wszystkie dane użytkownika są w niebezpieczeństwie (listy kontaktów, dokumenty itp.) i są wykradane bądź niszczone.

Cyberprzemoc

Cyberprzemoc to rodzaj przemocy, której akty dokonywane są przy użyciu nowych technologii. Do kategorii takich zjawisk zaliczamy: wyzywanie, straszenie, prześladowanie, oczernianie, poniżanie kogoś w internecie lub przy użyciu urządzeń mobilnych. W praktyce polega ona m.in. na przerabianiu i publikowaniu ośmieszających materiałów, zdjęć, filmów, upublicznianiu sekretów ofiar, wulgarnym, i złośliwym komentowaniu wpisów i zdjęć. Może to być także podszywanie się pod inną osobę za pomocą przechwyconego profilu, poczty, jak również celowe ignorowanie aktywności ofiary w sieci. Akty cyberprzemocy należy rozpatrywać zarówno w kontekście ofiary (osoby poszkodowanej), jak i sprawcy (osoby lub grupy osób) oraz świadka zdarzenia. Cechą charakterystyczną cybeprzemocy jest wyższą, niż w tradycyjnej formie przemocy, anonimowość. Pozwala ona sprawcom na odczuwanie złudnego wrażenia bezkarności. To z kolei może zachęcać do podejmowania działań przemocowych. Cyberprzemoc charakteryzuje się ciągłością trwania (zwykle nie kończy się na jednorazowym zdarzeniu) oraz szybkością rozpowszechniania się informacji/materiałów skierowanych przeciwko jej ofierze oraz ich dostępność.

Najczęściej w przypadkach cyberprzemocy dochodzi do naruszeń: art. 190 kk - groźba karalna, art. 190a kk – uporczywe nękanie (stalking), podszywanie się, , 191 kk - zmuszenie do określonego działania, 191a kk - naruszenie intymności seksualnej, utrwalenie wizerunku nagiej osoby bez jej zgody, 212 kk - zniesławienie, 216 kk - zniewaga, 267 kk - bezprawne uzyskanie informacji, 268 kk - utrudnianie zapoznania się z informacją, 268a kk - niszczenie danych informatycznych, 269 kk - uszkodzenie danych informatycznych), 269a kk - zakłócanie systemu komputerowego, art. 287 kk - oszustwo komputerowe, art.107 kodeksu wykroczeń - dokuczenia lub złośliwe wprowadzanie w błąd.

DoS/DDoS

DoS *(Denial of Service)*/DDoS *(Distributed Denial of Service)* jest atakiem, który blokuje serwisy internetowe poprzez zalewanie ich z Internetu zbyt wielką ilością pakietów (większą niż może obsłużyć dany serwer). Różnica pomiędzy wersją DoS a DDoS dotyczy głównie skali i związanej z nią liczby źródeł biorących udział w ataku. Może się zdarzyć, że z jakiegoś powodu serwis WWW szkoły padnie ofiarą takiego ataku i nie będzie dostępny przez pewien czas. Jednak, paradoksalnie może się okazać, że komputery szkolne wykonują ataki DoS nas inne serwery znajdujące się w Internecie. Dzieje się to wtedy, kiedy ulegają one infekcji szkodliwym oprogramowaniem i stają się częścią jakiegoś BOT-netu.

Drive by download – Zarażanie poprzez surfowanie

Jednym z najczęstszych wektorów ataków z wykorzystaniem szkodliwego oprogramowania jest zarażanie urządzeń użytkowników sieci Internet, korzystających z przeglądarki. Wiele stron WWW, ale także portali społecznościowych, zawiera w miejscach odwiedzanych przez internautów kody szkodliwych programów, które użytkownik nieświadomie ściąga na swe urządzenia, klikając w kolejne adresy i przeglądając strony internetowe. Tak więc sam użytkownik zaraża swój komputer, tablet czy smartfon aplikacjami, które wykradają identyfikatory i hasła dostępu, wymuszają okup za odblokowanie do danych na dysku, czy powodują, że nasz sprzęt staje się tzw. zombie – czyli zostaje przejęty przez intruzów i wykonuje polecenia bez wiedzy jego właściciela (np. rozsyła spam albo jest częścią sieci DDoS).

Surfowanie w Internecie wymaga zatem zachowania podstawowych zasad higieny. Jeśli surfujemy po adresach, które nie są nam znane, zawartość serwisu może budzić nasze wątpliwości czy podejrzenia (np. „darmowe" kanały płatnych telewizji), zwiększa to zagrożenie, że możemy zostać zarażeni szkodliwym oprogramowaniem. Także klikanie na adresy (tzw. linki) zawarte w poczcie elektronicznej przychodzące od niezweryfikowanych, bądź niefrasobliwych użytkowników jest prostą drogą do stania się ofiarą infekcji malwarem.

Malware - szkodliwe oprogramowanie

Każdy system oparty na pracy komputerów oraz wykorzystujący aplikacje może zostać zainfekowany szkodliwym oprogramowaniem (malware). Istnieje wiele typów takich zagrożeń w postaci: wirusów komputerowych, koni trojańskich, oprogramowania szpiegującego czy atakującego użytkowników bankowości elektronicznej. Szkodliwe programy mogą wniknąć poprzez połączenia z Internetem, są przynoszone przez niefrasobliwych użytkowników (np. na pamięciach USB), mogą przenosić się w czasie synchronizacji urządzeń (np. telefonu z komputerem). Brak aktualizacji oprogramowania zwiększa prawdopodobieństwo infekcji a brak systemów antywirusowych, antymalware, czy firewall powoduje całkowitą ekspozycję za zagrożenia bezpieczeństwa.

Nadużywanie internetu

Zjawisko to, jak dotąd, nie doczekało się jednej, powszechnie uznawanej definicji. Opisując zagadnienie stosuje się pojęcia takie jak „siecioholizm", „nadużywanie Internetu", „patologiczne używanie" czy „uzależnienie od Internetu". Część badaczy uważa, iż pojęcie „uzależnienie" nie może mieć zastosowania w kontekście internetu, z uwagi na fakt przyporządkowania temu pojęciu grupy uzależnień fizjologicznych (alkohol, substancje psychotropowe, nikotyna). Zdaniem innych „uzależnienie od Internetu" mieści się w grupie uzależnień behawioralnych, co daje podstawę do stosowania tego terminu również w kontekście Internetu. Uzależnienie od Internetu nie jest sklasyfikowane jako choroba według klasyfikacji zaburzeń psychicznych. Nadużywanie sieci związane zarówno z czasem, intensywnością korzystania z internetu, przy równoczesnym zaniedbywaniem innych aktywności. W wielu przypadkach stan taki ma znaczący wpływ na pogorszenie funkcjonowania człowieka w różnych sferach: fizycznej, psychicznej, społecznej, ekonomicznej, interpersonalnej.

Niebezpieczne kontakty /uwodzenie w internecie

Uwodzenie dzieci w Internecie (ang. child grooming). to rodzaj relacji tworzonej za pośrednictwem Internetu między osobą dorosłą a osobą małoletnia (poniżej 15 r.ż.), w celu jej uwiedzenia i wykorzystania. Działania podejmowane przez sprawcę nastawione są na nawiązanie więzi emocjonalnej z dzieckiem w celu zdobycia jego zaufania. Ma to w konsekwencji przekonać dziecko do podejmowania różnych czynności i ułatwić późniejsze jego seksualne wykorzystanie. Wykorzystanie seksualne nie wiąże się wyłącznie z fizycznym aktem w świecie realnym, ale również innymi formami takimi jak: prezentowanie dziecku materiałów pornograficznych, prowadzenie rozmów o charakterze erotycznym, składanie propozycji seksualnych, nakłanianie do wykonywania i wysyłania intymnych zdjęć/filmów, czy prezentowanie zachowań seksualnych podczas chatów i wideotransmisji. Grooming jest często procesem rozłożonym w czasie i przebiegającym wieloetapowo. Rozpoczyna się od zaprzyjaźnienia się z dzieckiem. Następnie jest ono „oswajane" ze szkodliwymi treściami, w kontaktach poruszane są tematy związane z seksem. Kolejny etap polega zachęcaniu do podejmowania czynności intymnych przy jednoczesnym naleganiu na utrzymaniu tajemnicy dotyczącej relacji. Podczas procesu uwodzenia sprawca stosuje różne techniki manipulacji, używa również szantażu czy groźby. Ryzyko podejmowania niebezpiecznych kontaktów online przez dzieci i młodzież jest często związane z niskimi kompetencjami w zakresie właściwiej oceny sytuacji, rozumienia i przewidywania skutków podejmowanych działań. Jednocześnie należy pamiętać, iż większość dzieci charakteryzuje otwartość, zaufanie do świata i chęć nawiązywania znajomości. Uwodzenie dzieci w Internecie jest przestępstwem uregulowanym w art. 200a kodeksu karnego.

Phishing

Phishingiem określa się nakłanianie użytkowników metodami socjotechnicznymi do ujawniania swoich wrażliwych danych (identyfikatorów i haseł, numerów i dat ważności kart kredytowych) w celu ich późniejszego wykorzystania do dokonywania oszustw przez cyberprzestępców. Typowym przykładem są wysyłane e-mailem instrukcje zmiany haseł do kont bankowych wysyłane przez intruzów podszywających się pod instytucje finansowe. Mogą to być także wiadomości dystrybuowane na portalach społecznościowych o „super okazjach" (towarów, usług) lub po prostu ciekawostek przykuwających uwagę. Phishing można spotkać nawet w grach internetowych.

Nieuważny użytkownik klikając w podejrzane linki wchodzi na zarażone, sfałszowane strony (często do złudzenia przypominające znajome strony – np. bankowe) i podążając za instrukcją (np. zmiany hasła do bankowości elektronicznej) podaje swoje wrażliwe dane intruzom.

Pornografia dziecięca
Materiały przedstawiające seksualne wykorzystanie dzieci

Termin określający materiały (tekst, film, zdjęcie, zapis audio), które powstały podczas seksualnego wykorzystania dziecka. Termin ten jest bardziej poprawny niż termin „pornografia dziecięca" ponieważ odzwierciedla charakter przestępstwa dokonanego na dziecku. Polski Kodeks Karny (art. 202 kk) zabrania produkcji, utrwalania, przechowywania, posiadania, uzyskiwania dostępu oraz prezentacji treści pornograficznych z udziałem małoletniego. Jak również: produkcji, rozpowszechniania, prezentowania, przechowywania, posiadania treści pornograficznych przedstawiających wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej.

„Erotyka dziecięca”

Treści, które przedstawiają dziecko w seksualnym kontekście (np. ubrane w erotyczną bieliznę, upozowane w erotycznych i wyzywających pozach), które nie stanowią naruszenia prawa. Wytwarzanie takich treści jest formą wykorzystania seksualnego małoletnich, a materiały są atrakcyjne dla osób o pedofilskich skłonnościach.

Ransomware

Spektakularnym przykładem infekcji jest typ wirusa zwany „ransomware”, który próbuje wymusić okup na użytkowniku, który w pewnym momencie od zarażenia, otrzymuje na ekranie informację, że zablokowano mu dostęp do danych na dysku i musi zapłacić przez internet sporą kwotę (np. kilkaset złotych) aby ten dostęp odzyskać. Użytkownik jest przy tym zwykle „straszony”, że ta operacja jest wynikiem jego działalności (np. wchodzenia na strony z pornografią dziecięcą) oraz wykonywana jest przez jednostki uprawnione (np. organy ścigania). Ponieważ ransomware jest coraz bardziej zawansowany technicznie (dane są szyfrowane profesjonalnymi algorytmami kryptograficznymi) szansa na ich odzyskanie jest praktycznie bliska zeru. Po zapłaceniu zaś okupu nie ma gwarancji, że dostęp do danych będzie odzyskany, za to jest pewność, że kolejne wymuszenia okupu będą następowały w przyszłości.

Seksting

Seksting to przesyłanie za pomocą Internetu i urządzeń mobilnych swoich zdjęć, filmów lub wiadomości o charakterze seksualnym. Zjawisko to dotyczy całej grupy internautów - dorosłych, dzieci i młodzieży. Szczególnie w przypadku tej ostatniej grupy możemy mówić o poważnym zagrożeniu i konsekwencjach wiążących się z tym zjawiskiem. Najczęściej nagie zdjęcia przesyłane są pomiędzy osobami znajomymi, które tworzą związek lub są na etapie nawiązywania relacji, często jako dobrowolna aktywność własna, ale i na prośbę obecnego czy przyszłego partnera. W założeniu ma to być korespondencja o prywatnym charakterze. Niestety zdarza się, co pokazują liczne doniesienia medialne, że materiały przekazywane w prywatnej korespondencji trafiają do publicznego dostępu, stając się niekiedy przyczyną tragedii. Zagadnienie sekstingu może w niektórych przypadkach być naruszeniem prawa. W polskim prawie istnieje szereg przepisów, które można odnosić do tego zagadnienia. Polski Kodeks karny (art. 202 kk) zabrania produkcji, utrwalania, przechowywania, posiadania, uzyskiwania dostępu oraz prezentacji treści pornograficznych z udziałem osoby nieletniej. Jest to przestępstwo ścigane z urzędu. Nielegalne jest ponadto składanie propozycji obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych (art. 200a kk) małoletniemu poniżej lat 15. Zabronione jest również utrwalanie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej używając w tym celu wobec niej przemocy, groźby bezprawnej lub podstępu oraz rozpowszechnianie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody (art. 191a kk).

Treści szkodliwe i nielegalne

Treści nielegalne to sprzeczne z obowiązującym w danym kraju prawem. W Polsce, zabronione jest publikowanie, rozpowszechnianie, posiadanie, utrwalanie, produkowanie, sprowadzanie, przechowywanie, prezentowanie treści pornograficznych z udziałem małoletniego (art. 202 kk), publiczne prezentowanie treści pornograficznych z udziałem zwierząt oraz związanych z przemocą (art. 202 kk), treści propagujących ustrój faszystowski lub inny totalitarny ustrój państwa (art. 256 kk) oraz treści znieważających o charakterze rasistowskim i ksenofobicznym (art. 257 kk). Publikacje te mają charakter zarówno zabroniony, jak i szkodliwy. W sieci można napotkać również treści, które nie są nielegalne w świetle prawa, ale należy kwalifikować je jako treści szkodliwe. To znaczy takie, które mogą wywołać negatywne emocje u odbiorcy i mieć negatywny wpływ na jego sferę emocjonalną i społeczną oraz zachowanie. Do szkodliwych treści zalicza się m.in. treści obrazujące przemoc, obrażenia fizyczne, prezentujące drastyczne sceny, okrucieństwo wobec zwierząt, treści nawołujące podejmowania działań autodestrukcyjnych, treści dyskryminacyjne oraz pornograficzne.

Włamania na stronę lub do systemów komputerowych „back-office”

Poprzez rozliczne podatności znajdujące się systemach komputerowych intruzi mogą włamać się do serwisu WWW udostępnianego przez szkołę, ale także celem włamania może być szkolny serwer zawierający dane (np. osobowe bądź finansowe). Jeśli systemy takie nie są stale administrowane i aktualizowane, prawdopodobieństwo stania się ofiarą ataku dramatycznie wzrasta. Zdarza się, że strona WWW ulega podmianie a nikt z personelu tego nie zauważa przez dłuższy czas, bo np. aktualizacje strony są czynione bardzo rzadko a strona nie jest monitorowana.

Wykorzystanie szkolnej infrastruktury do nielegalnej lub szkodliwej działalności

Sporym zagrożeniem dla szkoły jest także wykorzystywanie infrastruktury do funkcji niepożądanych bądź nawet nielegalnych. Może się zdarzyć, że uczniowie w czasie zajęć, korzystając ze szkolnej sieci WiFi ściągają duże ilości danych nie dotyczących procesu edukacji np. ściągają pliki multimedialne, zapychając łącze. Jest to działalność niepożądana. Gorzej, jeśli zajmują się nielegalną dystrybucją (np. nielegalnych kopii gier) grami hazardowymi lub zajmują się hackingiem albo prześladują rówieśników bądź nauczycieli. Jeśli tego typu działania nie są blokowane, monitorowane lub nie powodują reakcji ze strony kierownictwa placówki powoduje to duże zagrożenie dla funkcjonowania szkoły.

Oprócz nieuprawnionych działań własnych użytkowników, przy braku stosowania się do reguł bezpieczeństwa i pozostawieniu infrastruktury bez opieki nawet na pewien czas – możemy mieć także do czynienia z nieuprawnionym działaniem intruzów z wszelkimi tego konsekwencjami (utrata danych, śledztwa organów ścigania itp.).

Zagrożenia ze strony przenośnych nośników pamięci

Wszelkie nośniki zawierające dane, które można dołączyć do sprzętu komputerowego w szkole stanowią zagrożenie na równi z zagrożeniami internetowymi. Te same wirusy i konie trojańskie mogą przedostać się do sieci wewnętrznej (często nawet dużo łatwiej) przy pomocy zawirusowanego pendrive'a, płyty CD, dysku USB itp. Dlatego kontrola antywirusowa wyłącznie na styku z Internetem nie jest wystarczająca.

Zagrożenia związane z WiFi

Udostępnianie WiFi w szkole zawsze wiąże się z zagrożeniami. Szczególnie jeśli byłby to dostęp bez ograniczeń. Jest niezwykle istotne, by przemyśleć fakt i zakres udostępniania WiFi. W szczególności szyfrowanie dostępu do hotspotów i rejestracja użytkowników korzystających jest pierwszym krokiem do ograniczania zagrożeń. Jeśli bowiem ktokolwiek mógłby anonimowo skorzystać z szkolnej sieci WiFi należy się spodziewać, że zostanie to wykorzystane do przeprowadzania ataków – nie tylko na infrastrukturę szkoły ale także, poprzez internet na dowolny serwis (np. bankowy lub sklepy internetowe).

Załącznik nr 2.
Słownik najważniejszych pojęć związanych z użytkowaniem sieci

Administrator

Potocznie określany adminem. Informatyk, do którego zadań należy zarządzanie systemem informatycznym i dbanie o jego sprawne i ciągłe działanie. Można wyróżnić administratorów m.in.: aplikacji, baz danych, serwerów.

(admin, informatyk, system informatyczny, baza danych, serwer)

Adres IP

To unikatowy numer, liczba, nadawana urządzeniom będącym w sieci komputerowej.

(host, adres komputera, adres publiczny, protokół IP, IP, sieć komputerowa, komputer, sieć)

Antywirus

Zobacz: Program antywirusowy

Aplikacja mobilna

Oprogramowanie działające na urządzeniach przenośnych (m.in. smartfon, tablet), które powstaje dla różnych systemów operacyjnych (m.in. Android, Apple iOS, Windows Phone) i napisane jest w różnych językach programowania. Aplikacje mogą być wykorzystywane do różnych celów m.in. komunikacja, edukacja, rozrywka. Są one oferowane przez sklepy internetowe (m.in. Google Play, App Store) bezpłatnie lub za opłatą.

(smartfon, telefon komórkowy, tablet, komunikacja internetowa, urządzenia mobilne, nowe technologie, mobile apps, Web 2.0)

Audiobook

Inaczej książka mówiona, nagranie dźwiękowe zawierające odczytany przez lektora tekst publikacji książkowej. Audiobook zapisany jest w formacie audio lub np. MP3).

(edukacja medialna, nowe technologie, kompetencje medialne, umiejętności elektroniczne)

Aukcje internetowe

Zobacz: Zakupy online

Awatar

Reprezentacja uczestnika światów wirtualnych, która dotyczy zarówno rzeczywistych ludzi uczestniczących za ich pomocą w tych światach, jak i postaci generowanych przez oprogramowanie. Awatary są używane m.in. na forach dyskusyjnych, w grach komputerowych.

(gra komputerowa, gra online, fora dyskusyjne, forum internetowe)

Bankowość elektroniczna

Forma usługi oferowanej przez bank, która umożliwia jej użytkownikowi dostęp do rachunku za pomocą urządzenia elektronicznego z dostępem do internetu (m.in. komputera, smartofna).

(e-banking, bankowość internetowa, HTTPS, transakcja internetowa)

Blog

Rodzaj internetowego dziennika zawierający odrębne, często poświęcone konkretnemu tematowi i uporządkowane chronologicznie wpisy. Blogi dają zazwyczaj możliwość zamieszczania zdjęć, filmów, archiwizowania i kategoryzowania publikowanych treści, a także komentowania ich przez czytelników danego bloga. Osoba prowadząca bloga określana jest blogerem, zaś ogół blogów traktowany jako medium komunikacyjne nosi nazwę blogosfery.

(bloger, blogosfera, dziennik internetowy, pamiętnik internetowy, Web 2.0, mikroblog, log, vloger)

Botnet

Grupa komputerów zainfekowanych złośliwym oprogramowaniem (które pozostaje w ukryciu przed użytkownikiem) pozwalacych jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi urządzeniami w ramach botnetu. Dzięki tej kontroli możliwe jest np. zdalne rozsyłanie spamu oraz inne ataki z użyciem zainfekowanych komputerów.

(spam, trojan, złośliwe oprogramowanie, wirus, robak, cyberbezpieczeństwo, bezpieczeństwo komputerowe, bezpieczeństwo teleinformatyczne, CERT Polska, cyberprzestępczość, przestępczość komputerowa, oszustwo internetowe)

CERT

Zespół ds. reagowania na przypadki naruszenia bezpieczeństwa teleinformatycznego (ang. *Computer Emergency Response Team*). Typ organizacji rozpowszechniony na bazie koncepcji zespołu CERT CC utworzonego w 1988 r w USA. po incydencie z robakiem Morrisa (ang. *Morris Worm*). Zadaniem CERT jest całodobowe nadzorowanie ruchu internetowego i podejmowanie natychmiastowych akcji w razie pojawienia się zagrożenia. CERT publikuje też materiały edukacyjno-szkoleniowe.

(bezpieczeństwo komputerowe, bezpieczeństwo teleinformatyczne, cyberbezpieczeństwo, cyberochrona, ochrona danych, cyberzagrożenia, CERT Polska)

CERT Polska

CERT (ang. Computer Emergency Response Team) Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci internet. CERT Polska działa od 1996 roku, a od roku 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams). W ramach tej organizacji współpracuje z podobnymi grupami na całym świecie. Zespół CERT Polska działa w strukturach Naukowej i Akademickiej Sieci Komputerowej (NASK). Do głównych zadań zespołu należy m.in.: rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci, alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń, prowadzenie działań zmierzających do wzrostu świadomości dotyczącej bezpieczeństwa teleinformatycznego, prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów internetu, a także niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego.

(NASK, bezpieczeństwo komputerowe, bezpieczeństwo teleinformatyczne, cyberbezpieczeństwo, cyberochrona, ochrona danych, cyberzagrożenia)

Certyfikaty SSL

Narzędzie zapewniające ochronę witryn internetowych, a także gwarant zachowania poufności danych przesyłanych drogą elektroniczną. Pełne bezpieczeństwo jest efektem zastosowania szyfrowania danych przesyłanych między serwerem a komputerem użytkownika. Może to być serwer www, pocztowy, FTP lub inny. Certyfikat SSL zainstalowany na serwerze umożliwia jego uwierzytelnienie (ustalenie autentyczności) oraz nawiązanie bezpiecznego połączenia. Certyfikaty SSL rejestrowane są na określoną nazwę domenową, zawierają informacje o właścicielu domeny, jego adresie itp. Dane te są zabezpieczone kryptograficznie i nie można ich samodzielnie zmienić. Certyfikaty SSL są wystawiane za opłatą przez stosowne Urzędy Certyfikacji.

(certyfikat bezpieczeństwa, domena, szyfrowanie danych, serwer, FTP, SSL, protokół SSL, witryna internetowa, serwer www, komputer, poufność danych, ochrona danych)

Child grooming

Zobacz: Uwodzenie dzieci

Ciasteczko

Krótkie informacje tekstowe wysyłane przez serwis internetowy (z serwera WWW) i zapisywane na komputerze klienta w plikach txt. Ciasteczka są wykorzystywane do zapamiętywania stanu aplikacji internetowej lub ustawień dla konkretnego użytkownika. Mogą zawierać rozmaite informacje o użytkowniku danego serwisu WWW i "historii" jego łączności z danym serwisem (sesji). Zazwyczaj wykorzystywane są do automatycznego rozpoznawania danego użytkownika przez serwer, dzięki czemu może on wygenerować przeznaczoną dla niego stronę. Umożliwia to tworzenie spersonalizowanych serwisów WWW (ang. Cookie).

(HTTP cookie, ciasteczka, cookies, przeglądarka, przeglądarka internetowa, przeglądarka www, historia przeglądania, WWW, serwis WWW, serwer www, strona internetowa)

Cyberbezpieczeństwo

Definicja cyberbezpieczeństwa może być różna i zależy od tego do kogo się ona odnosi. Inne znaczenie może mieć ono dla pojedynczych użytkowników internetu, inne dla przedsiębiorstw, a jeszcze inne dla państw oraz całych narodów. Niezależnie jednak od punktu odniesienia, główna istota cyberbezpieczeństwa obejmuje zbiór działań i zasobów, które umożliwiają obywatelom, przedsiębiorstwom i państwom osiągnięcie celów informatycznych w sposób bezpieczny i niezawodny przy zachowaniu prywatności.

(cybersecurity, zespół abuse, CERT Polska, bezpieczeństwo komputerowe, ochrona danych, cyberochrona, bezpieczeństwo teleinformatyczne)

Cyberharassment (dosł. cyberprześladowanie)

Zobacz: cyberstalking

Cyberprostytucja

Zjawisko polegające na uzyskiwaniu korzyści materialnych w zamian za udostępnianie, przekazywanie poprzez internet materiałów erotycznych lub pornograficznych wytworzonych z własnym udziałem. Mogą to być zdjęcia i filmy lub (coraz częściej) pokaz na żywo za pomocą kamerki internetowej.

(wirtualna prostytucja, materiały erotyczne, erotyka, zachowania seksualne, materiały pornograficzne, kamerka internetowa, niebezpieczne zachowania, ryzykowne zachowania, uwodzenie, uwodzenie dzieci, child grooming, Dyżurnet.pl, hotline, telefon zaufania, tel. 116 111, tel. 800 100 100)

Cyberprzemoc

Przemoc z użyciem mediów elektronicznych. Do takich działań zalicza się m.in. nękanie, wyzywanie, straszenie, poniżanie kogoś w internecie lub przy użyciu telefonu, robienie komuś zdjęć lub filmów bez jego zgody, ich publikowanie i rozsyłanie lub podszywanie się pod kogoś w sieci. Cyberprzemoc może dotknąć wszystkich użytkowników internetu, bez względu na wiek czy poziom umiejętności posługiwania się komputerem. Sprawcy cyberprzemocy mają wrażenie że są anonimowi, co pobudza i zachęca ich do działania.

(przemoc rówieśnicza, przemoc online, agresja rówieśnicza, agresja elektroniczna, agresja w sieci, cyberbullying, dręczenie, prześladowanie, cyberstalking, agresja w szkole, niebezpieczne zachowania, telefon zaufania, tel. 116 111, tel. 800 100 100, Dyżurnet.pl, hotline)

Cyberprzestępczość

Inaczej przestępczość komputerowa, czyli niezgodna z prawem działalność skierowaną przeciwko systemom komputerowym lub wykonywana przy pomocy systemów komputerowych, sieci komputerowych czy internetu, jako narzędzi służących do dokonania przestępstwa.

(CERT Polska, przestępczość komputerowa, cyberbezpieczeństwo, cyberprzestępczość, phishing, robak, koń trojański, trojan, malware, spam, złośliwe oprogramowanie, zespół abuse, oszustwo internetowe)

Cyberstalking (dosł. cyberdręczenie)

Zjawisko natrętnego i złośliwego dręczenia pojedynczej osoby, grupy osób lub całej organizacji przy użyciu technologii informacyjnej, w szczególności internetu. Prześladowca określany jest często jako stalker.

(stalker, stalking, cyberdręczenie, dręczenie, prześladowanie)

Cyfrowy imigrant

Przedstawiciel pokolenia epoki precyfrowej, w którego życie nowe technologie i internet wkroczyły dopiero, kiedy dorastał lub był już dorosły. Twórcą terminu jest Marc Prensky, który po raz pierwszy opisał go w 2001 r. w artykule „Digital Natives, Digital Immigrants" („Cyfrowi tubylcy i Cyfrowi imigranci").

(nowe technologie, użytkownik internetu, edukacja medialna, wykluczenie cyfrowe, media literacy, przepaść cyfrowa)

Cyfrowy tubylec

Przedstawiciel młodszego pokolenia urodzonego i wychowywanego w erze informatycznej, w otoczeniu nowych technologii z dostępem do internetu. Nowe media są dla niego naturalnym środowiskiem. Zdobycze techniki nie stanowią dla niego żadnych barier w procesie komunikacji. Twórcą terminu jest Marc Prensky, który po raz pierwszy opisał go w 2001 r. w artykule „Digital Natives, Digital Immigrants" („Cyfrowi tubylcy i Cyfrowi imigranci").

(nowe technologie, użytkownik internetu, edukacja medialna, wykluczenie cyfrowe, media literacy, Web 2.0)

Czat

Rozmowa prowadzona między dwoma lub wieloma uczestnikami za pośrednictwem internetu, podczas której rozmówcy naprzemiennie przesyłają sobie wiadomości tekstowe. Wraz z rozwojem internetu, postępem technologicznym i pojawieniem się portali Web 2.0 tradycyjny czat wzbogacono o możliwość połączenia audio i wideo. Dzięki temu komunikacja online może służyć nie tylko rozrywce i celom prywatnym, ale także może być wykorzystywania w celach biznesowych (np. wideo-konferencje).

(czat wideo, wideo, wideo-konferencja, Web 2.0, komunikacja internetowa, nowe technologie, skype, Messenger, chat)

Dane osobowe

Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Możliwa jest idendyfikacja jednostki, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

(ochrona danych, tożsamość, prywatność online, bezpieczeństwo danych)

Domena internetowa

Ciąg nazw systemu Domain Name System (DNS) wykorzystywany w internecie, składający się z wyrazów umieszczonych w pewnym poddrzewie struktury DNS tj. zakończonych stałym sufiksem. Domena internetowa składa się z dwóch części - nazwy głównej oraz końcówki - rozszerzenia. Nazwę główną bardzo często tworzy nazwa firmy, organizacji, akcji lub jej skrót. Rozszerzenie jest odgórnie ustalone - można wybrać spośród możliwych propozycji. Każdy kraj posiada przypisane rozszerzenie np. Polska - „.pl".

(DNS, nazwa internetowa, rozszerzenie, .pl, strona www, WWW, serwis WWW, strona internetowa)

Dyżurnet.pl

Dyżurnet.pl to zespół ekspertów Naukowej i Akademickiej Sieci Komputerowej, działający jako punkt kontaktowy (hotline) do zgłaszania nielegalnych i szkodliwych treści w internecie. Aktywność Dyżurnetu skupia się przede wszystkim na działaniach na rzecz usunięcia z sieci materiałów dotyczących seksualnego wykorzystywania dzieci. Zespół Dyżurnet.pl analizuje treści wskazane przez użytkowników, wykonuje dokumentację techniczną, przesyła informacje do policji, prokuratury, administratorów serwisów internetowych czy też zagranicznych punktów kontaktowych zrzeszonych w INHOPE. Co ważne – zespół nie dokonuje interpretacji prawnej, nie wyszukuje nielegalnych treści w sieci i nie zachęca użytkowników internetu do ich wyszukiwania. Dyżurnet.pl prowadzi również działania informacyjne i edukacyjne, kierowane do różnych grup użytkowników.

(pornografia dziecięca, materiały przedstawiające seksualne wykorzystywanie dziecka, CSAM, erotyka dziecięca, NASK, treści nielegalne, treści szkodliwe, INHOPE, hotline, punkt kontaktowy)

E-book

To inaczej książka elektroniczna. Treść zapisana w formie elektronicznej, przeznaczona do odczytania za pomocą odpowiedniego oprogramowania zainstalowanego na urządzeniu komputerowym np. komputerze osobistym, czytniku e-booka, palmtopie.

(eBook, książka elektroniczna, publikacja elektroniczna, e-książka, czytnik książek elektronicznych)

E-commerce

Handel elektroniczny, procedury wykorzystujące środki i urządzenia elektroniczne (telefon stacjonarny i komórkowy, faks, internet) w celu zawarcia transakcji handlowej. Najbardziej popularną metodą handlu elektronicznego jest handel internetowy, gdzie występują transakcje handlowe pomiędzy sprzedającymi a kupującymi. Najbardziej powszechną formą handlu elektronicznego są sklepy internetowe.

(handel online, handel internetowy, zakupy online, aukcje internetowe, bankowość elektroniczna, e-handel, transakcja online, sklep internetowy)

Edukacja medialna

Kształtowanie umiejętności świadomego, krytycznego, odpowiedzialnego i selektywnego korzystania ze środków masowego przekazu, tworzenia i nadawania przekazów medialnych.

(media literacy, kompetencje medialne, e-learning, umiejętności elektroniczne)

E-learning

Nauczanie z wykorzystaniem sieci komputerowych i internetu, oznacza wspomaganie procesu dydaktyki za pomocą komputerów osobistych i internetu. Dzięki takiej formie edukacji możliwe jest ukończenie kursu, szkolenia, a nawet studiów bez konieczności fizycznej obecności w sali wykładowej.

(edukacja medialna, kursy online, media literacy, umiejętności elektroniczne, kompetencje medialne)

E-mail

zobacz: poczta elektroniczna

Emotikon

Ideogram złożony ze znaków tekstowych, najczęściej przedstawiający symboliczny ludzki grymas twarzy i będący wyrazem nastroju, powszechnie używany przez użytkowników internetu. Przykładem emotikonu jest uśmieszek lub buźka.

(komunikacja internetowa, Web 2.0, telefon komórkowy, smartfon, laptop, chat, czat, messanger)

Erotyka dziecięca

Treści, które przedstawiają dziecko w seksualnym kontekście natomiast nie są nielegalne. Małoletni są upozowani w erotycznych i wyzywających pozach, ubrane w erotyczną bieliznę. Wytwarzanie takich treści jest formą wykorzystania seksualnego małoletnich, a materiały są atrakcyjne dla osób o pedofilskich skłonnościach.

(pornografia dziecięca, Dyżurnet.pl, hotline, treści szkodliwe, tel. 116 111, tel. 800 100 100, telefon zaufania)

Filtr rodzicielski

Program lub usługa, chroniąca przed dostępem dziecka do materiałów szkodliwych - treści pornograficznych i przemocy w internecie. Usługę oferują niektórzy dostawcy internetu. Rodzic może także nabyć taką usługę w postaci programu do zainstalowania na komputerze. Filtr rodzinny nie daje 100 proc. gwarancji bezpieczeństwa dziecka.

(program ochrony rodzicielskiej, program filtrujący, kontrola rodzicielska, narzędzia ochrony rodzicielskiej, filtr kontroli rodzicielskiej, ochrona dziecka, filtr treści, treści pornograficzne, treści szkodliwe)

Flejm

Kłótnia internetowa polegająca na wymianie obraźliwych komentarzy. Często jest onaspowodowana skrajnymi różnicami w opinii na dany temat, np. polityczny.

(kłótnia internetowa, forum internetowe, trolling, mowa nienawiści, hate speech, hejt, chat, czat)

Fonoholizm

Zjawisko nadmiernego korzystania z telefonu komórkowego, który towarzyszy takiej osobie nieustannie, co może nagatywnie wpłynąć na jej życie społeczne, wyniki w nauce czy pracy.

(dysfunkcyjne korzystanie z telefonu, dysfunkcyjne korzystanie z internetu, infoholizm, uzależnienie od internetu, uzależnienie od telefonu, nadużywanie internetu, nadużywanie telefonu, kompulsywne korzystanie z internetu, kompulsywne korzystanie z telefonu)

Forum dyskusyjne

Forma grupy dyskusyjnej w internecie, która służy do wymiany informacji i poglądów między osobami o podobnych zainteresowaniach. Fora dyskusyjne prowadzone są przez większość portali i wortali. Są one także powszechnie używane na stronach instytucji, uczelni, czasopism itp.

(komunikacja internetowa, Web 2.0, forum internetowe, grupa dyskusyjna)

Geolokalizacja

Położenie oraz proces określania geograficznego położenia fizycznych przedmiotów lub osób zazwyczaj za pomocą GPS, bądź adresu IP urządzenia. Położenie zwykle określane jest poprzez współrzędne geograficzne, ale także innego rodzaju dane adresowe (kod pocztowy, miasto, ulica i numer domu).

(usługa geolokalicazji, aplikacje mobilne, dane adresowe, adres IP)

Gra komputerowa

Rodzaj oprogramowania komputerowego przeznaczonego do celów rozrywkowych bądź edukacyjnych. Gra wymaga od użytkownika (gracza) rozwiązywania zadań logicznych lub zręcznościowych.

(gracz, rozrywka, edukacja, Web 2.0, urządzenia mobilne, konsola)

Gra online

To gra, której uruchomienie wymaga dostępu do internetu.

(gracz, rozrywka, edukacja, Web 2.0, urządzenia mobilne, konsola)

Grooming

Zobacz: uwodzenie dziecka online

Hacker

Osoba o bardzo dużych, praktycznych umiejętnościach informatycznych (lub elektronicznych), która identyfikuje się ze społecznością hakerską. Hakerzy odznaczają się bardzo dobrą orientacją w internecie, znajomością wielu języków programowania oraz systemów operacyjnych.

(informatyk, język programowania, system operacyjny, umiejętności elektroniczne)

Hacking

Uzyskanie nieuprawnionego dostępu do komputera, systemu komputerowego, danych czy informacji zawartych w systemach komputerowych. Hacking często jest elementem koniecznym do popełnienia przestępstwa komputerowego.

(przestępczość komputerowa, oszustwo internetowe, cyberprzestępczość, CERT Polska, trojan, koń trojański, złośliwe oprogramowanie, wirus, robak, cyberbezpieczeństwo, bezpieczeństwo komputerowe, bezpieczeństwo teleinformatyczne)

Hasło internetowe

Hasło dostępu do danych internetowych danego użytkownika (np. poczty elektronicznej, konta w serwisie społecznościowym, bloga, bankowości elektronicznej). Każdy użytkownik tworząc hasło powinien kierować się zasadą, że jest ono znane tylko przez niego i jest mocne (trudne do rozszyfrowania przez inne osoby i łatwe do zapamiętania przez autora). Mocne hasło internetowe może składać się z ciągu znaków – cyfr, liter i znaków specjalnych. Zaleca się używanie różnych haseł do różnych serwisów.

(poczta elektroniczna, serwis społecznościowy, blog, bankowość elektroniczna, prywatność online, bezpieczeństwo danych, profil internetowy, ochrona danych)

Hasztag

Pojedyncze słowo lub wyrażenie bez spacji poprzedzone symbolem #. Hasztag służy grupowaniu wiadomości i informacji na określony temat. Hasztag jest zazwyczaj używany w serwisach społecznościowych i mikroblogach (np. Twitter, Facebook, Instagram).

(hashtag, serwis społecznościowy, mikroblog, Web 2.0, komunikacja internetowa, Twitter, Facebook, Instagram)

Hazard online

Gry pieniężne w internecie, w których o wygranej w mniejszym lub większym stopniu decyduje przypadek.

(ryzykowne zachowanie, nadużywanie internetu, nadmierne korzystanie z internetu, nadmierne korzystanie z komputera, uzależnienie)

Hejt internetowy

Termin ten stosuje się przede wszystkim do takich wypowiedzi, które są agresywne i nie mają podłoża ideologicznego.

(hate speech, mowa nienawiści, ksenofobia, rasizm, szkodliwe treści)

Host

Każdy komputer podłączony do internetu (lub sieci lokalnej wykorzystującej protokół IP) i posiadający unikalny adres IP.

(adres sieciowy, adres IP, komputer, protokół IP)

Hosting

Udostępnianie przez dostawcę usług internetowych zasobów serwerowni. Innymi słowy, polega to na oddaniu do dyspozycji m.in. określonej objętości dysku twardego, maksymalnej ilości danych do przesłania przez łącza internetowe serwerowni.

(serwer, serwerownia, host, dysk twardy)

Hotline

Zespół, do którego można anonimowo przekazać zgłoszenie o treściach potencjalnie nielegalnych prezentowanych w internecie lub przesyłanych za jego pośrednictwem. Narodowe punkty hotline są zrzeszone w międzynarodowym stowarzyszeniu INHOPE, dzięki czemu podlegają weryfikacji, współpracują ze sobą, wymieniają doświadczenia oraz podejmują wspólne interwencje wobec nielegalnych treści zamieszczonych w internecie.

Polskim narodowym zespołem hotline jest Dyżurnet.pl działający w ramach instytutu badawczego NASK. Dzięki ścisłej współpracy z Policją oraz innymi zespołami reagującymi zrzeszonymi w stowarzyszeniu INHOPE, zespół podejmuje szybkie interwencje wobec nielegalnych treści publikowanych w sieci i zgłoszonych przez użytkowników internetu.

(Dyżurnet.pl, INHOPE, nielegalne treści, szkodliwe treści, NASK, punkt kontaktowy, materiały przedstawiające seksualne wykorzystywanie dziecka, CSAM)

Hotspot

Bezpłatny i otwarty punt umożliwiający dostęp do internetu najczęściej za pomocą łączności bezprzewodowej oferowanej przez standard WiFi. Hotspoty są najczęściej rozmieszczone w centrach miast (np. rynki, parki), w restauracjach, centrach handlowych, hotelach, lotniskach, dworcach, niektórych środkach komunikacji miejskiej takich jak autobusy, pociągi czy metro.

(bezprzewodowy internet, wifi, dostęp do internetu, łączność bezprzewodowa)

HTTP (ang. Hypertext Transfer Protocol)

Protokół przesyłania dokumentów hipertekstowych. Protokół sieci WWW. Za pomocą protokołu HTTP przesyła się żądania udostępnienia dokumentów WWW i informacje o kliknięciu odnośnika oraz informacje z formularzy. Zadaniem stron WWW jest publikowanie informacji – natomiast protokół HTTP właśnie to umożliwia.

(WWW, serwer, protokół, HTTPS)

HTTPS (ang. Hypertext Transfer Protocol Secure)

Szyfrowana wersja protokołu HTTP. W przeciwieństwie do komunikacji niezaszyfrowanego tekstu w HTTP klient-serwer, szyfruje go za pomocą protokołu SSL. Zapobiega to przechwytywaniu i zmienianiu przesyłanych danych.

(protokół SSL, SSL, protokół, HTTP, szyfrowanie danych, ochrona danych, poufność danych, bankowość elektroniczna, serwer, WWW)

Infoholizm

Zjawisko dotyczące niekontrolowanego przebywania człowieka w cyberprzestrzeni, określane też jako nadmierne korzystanie z internetu i komputera. Zachowanie to może skutkować negatywnymi konsekwencjami w życiu społecznym,nauce i pracy.

(siecioholizm, netoholizm, dysfunkcyjne korzystanie z internetu, fonoholizm, uzależnienie od internetu, nadużywanie internetu, kompulsywne korzystanie z internetu, uzależnienie od komputera)

Internauta

Użytkownik internetu.

(użytkownik internetu, internet, surfowanie, surfować)

Internet

Ogólnoświatowa sieć komputerowa, która łączy lokalne sieci, korzystające z pakietowego protokołu komunikacyjnego TCP/IP, mająca jednolite zasady adresowania i nazywania węzłów (komputerów włączonych do sieci) oraz protokoły udostępniania informacji.

(sieć, sieć komputerowa, surfowanie, surfować)

Internet mobilny

Internet umożliwiający dostęp do serwisów WWW z poziomu urządzeń przenośnych (np. telefonu komórkowego, netbooka).

(urządzenia mobilne, urządzenia przenośne, dostęp do internetu, telefon komórkowy)

Kamera internetowa

Niewielka kamera podłączana do komputera, służąca do przesyłania obrazu bezpośrednio do internetu. Z pomocą takiego urządzenia można także wykonywać cyfrowe zdjęcia i nagrywać filmy.

(nowe technologie, Web 2.0, komunikacja internetowa, webcam, kamerka internetowa, streaming, transmisja online)

Komputer

Elektroniczna maszyna cyfrowa przeznaczona do przetwarzania informacji (danych) przedstawionych w postaci cyfrowej. Komputer sterowany jest programem zapisanym w pamięci. Pojęcie komputera obejmuje komputery zaprogramowane na stałe, używane jako automaty sterujące (np. w urządzeniach gospodarstwa domowego), jak i komputery uniwersalne, które można dowolnie zaprogramować. Najpopularniejszymi komputerami są komputery osobiste, które przeznaczone są dla pojedynczych użytkowników i umożliwiają mu korzystanie np. z oprogramowania biurowego, przeglądarek internetowych.

(komputer osobisty, maszyna cyfrowa, sprzęt elektroniczny, urządzenie elektroniczne, nowe technologie, urządzenia mobilne)

Komunikator internetowy

Program komputerowy, który pozwala na przesyłanie natychmiastowych komunikatów pomiędzy dwoma lub większą liczbą komputerów, poprzez sieć komputerową, zazwyczaj internet. Komunikacja ta może odbywać się w czasie rzeczywistym i daje możliwość przesyłania poza samym tekstem także zdjęć, dźwięków i obrazów wideo. Duża zaletą komunikatorów internetowych jest to, że pokazują one status użytkowników (informacja o jego obecności) co zwiększa znacznie szansę na prowadzenie bezpośredniej konwersacji.. Przykładem komunikatora internetowego jest Skype, Google Talk, Facebook Messenger (ang. *Instant Messenger*).

(*skype, Messenger, Google Talk, Facebook Messenger, komunikacja internetowa, nowe technologie, Web 2.0, Instant Messenger, czat, chat)*

Konsola gier wideo

Konsola do gier, komputer o wyspecjalizowanej architekturze przeznaczony do uruchamiania gier wideo.

(gra wideo, gra komputerowa, konsola do gier)

Kontrola rodzicielska

Opcje, stosowane głównie w usługach telewizji kablowej i satelitarnej, telefonach komórkowych, użytkowaniu komputera, w tym w grach video i korzystaniu z internetu, a także w systemach operacyjnych, które mają pomóc rodzicom w ochronie dzieci przed dostępem do nieodpowiednich dla nich treści (m.in. agresja, brutalne sceny, zachowania seksualne).

(system operacyjny, program ochrony rodzicielskiej, program filtrujący, narzędzia ochrony rodzicielskiej, filtr kontroli rodzicielskiej, filtr rodzinny, ochrona dziecka, filtr treści, treści pornograficzne, szkodliwe treści, zachowania seksualne)

Koń trojański

Szkodliwe oprogramowanie, które podszywa się pod przydatne dla użytkownika aplikacje, pod nazwą lub w części pliku i implementuje niepożądane, ukryte przed użytkownikiem różne funkcje (np. programy szpiegujące). Nazwa pochodzi od mitologicznego konia trojańskiego.

(spam, trojan, złośliwe oprogramowanie, wirus, robak, cyberbezpieczeństwo, bezpieczeństwo komputerowe, bezpieczeństwo teleinformatyczne, CERT Polska, cyberprzestępczość, przestępczość komputerowa, oszustwo internetowe)

Ksenofobia

Niechęć, wrogość wobec innych grup etnicznych. Zazwyczaj dotyczy cudzoziemców lub mniejszości narodowych i oparta jest na ich stereotypowym postrzeganiu. Klasyfikowana przez specjalistów jako język wrogości niepodlegający sankcji karnej. Nawoływanie do nienawiści oraz znieważanie na tle różnic narodowościowych penalizowane jest w Polsce na podstawie art. 256 i 257 kk.

(mowa nienawiści, hate speech, hejt, rasizm, nienawiść, dyskryminacja, szkodliwe treści, nielegalne treści, Dyżurnet.pl, hotline).

Laptop

Inaczej notebook, przenośny komputer osobisty. Inne zminiaturyzowane komputery (mniejsze od laptopów) to netbooki, palm topy lub smartfony (ang. *lap* – kolana, *top* – na wierzchu).

(nowe technologie, urządzenia mobilne, komputer osobisty, komputer, notebook)

Licencje Creative Commons (CC)

Zestaw licencji, na mocy których można udostępniać utwory objęte prawami autorskimi. Licencje te pozwalają twórcom utworów zachować własne prawa i jednocześnie dzielić się swoją twórczością z innymi. Licencje te są tworzone i utrzymywane przez organizację Creative Commons.

(prawa autorskie, CC, licencja, creative commons, copyright)

Login

Jest to identyfikator użytkownika wymagany, aby uzyskać dostęp (zalogować się) do systemu komputerowego.

(logowanie, zalogować się, identyfikator użytkownika, hasło uwierzytelniające)

Logowanie

Jest to proces uwierzytelniania i autoryzacji użytkownika komputera, polegający głównie na podaniu identyfikatora użytkownika (loginu) i hasła uwierzytelniającego w celu uzyskania dostępu do systemu informatycznego, systemu komputerowego, komputera czy sieci komputerowej.

(login, zalogować się, hasło uwierzytelniające, identyfikator użytkownika)

Malware

Skrót od angielskich słów malicious software – czyli złośliwe oprogramowanie mające na celu zniszczenie komputera bądź zapisanych na nim informacji. Malware obejmuje wirusy, robaki, konie trojańskie, spyware, nieuczciwe oprogramowanie typu adware oraz inne szkodliwe dla komputera oprogramowanie.

(spam, wirus, robak, koń trojański, trojan, złośliwe oprogramowanie, cyberbezpieczeństwo, bezpieczeństwo komputerowe, bezpieczeństwo teleinformatyczne, CERT Polska, cyberprzestępczość, przestępczość komputerowa, oszustwo internetowe)

Materiały przedstawiające seksualne wykorzystywanie dziecka

Termin określający materiały (tekst, film, zdjęcie, zapis audio), które powstały podczas seksualnego wykorzystania dziecka (gwałtu), termin ten jest bardziej poprawny niż termin „pornografia dziecięca". Polski Kodeks karny zabrania: produkcji, utrwalania, sprowadzania, przechowywania, posiadania, uzyskiwania dostępu oraz prezentacji treści pornograficznych z udziałem małoletniego, jak również: produkcji, rozpowszechniania, prezentowania, przechowywania, posiadania treści pornograficznych przedstawiających wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej.

(pornografia dziecięca, Dyżurnet.pl, hotline, treści nielegalne, tel. 116 111, tel. 800 100 100, telefon zaufania, CSAM)

Mem internetowy

Dowolna, chwytliwa porcja informacji, która jest udostępniana w internecie i może przybrać wiele form – obrazka, filmu, zdania. Cechą charakterystyczną memu jest jego popularność w sieci, a także to, że są regularnie powielane, modyfikowane i rozprzestrzeniane przez użytkowników za pośrednictwem portali społecznościowych, forów internetowych czy komunikatorów.

(forum internetowe, memy, portal społecznościowy, serwis społecznościowy)

Mikroblog

Rodzaj dziennika internetowego, w którym publikuje się krótkie wpisy mające zazwyczaj długość jednego zdania. Wpisy te zazwyczaj są noskiem informacji o czynności jaką się w danej chwili wykonuje, krótkich przemyśleń lub planów na najbliższy czas. Mikroblog może, oprócz wpisów tekstowych, zawierać zdjęcia, klipy dźwiękowe czy filmowe. Może on być dostępny dla każdego lub wąskiej grupy wybranych przez autora czytelników. Przykładem mikroblogu jest Twitter,

(Twitter, blog, bloger, komunikacja internetowa, Web 2.0, nowe technologie)

Mikropłatność

Forma drobnej opłaty pobierana od użytkownika internetu w celu nabycia wirtualnego dobra, kontynuowania lub pełnego skorzystania z usługi online, aplikacji mobilnej czy gry online. Przykładem wirtualnego towaru nabytego za pomocą mikropłatności może być broń lub stroje dla postaci w grze komputerowej.

(gra komputerowa, gra online, usługi online, aplikacje mobilne, bezpieczne zakupy, e-commerce, aukcje internetowe)

Moderator

Osoba lub grupa osób o specjalnych uprawnieniach, której zadaniem jest zapewnienie porządku oraz przestrzegania przez użytkowników regulaminu strony www, forum internetowego, listy dyskusyjnej, serwisu społecznościowego. Moderator zazwyczaj posiada dostęp do narzędzi technicznych, które umożliwiają mu zarządzanie treścią i kontami użytkowników na poziomie wyższym niż zwykli uczestnicy danego serwisu (np. edytowanie lub usuwanie komentarzy i internetowych postów, blokowanie kont użytkowników). Naruszenia regulaminu lub inne wątpliwości dotyczące treści publikowanych na danej witrynie w pierwszej kolejności należy zgłaszać do moderatora.

(forum internetowe, strona www, strona internetowa, regulamin, komentarze, lista dyskusyjna, serwis społecznościowy, portal)

Mowa nienawiści (ang. hate speech)

Znieważenie, pomawianie lub rozbudzanie nienawiści wobec osoby, grupy osób lub innego wskazanego podmiotu. Mowa nienawiści jest narzędziem rozpowszechniania antyspołecznych uprzedzeń i dyskryminacji ze względu na rozmaite cechy, takie jak: rasa (rasizm), pochodzenie etniczne (ksenofobia), narodowość (szowinizm), płeć (seksizm), tożsamość płciowa (transfobia), orientacja psychoseksualna (homofobia), wiek (ageizm), światopogląd religijny (antysemityzm, chrystianofobia, islamofobia).

(hate speech, nienawiść, dyskryminacja, szkodliwe treści, ksenofobia, rasizm, szowinizm, homofobia, antysemityzm, hejt, nielegalne treści, Dyżurnet.pl, hotline)

Multimedia

Media, które stanowią połączenie kilku i różnych form przekazu informacji (np. dźwięk, wideo, animacja, tekst) w celu dostarczania odbiorcom informacji lub rozrywki. Termin „multimedia" ma również zastosowanie w mediach elektronicznych służących do rejestrowania oraz odtwarzania treści multimedialnych.

(edukacja medialna, media literacy, nowe technologie, tablica multimedialna)

Nadmierne korzystanie z internetu

Coraz powszechniejsze zjawisko dotyczące spędzania w Internecie znacznej ilości czasu co może powodować niekorzystne konsekwencje w życiu społecznym, w nauce oraz w pracy. Częstymi objawami nadmiernego korzystania z sieci jest niedosypianie, brak regularnych posiłków, zaburzenia w dotychczasowych aktywnościach oraz w relacjach z przyjaciółmi, rodziną itp.

(dysfunkcyjne korzystanie z internetu, infoholizm, siecioholizm, fonoholizm, uzależnienie od internetu, nadużywanie internetu, kompulsywne korzystanie z internetu, uzależnienie od komputera)

NASK

Naukowa i Akademicka Sieć Komputerowa prowadzi działalność naukową i badawczo-wdrożeniową w dziedzinie sieci teleinformatycznych. W strukturach instytutu działa zespół CERT Polska powołany w celu reagowania na zdarzenia naruszające bezpieczeństwo w sieci internet. NASK prowadzi także rejestr domeny „.pl", a jako operator telekomunikacyjny oferuje innowacyjne rozwiązania teleinformatyczne. Ważną rolę pełni również działalność edukacyjna i popularyzacja. W Akademii NASK prowadzone są szkolenia dla firm i instytucji ze szczególnym uwzględnieniem tematyki bezpieczeństwa ICT. Od lat realizowane są projekty promujące bezpieczne korzystanie z nowych technologii i internetu wśród dzieci i młodzieży. Od 2005 roku NASK jest koordynatorem Polskiego Centrum Programu Safer Internet. W ramach PCPSI w NASK funkcjonuje Dyżurnet.pl, punkt kontaktowy, który przyjmuje zgłoszenia dotyczące nielegalnych treści w internecie.

(bezpieczny internet, Dyżurnet.pl, CERT Polska, bezpieczeństwo dzieci w sieci, domena, .pl)

Netbook

Mały, przenośny komputer osobisty, zazwyczaj lżejszy od laptopa. Przeznaczony jest głównie do przeglądania internetu, aplikacji online, pracy w podróży.

(nowe technologie, urządzenia mobilne, komputer osobisty)

Netykieta

Zbiór zasad określający właściwe zachowania w internecie np.: (nie pisania wielkimi literami – co jest synonimem krzyku).

(regulamin, moderator, moderacja, serwis społecznościowy, fora dyskusyjne, hejt, hejting, flejm, mowa nienawiści, trollowanie, rolling, troll)

Newsletter

Elektroniczna forma biuletynu, czasopisma rozsyłanego za pomocą poczty elektronicznej do prenumeratorów.

(komunikacja internetowa, poczta elektroniczna, Web 2.0, nowe technologie)

Nick

Nazwa użytkownika pozwalająca na logowanie się do różnych usług internetowych bez upubliczniania swojego imienia/nazwiska

(nazwa użytkownika, username)

Ochrona rodzicielska

Zobacz: filtr rodzicielski

Online

Pierwotnie on-line z ang. co znaczy: na linii – zwykle status osoby, serwera lub innego podmiotu związanego z dostępem do internetu, który informuje o dostępności – aktywności. Przeciwieństwem trybu online jest tryb offline.

(na linii, aktywny w sieci, offline, surfować)

Open source

Odłam ruchu wolnego oprogramowania, który proponuje nazwę open source software jako alternatywną dla free software, głównie z przyczyn praktycznych, a nie filozoficznych. Otwarte oprogramowanie to oprogramowanie, którego licencja pozwala na legalne i nieodpłatne kopiowane, zarówno kodu wynikowego jak i źródłowego oraz na dowolne modyfikacje kodu źródłowego.

(free software, open source movement, free software, otwarte oprogramowanie)

Palmtop

Bardzo mały, przenośny komputer osobisty (mniejszy od laptopa, czy też netbooka), który bez problemu mieści się w dłoni lub kieszeni. (ang. *palm* – dłoń, *top* – na wierzchu).

(nowe technologie, urządzenia mobilne, komputer kieszonkowy, komputer osobisty, notatnik elektroniczny)

Peer-to-Peer

Model komunikacji w sieci zapewniający wszystkim hostom te same uprawnienia, w odróżnieniu od architektury klient – serwer. Najpopularniejszym przykładem modelu P2P są programy do bezpośredniej wymiany plików w internecie.

(P2P computing, program do wymiany plików, host)

Phishing

Metoda oszustwa komputerowego polegająca na podszywaniu się pod inną osobę lub instytucję w celu wyłudzenia danych bądź pozyskania korzyści (np. danych logowania, szczegółów karty kredytowej itp.). Jest to atak oparty na tzw. inżynierii społecznej.

(socjotechnika, wyłudzenie, CERT Polska, cyberbezpieczeństwo, zagrożenia internetowe, bankowość elektroniczna, oszustwo internetowe, przestępczość komputerowa, spam, złośliwe oprogramowanie, zespół abuse)

Poczta elektroniczna

Usługa internetowa służąca do przesyłania wiadomości tekstowych, tzw. listów elektronicznych.

(e-poczta, e-mail, mejl, electronic mail, e-mail)

Polskie Centrum Programu Safer Internet (PCPSI)

Powołane zostało w 2005 r. w ramach programu Komisji Europejskiej Safer Internet, a obecnie funkcjonuje w ramach programu Connecting Europe Facility. Tworzą je Fundacja Dzieci Niczyje (FDN) oraz Naukowa i Akademicka Sieć Komputerowa (NASK). Centrum podejmuje szereg kompleksowych działań na rzecz bezpieczeństwa dzieci i młodzieży korzystających z internetu i nowych technologii. W ramach Polskiego Centrum Programu „Safer Internet" realizowane są 3 projekty: Saferinternet.pl, Pomoc telefoniczna i online - telefon zaufania dla dzieci i młodzieży 116 111 oraz telefon dla rodziców i nauczycieli w sprawach bezpieczeństwa dzieci 800 100 100 oraz Dyżurnet.pl (punkt kontaktowy, tzw. hotline, do którego można anonimowo zgłaszać przypadki występowania w internecie treści zabronionych prawem takich, jak pornografia dziecięca, pedofilia, treści o charakterze rasistowskim i ksenofobicznym).

(NASK, PCPSI, Safer Internet, Connecting Europe Facility, CEF, Dyżurnet.pl, telefon zaufania, tel. 116 111, tel. 800 100 100)

Prawa autorskie

Ogół praw przysługujących autorowi utworu, pomysłu, dzieła upoważniających autora do decydowania o użytkowaniu swojej własności intelektualnej i czerpaniu z niej korzyści finansowych.

(copyright, licencja creative commons, creative commons, CC)

PRO-ANA

Styl życia polegający na dążeniu do doskonałości, za jaką uważa się wychudzoną figurę. *Ana* pochodzi od słowa anoreksja, czyli zaburzenia odżywiania polegającego na patologicznym głodzeniu się. Pro-ana promuje anoreksję i jest bardzo aktywny w Internecie, popularny szczególnie wśród dziewcząt, które odchudzając się zakładają blogi. Znakiem rozpoznawczym jest dekalog pro-ana, który rozpoczyna się hasłem: „Jeśli nie jesteś szczupła, to znaczy, że nie jesteś atrakcyjna", promotorzy pro-ana często posługują się symbolami motyli.

(porcelanowe motyle, szkodliwe treści, ryzykowne zachowania, anoreksja, telefon zaufania, tel. 116 111, tel. 800 100 100)

Profil

Zbiór informacji o użytkowniku budujący jego tożsamość w społecznościach internetowych (na portalach, w komunikatorach, czatach, grach internetowych). Profile, w zależności od zastosowanych ustawień, mogą być publiczne bądź prywatne.

(prywatność online, nick, login, ochrona danych, bezpieczeństwo danych, serwis społecznościowy, portal społecznościowy, blog, vlog, bloger, vloger, profil internetowy)

Program antywirusowy

To programy, które przeciwdziałają programom szpiegującym lub wirusom poprzez skanowanie wszystkich pobieranych przez komputer plików i blokowanie tych, które mogą zagrażać użytkownikowi.

(program antyspyware, antywirus, wirus, cyberbezpieczeństwo, CERT Polska, złośliwe oprogramowanie)

Prywatność

To prawo przysługujące każdemu człowiekowi. W kontekście internetowym mówimy o umiejętności dbania o ochronę swoich danych, właściwego kontrolowania umieszczanych przez siebie oraz publikowanych przez innych informacji na nasz temat.

(ochrona danych, bezpieczeństwo danych, prywatność online, serwis społecznościowy, portal społecznościowy, profil internetowy, dane osobowe, hasło, ryzykowne zachowania, zagrożenia internetowe, cyberprzemoc)

Przeglądarka internetowa

Program komputerowy wykorzystywany do oglądania stron internetowych. Do najbardziej popularnych przeglądarek internetowych należą Google Chrome, Mozilla Firefox, Internet Explorer, Safari. Najnowsze wersje przeglądarek zawierają zaawansowane funkcje kontroli rodzicielskiej.

(przeglądarka www, wyszukiwanie informacji, internet)

Rasizm

Zespół poglądów głoszących tezę o nierówności ludzi, a wynikająca z nich ideologia przyjmuje wyższość jednych ras nad innymi. Przetrwanie rasy „wyższej" staje się wartością nadrzędną i z racji swej wyższości dąży do panowania nad rasami niższymi, a w wersji skrajnej do ich eliminacji. Nawoływanie do nienawiści rasowej oraz znieważanie ze względu na pochodzenie rasowe penalizowane jest w Polsce na podstawie art. 256 i 257 kk.

(Dyżurnet.pl, hotline, nielegalne treści, szkodliwe treści, mowa nienawiści, hejt, hate speech, moderacja, moderator, administrator, zespół abuse)

Sekstortion

Forma wykorzystania seksualnego, którego celem jest pozyskanie materiałów pornograficznych lub usług seksualnych na drodze szantażu wobec ofiary. Często sprawca szantażu pozyskuje materiały pronograficzne ofiary w wyniku sekstingu i zmusza ofiarę do przesłania kolejnych materiałów lub poddania się aktom seksualnym.

(prywatność online, sextortion, ochrona danych, seksting, cyberprzemoc, treści pornograficzne, ryzykowne zachowania, telefon zaufania, tel. 116 111, tel. 800 100 100, materiały przedstawiające seksualne wykorzystywanie dziecka, CSAM, hotline, Dyżurnet.pl)

Serwer

Potocznie jest to komputer udostępniający zasoby innym komputerom podłączonym do sieci. Zasobami mogą być między innymi strony internetowe (serwer WWW), poczta e-mail (serwer pocztowy), bazy danych (serwer baz danych).

(serwer www, WWW, serwer pocztowy, sieć, serwerownia, internet)

Serwis społecznościowy

Serwis internetowy, który istnieje w oparciu o zgromadzoną wokół niego społeczność internautów. Tworzy tak zwane media społecznościowe (ang. *social media*). Najpopularniejszy portal społecznościowy obecnie to Facebook, wczesniej Myspace, a w Polsce nk.pl (dawniej nasza-klasa.pl)

(portal społecznościowy, profil internetowy, prywatność online, social media, Web 2.0, Facebook, nk.pl)

Sexting

Zjawisko dotyczące przesyłania za pomocą komputera oraz urządzeń mobilnych z dostępem do internetu swoich zdjęć, wiadomości o seksualnym charakterze lub też samodzielnie wykonanych materiałów video. Problem sextingu obejmuje wszystkie grupy wiekowe, jednak proceder ten jest najbardziej popularny i niebezpieczny wśród nastolatków (wynika to z popularności i umiejętności korzystania z nowych technologii, a także typowego dla okresu dojrzewania zainteresowania sprawami seksualnymi). Zagrożenie sextingu związane jest z niebezpieczeństwem upublicznienia i rozpowszechniania prywatnego materiału przez odbiorców np. erotycznego pokazu. W niektórych przypadkach wytwarzanie, przesyłanie lub publiczne udostępnianie może być nielegalne (patrz: pornografia dziecięca i cyberprzemoc) a czasem może nawet prowadzić do pozyskiwania korzyści materialnych związanych ze sprzedażą materiałów.

(erotyka, erotyka dziecięca, treści pornograficzne, pornografia dziecięca, cyberprostytucja, niebezpieczne zachowania, ryzykowne zachowania, cyberprzemoc, Dyżurnet.pl, tel. 116 111, tel. 800 100 100, telefon zaufania)

Smartfon

Przenośne urządzenie telefoniczne łączące w sobie funkcje telefonu komórkowego i komputera kieszonkowego. Pierwsze smartfony powstały pod koniec lat 90., a obecnie łączą funkcje telefonu komórkowego, poczty elektronicznej, przeglądarki sieciowej, pagera, GPS, jak również cyfrowego aparatu fotograficznego i kamery wideo.

(smartphone, telefon komórkowy, urządzenia mobilne, nowe technologie, wyszukiwarka)

Spam

Niechciane lub niepotrzebne wiadomości elektroniczne.

(poczta elektroniczna, CERT Polska, zagrożenia internetowe, serwisy społecznościowe, wirus, przestępczość komputerowa, phishing, robak, koń trojański, trojan, malware, złośliwe oprogramowanie, zespół abuse, oszustwo internetowe)

Stalking

Zobacz: cyberstalking

Strona internetowa

Dokument HTML udostępniony w internecie przez serwer WWW. Po stronie urządzenia dotępowego użytkownika, strona WWW jest otwierana i wyświetlana za pomocą przeglądarki internetowej.

(strona www, web page, witryna internetowa, domena)

Surfowanie

Analogiczna czynność do przełączania kanałów w telewizji. Przeglądanie stron internetowych w poszukiwaniu ciekawych dla nas programów lub informacji.

(surfing, wyszukiwanie informacji, przeglądarka www, przeglądarka internetowa, internet, sieć)

Tablet

Przenośny komputer większy niż smartfon, którego główną właściwością jest posiadanie dużego ekranu z zastosowaną technologią Multi-Touch. Tablety nie posiadają fizycznej klawiatury, użytkownik posługuje się klawiaturą wirtualną, dotykając ekran bezpośrednio.

(ipad, komputer, nowe technologie, urządzenia mobilne)

Tablica multimedialna

Inaczej tablica interaktywna, urządzenie, które przypomina duży biały monitor lub tablicę, która reaguje na dotyk i umożliwia współdziałanie z podłączonym do niej komputerem oraz projektorem multimedialnym. W zależności od technologii, w której tablica została wykonana, można używać specjalnego pióra lub dłoni. Osoba korzystająca z tablicy może za jej pomocą obsługiwać dowolny program uruchomiony w komputerze. Interaktywna tablica zazwyczaj dysponuje też własnym specjalistycznym oprogramowaniem, które umożliwia przygotowanie zasobów do wykorzystania podczas lekcji czy prezentacji.

(tablica interaktywna, edukacja medialna, kompetencje medialne, media literacy, umiejętności elektroniczne)

Telefon komórkowy

Telefon działający w oparciu o telefonię komórkową, czyli urządzenie telekomunikacyjne umożliwiające bezprzewodowe połączenia pomiędzy użytkownikami.

(komórka, urządzenie mobilne)

Telefon zaufania

Linia telefoniczna przeznaczona do świadczenia pomocy, wsparcia osobom potrzebującym przez osoby przygotowane do udzielania takiej pomocy – mogą to być psychologowie, terapeuci itp. Telefon zaufanie może być przeznaczony dla osób z np.: problemem dotyczącym nadużywania środków odurzających, ofiar przemocy itp.

(tel. 116 111)

Telefon zaufania dla dzieci i młodzieży 116 111

Ogólnopolski, bezpłatny i anonimowy telefon zaufania przeznaczony dla dzieci i młodzieży, czynny 7 dni w tygodniu od godziny 12 do 22. Dostępny jest pod zharmonizowanym w Europie numerem 116 111, połączenie nie jest widoczne na rachunkach ani na billingach większości sieci. Numer ma docelowo działać we wszystkich krajach Unii Europejskiej.

(telefon zaufania, tel. 116 111)

Treści nielegalne

Treści internetowe, które łamią prawo krajowe lub namawiają do jego łamania. Najczęściej są to treści szerzące rasizm, faszyzm i ksenofobię oraz treści pornograficzne z udziałem osoby małoletniej, ale odnosić się mogą do każdej informacji, której upublicznienie może być nielegalne (np. dane osobowe).

(zagrożenia internetowe, Dyżurnet.pl, hotline, CERT Polska, prywatność online, treści pornograficzne, moderacja, administrator, kontrola rodzicielska, filtr rodzicielski, regulamin, ryzykowne zachowania, materiały przedstawiające seksualne wykorzystywanie dziecka, CSAM)

Treści pornograficzne

W polskim prawie nie istnieje definicja terminu „treści pornograficzne". Ocena zależy więc od sądu, który może powołać w tej sprawie biegłego (np. seksuologa). Definiując termin „treści pornograficzne" lub „pornografia" zwraca się uwagę na element subiektywny (czyli na zamiar twórcy) oraz obiektywny (czyli odnoszący się do samej treści oraz skutków jej odbioru). Polski Kodeks karny reguluje obrót niektórymi rodzajami materiałów pornograficznych. Jednym z najważniejszych z punktu widzenia ochrony dzieci i młodzieży przed szkodliwymi treściami jest art. 200 §3, który zabrania prezentowania treści pornograficznych dzieciom do lat 15.

(zagrożenia internetowe, moderacja, administrator, kontrola rodzicielska, filtr rodzicielski, regulamin, Dyżurnet.pl, hotline, materiały przedstawiające seksualne wykorzystywanie dziecka, CSAM)

Treści szkodliwe

Treści szkodliwe to takie, które mogą wywołać negatywne emocje u odbiorcy, treści promujące niebezpieczne zachowania i dlatego są nieodpowiednie dla dzieci. Do szkodliwych treści zalicza się m.in: treści obrazujące przemoc, obrażenia fizyczne bądź śmierć (np. zdjęcia/filmy prezentujące ofiary wypadków), okrucieństwo wobec zwierząt, treści nawołujące do samookaleczeń lub samobójstw, zachowań szkodliwych dla zdrowia czy zażywanie niebezpiecznych substancji; treści dyskryminacyjne, zawierające postawy wrogości a nawet nienawiści; treści pornograficzne.

Treści te nie muszą być zabronione przez prawo krajowe lub regulamin serwisu internetowego, jednak zaleca się, aby treści które nie są przeznaczone dla osób poniżej 18 roku życia opatrzone były ostrzeżeniem oraz wyraźną informacją o ich charakterze.

(zagrożenia internetowe, moderacja, szkodliwe treści, administrator, kontrola rodzicielska, filtr rodzicielski, regulamin, Dyżurnet.pl, hotline, ryzykowne zachowania)

Trollowanie

Nieprzyjazne zachowania wobec innych użytkowników internetu, które mają na celu przeszkodzenie w prowadzonej dyskusji.

(troll, netykieta, fora dyskusyjne, serwisy społecznościowe, czat, chat, moderator, moderacja, hejt, hejtowanie, szkodliwe treści)

Troll parenting

Publikowanie przez rodziców i opiekunów w internecie wizerunku dziecka w ośmieszającym czy wręcz kompromitującym kontekście.

(cyberprzemoc, ośmieszenie, prywatność dziecka, prywatność online, ryzykowne zachowania, szkodliwe treści)

Urządzenie mobilne

Przenośne urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie oraz wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią.

(tablet, smartfon, komputer przenośny, notebook, netbook, palmtop, laptop, wifi)

Usługa geolokalizacji

Zobacz: geolokalizacja

Uwodzenie dzieci online

Proces, podczas którego dorosły przygotowuje dziecko do wykorzystania seksualnego (również do pozyskania materiałów pornograficznych).

(niebezpieczne kontakty, treści pornograficzne, ryzykowne zachowania, telefon zaufania, tel. 116 111, tel. 800 100 100, child grooming, erotyka dziecięca, materiały przedstawiające seksualne wykorzystywanie dziecka, CSAM)

Uzależnienie

Zobacz: nadmierne korzystanie z internetu.

Vlog

Rodzaj bloga internetowego, którego zasadniczą treść stanowią pliki filmowe (VODcast) publikowane przez autora w kolejności chronologicznej. Pliki udostępniane są do odtwarzania w technologii video-streamingu lub do pobrania na komputer użytkownika – gościa i widza wideobloga. Vlogerzy publikują swoje filmy głównie w serwisie YouTube oraz Dailymotion.

(videoblog, blog, wideoblog, vloger, Web 2.0, bloger)

Web 2.0

Potoczne określenie serwisów internetowych, powstałych po 2001, w których działaniu podstawową rolę odgrywa treść generowana przez użytkowników danego serwisu.

(serwis społecznościowy, portal społecznościowy, użytkownik internetu, blog, bloger, vlog, vloger, mikroblog)

Wi-Fi

Potoczne określenie zestawu standardów stworzonych do budowy bezprzewodowych sieci komputerowych. Technologia wifi umożliwia korzystanie z internetu bez dodatkowej infrastruktury posiadaczom urządzeń mobilnych (bez użycia transferu danych z pakietów od operatorów komórkowych). Obecnie darmowy dostęp wifi udostępniany jest przez hotele, kawiarnie restaurację, jak również w publicznej przestrzeni miejskiej.

(sieć bezprzewodowa, internet mobilny, urządzenia mobilne, sieć, internet, wifi)

Wikipedia

Wielojęzyczna encyklopedia internetowa działająca w oparciu o zasadę otwartej treści. Funkcjonuje wykorzystując oprogramowanie MediaWiki wywodzące się z koncepcji WikiWikiWeb, umożliwiające edycję każdemu użytkownikowi odwiedzającemu stronę i aktualizację jej treści.

(wikiwikiweb, wolna encyklopedia, Web 2.0, wyszukiwanie informacji)

Wirtualna prostytucja

Zobacz: Cyberprostytucja.

Wirus

Program komputerowy posiadający zdolność powielania się, tak jak prawdziwy wirus, stąd jego nazwa. Wirus do swojego działania potrzebuje i wykorzystuje system operacyjny, aplikacje oraz zachowanie użytkownika komputera.

(zagrożenia internetowe, CERT Polska, antywirus, program antywirusowy, spam, oszustwo internetowe, oszustwo komputerowe, cyberzagrożenia)

Wykluczenie cyfrowe

Termin stosowany do określenia różnicy między tymi osobami i społeczeństwami, które mają dostęp do technologii informacyjnych, a tymi które takiego dostępu nie mają.

(przepaść cyfrowa, cyfrowy imigrant, cyfrowy tubylec, różnica pokoleniowa)

Wyszukiwarka

Narzędzie internetowe pozwalające na przeszukiwanie stron internetowych pod kątem danej informacji, którą chcemy znaleźć np.: google, bingo.

(przeglądarka internetowa, przeglądarka www, infoholizm, surfowanie, sieć, internet)

Zagrożenia internetowe

Różnego typu niebezpieczeństwa, zarówno technologiczne jak również społeczne, na które narażony jest użytkownik internetu.

(cyberprzestępczość, cyberprzemoc, mowa nienawiści, wirus)

Zespół Abuse

Dedykowany zespół pracowników zajmujący się bezpieczeństwem danej witryny lub serwisu internetowego.

(zespół ds. przeciwdziałania nadużyciom, moderacja, moderator, administrator, Dyżurnet.pl, CERT Polska)

Zniesławienie

Występek polegający na pomówieniu innej osoby, grupy osób, instytucji, osoby prawnej lub jednostki organizacyjnej nie mającej osobowości prawnej o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności. Zniesławienie, pomówienie (art. 212 kk) jest przestępstwem ściganym z oskarżenia prywatnego, należy więc z zabezpieczonymi dowodami zgłosić sprawę do prokuratury lub na policję. Treści można zgłosić również do moderacji serwisu wraz z wnioskiem o ich usunięcie.

(cyberprzemoc, zagrożenia internetowe, moderacja, moderator, pomówienie, obmówienie, oszczerstwo, cyberprzestępczość)

Zniewaga

Obraza lub obelga. Polega na znieważaniu gestem, słowem lub obrazem innej osoby. Zniewaga (art. 216 kk) jest przestępstwem ściganym z oskarżenia prywatnego należy więc z zabezpieczonymi dowodami zgłosić sprawę do prokuratury lub na policję (zobacz: Cyberprzemoc). Treści można zgłosić również do moderacji serwisu wraz z wnioskiem o ich usunięcie.

(cyberprzemoc, zagrożenia internetowe, cyberprzestępczość, moderacja, moderator, obraza, obelga)

Załącznik nr 2. Słownik najważniejszych pojęć związanych z użytkowaniem sieci opracowany został w projekcie ramach zadania nr 1.: *„Integracja istniejących materiałów na temat bezpiecznego korzystania z Internetu”*. Więcej informacji na stronie projektu: www.bezpiecznyinternet.edu.pl.

Opracowanie autorstwa: Julia Gursztyn, Martyna Różycka, Anna Rywczyńska

Załącznik nr 3. Przykładowa procedura samooceny placówki w zakresie zapewniania bezpieczeństwa online

- **Ankieta dotycząca infrastruktury**

  Zaleca się aby placówka cyklicznie dokonywała przegląd poziomu bezpieczeństwa. W efekcie, raport z takiego przeglądu stanowił by potwierdzenie (deklaratywne) spełniania wymagań poziomu minimalnego,podwyższonego bądź profesjonalnego.

  Na poziomie minimalnym przegląd dokonywany byłby raz do roku.

  Na poziomie podwyższonym oraz profesjonalnym - dwa razy do roku.

- **Działania audytowe**

  Na poziomie profesjonalnym, oprócz wewnętrznego przeglądu dwa razy do koku zaleca się dokonywania zewnętrznego audytu bezpieczeństwa – raz na dwa lata. Powinien temu towarzyszyć techniczny audyt, o którym mowa w opisie charakterystyki poziomu profesjonalnego.

  W ramach dokonywania wewnętrznych przeglądów należy oprócz potwierdzenia istnienia odpowiednich elementów infrastruktury zawrzeć także informację o wydatkach poniesionych na infrastrukturę (w tym na elementy związane z bezpieczeństwem IT, sposób administrowania infrastrukturą), zauważonych incydentach i zagrożeniach oraz podjętych środkach zaradczych.

- **Procedura postępowania w przypadku zauważonych braków**

  Niewystarczający budżet na bezpieczną infrastrukturę IT, brak zasobów technicznych (jeśli występuje jako wniosek z raportu w dwóch kolejnych raportach) powinien być przedmiotem działań strukturalnych, takich jak: zewnętrzna analiza problemu oraz działania w celu zapewnienia wyższego budżetu bądź optymalizacji wydatkowanych środków przez placówkę.

Załącznik nr 4. Zalecenia odnośnie treści polityki bezpieczeństwa i regulaminów korzystania z infrastruktury sieciowej

Polityka bezpieczeństwa

Polityka bezpieczeństwa IT powinna być oficjalnym dokumentem, zatwierdzonym przez kierownika danej placówki. Powinna opisywać podejście kierownictwa do zapewniania odpowiedniego poziomu bezpieczeństwa poprzez: stosowanie zabezpieczeń technicznych, istnienie regulaminów korzystania z infrastruktury IT, procesów administrowania infrastrukturą i monitorowania stanu bezpieczeństwa, procedur reagowania na pojawiające się incydenty zagrażające lub naruszające bezpieczeństwo, a także powinna odnosić się do ustawowych obowiązków zapewniania bezpieczeństwa (np. ustawa o ochronie danych osobowych).

Zalecenia odnoście treści dokumentu polityki bezpieczeństwa

Dokument powinien zawierać wyłącznie przydatne informacje. Należy unikać tworzenia, bądź akceptowania dokumentów, których jedyną rolą będzie spełnienie formalnego obowiązku posiadania polityki. Dokument polityki zatwierdza dyrektor szkoły i ponosi odpowiedzialność za wdrażanie i przestrzeganie polityki. Rekomenduje się, aby dokument polityki był wzorowany na standardzie PN-ISO/IEC 27001:2013.

Zalecenia odnośnie dostawcy Internetu – wytyczne do treści polityki:

- Czy dostawca jest na liście UKE – rejestr przedsiębiorców telekomunikacyjnych (https://www.uke.gov.pl/marta/?p=2)?
- Jakie zapewnia gwarancje niezawodności (SLA)?
- Czy istnieją zapisy co do postępowania w przypadkach zagrażających bezpieczeństwu: kontakt e-mail, telefoniczny, formularz na stronie?

Zalecenia odnośnie infrastruktury:

W zależności od założonego poziomu bezpieczeństwa (minimalny, podwyższony, profesjonalny) należy udokumentować elementy architektury IT, które są wykorzystywane (wraz z funkcjami bezpieczeństwa jakie pełnią). Każdy z elementów powinien mieć przypisanego opiekuna bądź administratora. W procedurach zakupowych sprzętu i usług należy uwzględnić wymogi bezpieczeństwa adekwatne do założonego poziomu bezpieczeństwa IT placówki.

Zalecenia odnośnie użytkowania infrastruktury i zasobów

W polityce powinno znaleźć się odwołanie do regulaminu korzystania z sieci. Regulamin zaś powinien odpowiednio, szczegółowo opisywać zasady, które można nazwać zasadami higieny korzystania z infrastruktury IT oraz działania uprawnione, a także niezgodne z regulaminem.

Ewaluacja i zmiany

Polityka bezpieczeństwa powinna zakładać cykliczną ewaluację poziomu bezpieczeństwa (załącznikiem powinna być ankieta ewaluacyjna), a także tryb wprowadzania modyfikacji.

Podnoszenie świadomości bezpieczeństwa

Dokument polityki powinien opisywać konkretne sposoby podnoszenia świadomości bezpieczeństwa w odniesieniu do kadry placówki, ale też uczniów.

Szkolenia i ich częstotliwość

Zaleca się, by szkolenia dla kadry odbywały się co najmniej raz w roku. Jeśli chodzi o uczniów, należy w polityce opisać w jaki sposób informacje związane z bezpieczeństwem będą im przekazywane (na lekcjach, stronie startowej portalu szkolnego, plakatach), a także w jaki sposób szkoła będzie uczestniczyła w kampaniach związanych z bezpieczeństwem (np. Dzień Bezpiecznego Internetu, Europejski Miesiąc Bezpieczeństwa Cyberprzestrzeni, itp.).

Załącznik nr 5. Zalecenia odnośnie regulaminu korzystania z sieci

Regulamin powinien odpowiednio szczegółowo opisywać zasady tzw. higieny korzystania z infrastruktury IT i działania uprawnione oraz niezgodne z regulaminem. Regulamin powinien też wskazywać procedury postepowania, a także pewien zestaw sankcji, w przypadku łamania regulaminu. Zbiór zasad można podzielić na dwa dokumenty: regulamin dla kadry oraz regulamin dla uczniów.

W ramach zapewnienia higieny bezpieczeństwa – w regulaminie należy zawrzeć zalecenia do stosowania przez uczniów i nauczycieli podstawowych zasad bezpieczeństwa przy korzystaniu z systemów cyberprzestrzeni (jako element profilaktyki) odnośnie takich zagadnień jak:

- polityka haseł i jej stosowanie,
- uwierzytelnianie dwuskładnikowe jako zalecana forma podwyższonego bezpieczeństwa,
- bezpieczne zachowania w codziennej praktyce,
- nie klikanie w nieznane linki,
- nie otwieranie podejrzanych załączników,
- stosowanie kopii zapasowych off-line (w miejscu innym niż oryginał),
- zgłaszanie zagrożeń i incydentów.

Reagowanie na pojawiające się zagrożenia i zdarzenia jest istotnym elementem postępowania użytkownika.

- Jest konieczne aby w placówce istniała procedura reagowania na zagrożenia techniczne i incydenty. Powinna ona być spójna z procedurą zgłaszania cyberzagrożeń społecznych. Mamy tu do czynienia ze zgłaszaniem zauważonych zagrożeń czy naruszeń bezpieczeństwa przez użytkowników do określonego punktu w placówce. Następnie mogą nastąpić dalsze etapy reagowania w postaci zgłoszenia incydentu przez uprawnione osoby danej placówki oświatowej do organów ścigania, zespołów reagowania typu CERT, w szczególności do zespołu bezpieczeństwa dostawcy Internetu.
- Istotnym elementem procedury powinna być dokumentacja: rejestrowanie wszystkich przypadków, zabezpieczanie śladów i dowodów, dokonanie opisu zdarzenia.
- Użytkownicy powinni być cyklicznie edukowani w zakresie reakcji na incydenty oraz trybach zgłaszania – zgodnego z procedurą.
- Odpowiednie służby w placówce powinny zapewnić wyciągnięcie wniosków z pojawiających się zdarzeń zagrażającym bezpieczeństwu IT, rekomendowanie działań profilaktycznych.
- Kierownictwo placówki powinno być informowane na bieżąco o poważnych incydentach bezpieczeństwa oraz powinno otrzymywać okresowe raporty ze wszystkich przypadków naruszeń.

Załącznik nr 6. Dokumentacja procedury interwencyjnej zastosowanej w placówce

Data

DOKUMENTACJA PROCEDURY INTERWENCYJNEJ ZASTOSOWANEJ W PLACÓWCE

Nr ___

1. Sposób zgłoszenia

□ Pośredni

□ Bezpośredni

.....
.....(możliwość szczegółowego opisu)

2. Data przyjęcia zgłoszenia: .....

3. Osoby uczestniczące

.....
.....

4. Opis przebiegu zdarzenia

.....
.....
.....

5. Zabezpieczone dowody

.....
.....
.....

6. Zastosowane środki wychowawcze, dyscyplinarne, rekomendacje

.....
.....
.....

7. Plan monitoringu zdarzenia.

……
……
……

Załączniki

Przykładowe załączniki:

- *Notatki z rozmów z uczestnikami zdarzenia*
- *Zrzuty ekranu z dn. …*
- *Treść korespondencji SMS/email*
- *Kopia wniosków/zgłoszeń do Sądu Rodzinnego/ Policji*

Opracowanie dokumentacji zespół w składzie:

……

……

……

……

……

……

Załącznik nr 7. Przepisy regulujące zasady współpracy placówek oświatowych z policją, sądem rodzinnym, poradniami psychopedagogicznymi

Ogólnym aktem prawnym jest Ustawa z dnia 26 10. 1982 r. o postępowaniu w sprawach nieletnich.

Współpraca z Policją

Ustawa z dnia 26 10. 1982 r. o postępowaniu w sprawach nieletnich:

Art. 4. § 1. Każdy, kto stwierdzi istnienie okoliczności świadczących o demoralizacji nieletniego, w szczególności naruszanie zasad współżycia społecznego, popełnienie czynu zabronionego, systematyczne uchylanie się od obowiązku szkolnego lub kształcenia zawodowego, używanie alkoholu lub innych środków w celu wprowadzenia się w stan odurzenia, uprawianie nierządu, włóczęgostwo, udział w grupach przestępczych, ma społeczny obowiązek odpowiedniego przeciwdziałania temu, a przede wszystkim zawiadomienia o tym rodziców lub opiekuna nieletniego, szkoły, sądu rodzinnego, **Policji** lub innego właściwego organu.

§2. Każdy, dowiedziawszy się o popełnieniu czynu karalnego przez nieletniego, ma społeczny obowiązek zawiadomić o tym sąd rodzinny lub policję.

§ 3. Instytucje państwowe i organizacje społeczne, które w związku ze swą działalnością dowiedziały się o popełnieniu przez nieletniego czynu karalnego ściganego z urzędu, są obowiązane niezwłocznie zawiadomić o tym sąd rodzinny lub policję oraz przedsięwziąć czynności niecierpiące zwłoki, aby nie dopuścić do zatarcia śladów i dowodów popełnienia czynu.

Dodatkowo:

Ustawa z dnia 6 kwietnia 1990 r. **o Policji**

Art. 1 ust. 1 pkt. 3 Do podstawowych zadań Policji należą:

3) inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi;

Policja jest uprawiona do podejmowania programów, kampanii, współpracy ze szkołami i innymi jednostkami organizacyjnymi.

Współpraca z sądem rodzinnym

1) Ustawa z dnia 26 10. 1982 r. o postępowaniu w sprawach nieletnich:

Art. 4. § 1. Każdy, kto stwierdzi istnienie okoliczności świadczących o demoralizacji nieletniego, w szczególności naruszanie zasad współżycia społecznego, popełnienie czynu zabronionego, systematyczne uchylanie się od obowiązku szkolnego lub kształcenia zawodowego, używanie alkoholu lub innych środków w celu wprowadzenia się w stan odurzenia, uprawianie nierządu, włóczęgostwo, udział w grupach przestępczych, ma społeczny obowiązek odpowiedniego przeciwdziałania temu, a przede wszystkim zawiadomienia o tym rodziców lub opiekuna nieletniego, szkoły, **sądu rodzinnego,**

Policji lub innego właściwego organu.

2. Każdy, dowiedziawszy się o popełnieniu czynu karalnego przez nieletniego, ma społeczny obowiązek zawiadomić **o tym sąd rodzinny** lub Policję.

§ 3. Instytucje państwowe i organizacje społeczne, które w związku ze swą działalnością dowiedziały się o popełnieniu przez nieletniego czynu karalnego ściganego z urzędu, są obowiązane niezwłocznie zawiadomić **o tym sąd rodzinny** lub Policję oraz przedsięwziąć czynności niecierpiące zwłoki, aby nie dopuścić do zatarcia śladów i dowodów popełnienia czynu.

Współpraca z poradnią psychologiczno-pedagogiczną

Rozporządzenie Ministra Edukacji Narodowej z dnia 1 lutego 2013 r. w **sprawie szczegółowych zasad działania publicznych poradni psychologiczno-pedagogicznych, w tym publicznych poradni specjalistycznych (Dz. U. z dnia 13 lutego 2013 r.)**

Na podstawie art. 71 ust. 1 pkt 2 Ustawy z dnia 7 .09. 1991 r. o systemie oświaty (Dz. U. z 2004 r. Nr 256, poz. 2572, z późn. zm.2)) zarządza się, co następuje:

§ 1. Publiczne poradnie psychologiczno-pedagogiczne, w tym publiczne poradnie specjalistyczne, zwane dalej "poradniami", udzielają dzieciom, od momentu urodzenia, i młodzieży pomocy psychologiczno-pedagogicznej oraz pomocy w wyborze kierunku kształcenia i zawodu, udzielają rodzicom i nauczycielom pomocy psychologiczno-pedagogicznej związanej z wychowywaniem i kształceniem dzieci i młodzieży, a także wspomagają przedszkola, szkoły i placówki w zakresie realizacji zadań dydaktycznych, wychowawczych i opiekuńczych.

§ 2. Do zadań poradni należy:

1) diagnozowanie dzieci i młodzieży;

2) udzielanie dzieciom i młodzieży oraz rodzicom bezpośredniej pomocy psychologiczno-pedagogicznej;

3) realizowanie zadań profilaktycznych oraz wspierających wychowawczą i edukacyjną funkcję przedszkola, szkoły i placówki, w tym wspieranie nauczycieli w rozwiązywaniu problemów dydaktycznych i wychowawczych;

4) organizowanie i prowadzenie wspomagania przedszkoli, szkół i placówek w zakresie realizacji zadań dydaktycznych, wychowawczych i opiekuńczych.

§ 8. 1. Pomoc psychologiczno-pedagogiczna udzielana bezpośrednio dzieciom i młodzieży oraz rodzicom polega w szczególności na:

1) prowadzeniu terapii dzieci i młodzieży oraz ich rodzin;

2) udzielaniu wsparcia dzieciom i młodzieży wymagającym pomocy psychologiczno-pedagogicznej lub pomocy w wyborze kierunku kształcenia i zawodu oraz planowaniu kształcenia i kariery zawodowej;

3) udzielaniu pomocy rodzicom w rozpoznawaniu i rozwijaniu indywidualnych potrzeb rozwojowych i edukacyjnych oraz indywidualnych możliwości psychofizycznych dzieci i młodzieży oraz w rozwiązywaniu problemów edukacyjnych i wychowawczych.

2. Pomoc, o której mowa w ust. 1, jest udzielana w szczególności w formie:

1) indywidualnych lub grupowych zajęć terapeutycznych dla dzieci i młodzieży;

2) terapii rodziny;

3) grup wsparcia;

4) prowadzenia mediacji;

5) interwencji kryzysowej;

6) warsztatów;

7) porad i konsultacji;

8) wykładów i prelekcji;

9) działalności informacyjno-szkoleniowej.

§ 9. 1. Realizowanie przez poradnie zadań, o których mowa w § 2 pkt 3, polega w szczególności na:

1) udzielaniu nauczycielom, wychowawcom grup wychowawczych lub specjalistom, o których mowa w § 5 ust. 2, pomocy w:

a) rozpoznawaniu indywidualnych potrzeb rozwojowych i edukacyjnych oraz możliwości psychofizycznych dzieci i młodzieży, w tym w rozpoznawaniu ryzyka wystąpienia specyficznych trudności w uczeniu się u uczniów klas I-III szkoły podstawowej,

b) planowaniu i realizacji zadań z zakresu doradztwa edukacyjno-zawodowego;

c) rozwijaniu zainteresowań i uzdolnień uczniów;

2) współpracy z przedszkolami, szkołami i placówkami w udzielaniu i organizowaniu przez przedszkola, szkoły i placówki pomocy psychologiczno-pedagogicznej oraz opracowywaniu i realizowaniu indywidualnych programów edukacyjno-terapeutycznych oraz indywidualnych programów zajęć rewalidacyjno-wychowawczych;

3) współpracy, na pisemny wniosek dyrektora przedszkola, szkoły lub placówki lub rodzica dziecka niepełnosprawnego albo pełnoletniego ucznia niepełnosprawnego, w określeniu niezbędnych do nauki warunków, sprzętu specjalistycznego i środków dydaktycznych, w tym wykorzystujących technologie informacyjno-komunikacyjne, odpowiednich ze względu na indywidualne potrzeby rozwojowe i edukacyjne oraz możliwości psychofizyczne dziecka niepełnosprawne- go albo pełnoletniego ucznia niepełnosprawnego;

4) udzielaniu nauczycielom, wychowawcom grup wychowawczych lub specjalistom, o których mowa w § 5 ust. 2, pomocy w rozwiązywaniu problemów dydaktycznych i wychowawczych;

5) podejmowaniu działań z zakresu profilaktyki uzależnień i innych problemów dzieci i młodzieży;

6) prowadzeniu edukacji dotyczącej ochrony zdrowia psychicznego wśród dzieci i młodzieży, rodziców i nauczycieli;

7) udzielaniu, we współpracy z placówkami doskonalenia nauczycieli i bibliotekami pedagogicznymi, wsparcia merytorycznego nauczycielom, wychowawcom grup wychowawczych i specjalistom, o których mowa w § 5 ust. 2.

2. Zadania, o których mowa w ust. 1, są realizowane w szczególności w formie:

1) porad i konsultacji;

2) udziału w spotkaniach odpowiednio nauczycieli, wychowawców grup wychowawczych i specjalistów, o których mowa w § 5 ust. 2;

3) udziału w zebraniach rad pedagogicznych;

4) warsztatów;

5) grup wsparcia;

6) wykładów i prelekcji;

7) prowadzenia mediacji;

8) interwencji kryzysowej;

9) działalności informacyjno-szkoleniowej;

10) organizowania i prowadzenia sieci współpracy i samokształcenia dla nauczycieli, wychowawców grup wychowawczych i specjalistów, o których mowa w § 5 ust. 2, którzy w zorganizowany sposób współpracują ze sobą w celu doskonalenia swojej pracy, w szczególności poprzez wymianę doświadczeń.

Ustawa z dnia 9.06.2011 r. o wspieraniu rodziny i systemie pieczy zastępczej

Art. 2. 1. Wspieranie rodziny przeżywającej trudności w wypełnianiu funkcji opiekuńczo-wychowawczych to zespół planowych działań mających na celu przywrócenie rodzinie zdolności do wypełniania tych funkcji.

2. System pieczy zastępczej to zespół osób, instytucji i działań mających na celu zapewnienie czasowej opieki i wychowania dzieciom w przypadkach niemożności sprawowania opieki i wychowania przez rodziców.

3. Jednostkami organizacyjnymi wspierania rodziny i systemu pieczy zastępczej są jednostki organizacyjne jednostek samorządu terytorialnego wykonujące zadania w zakresie wspierania rodziny i systemu pieczy zastępczej, placówki wsparcia dziennego, organizatorzy rodzinnej pieczy zastępczej, placówki opiekuńczo-wychowawcze, regionalne placówki opiekuńczo-terapeutyczne, interwencyjne ośrodki preadopcyjne, ośrodki adopcyjne oraz podmioty, którym zlecono realizację zadań z zakresu wspierania rodziny i systemu pieczy zastępczej.

Art. 3. 1. Obowiązek wspierania rodziny przeżywającej trudności w wypełnianiu funkcji opiekuńczo-wychowawczych oraz organizacji pieczy zastępczej, w zakresie ustalonym ustawą, spoczywa na jednostkach samorządu terytorialnego oraz na organach administracji rządowej.

2. Obowiązek, o którym mowa w ust. 1, jednostki samorządu terytorialnego oraz organy administracji rządowej realizują w szczególności we współpracy ze środowiskiem lokalnym, sądami i ich organami pomocniczymi, Policją, instytucjami oświatowymi, podmiotami leczniczymi, a także kościołami i związkami wyznaniowymi oraz organizacjami społecznymi.

3. Zadania z zakresu wspierania rodziny i systemu pieczy zastępczej są realizowane zgodnie z zasadą pomocniczości, zwłaszcza gdy przepisy ustawy przewidują możliwość zlecania realizacji tych zadań przez organy jednostek samorządu terytorialnego

Obowiązki (uprawnienia) dyrektora jako osoby kierującej placówką:

2) Ustawa z dnia 26 10. 1982 r. o postępowaniu w sprawach nieletnich:

Art. 4. § 1. Każdy, kto stwierdzi istnienie okoliczności świadczących o demoralizacji nieletniego, w szczególności naruszanie zasad współżycia społecznego, popełnienie czynu zabronionego, systematyczne uchylanie się od obowiązku szkolnego lub kształcenia zawodowego, używanie alkoholu lub innych środków w celu wprowadzenia się w stan odurzenia, uprawianie nierządu, włóczęgostwo, udział w grupach przestępczych, ma społeczny obowiązek odpowiedniego przeciwdziałania temu, a przede wszystkim zawiadomienia o tym rodziców lub opiekuna nieletniego, szkoły, sądu rodzinnego, Policji lub innego właściwego organu.

2. Każdy, dowiedziawszy się o popełnieniu czynu karalnego przez nieletniego, ma społeczny obowiązek zawiadomić o tym sąd rodzinny lub Policję.

§ 3. Instytucje państwowe i organizacje społeczne, które w związku ze swą działalnością dowiedziały się o popełnieniu przez nieletniego czynu karalnego ściganego z urzędu, są obowiązane niezwłocznie zawiadomić o tym sąd rodzinny lub Policję oraz przedsięwziąć czynności niecierpiące zwłoki, aby nie dopuścić do zatarcia śladów i dowodów popełnienia czynu.

3) Ustawa z dnia z 7.09.1991 r. o systemie oświaty:

Art. 4a. (40) Szkoły i placówki zapewniające uczniom dostęp do Internetu są obowiązane podejmować działania zabezpieczające uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju, w szczególności zainstalować i aktualizować oprogramowanie zabezpieczające.

Art. 39 ust. 2. Dyrektor szkoły lub placówki może, w drodze decyzji, skreślić ucznia z listy uczniów w przypadkach określonych w statucie szkoły lub placówki. Skreślenie następuje na podstawie uchwały rady pedagogicznej, po zasięgnięciu opinii samorządu uczniowskiego.

ust. 2a. Przepis ust. 2 nie dotyczy ucznia objętego obowiązkiem szkolnym. W uzasadnionych przypadkach uczeń ten, na wniosek dyrektora szkoły, może zostać przeniesiony przez kuratora oświaty do innej szkoły.

Art. 39. 1. Dyrektor szkoły lub placówki w szczególności:

1) kieruje działalnością szkoły lub placówki oraz reprezentuje ją na zewnątrz;

2) sprawuje nadzór pedagogiczny, z zastrzeżeniem art. 36 ust. 2;

3) sprawuje opiekę nad uczniami oraz stwarza warunki harmonijnego rozwoju psychofizycznego poprzez aktywne działania prozdrowotne;

4) realizuje uchwały rady szkoły lub placówki oraz rady pedagogicznej, podjęte w ramach ich kompetencji stanowiących;

5) dysponuje środkami określonymi w planie finansowym szkoły lub placówki zaopiniowanym przez radę szkoły lub placówki i ponosi odpowiedzialność za ich prawidłowe wykorzystanie, a także może organizować administracyjną, finansową i gospodarczą obsługę szkoły lub placówki;

5a) (326) wykonuje zadania związane z zapewnieniem bezpieczeństwa uczniom i nauczycielom w czasie zajęć organizowanych przez szkołę lub placówkę;

6) wykonuje inne zadania wynikające z przepisów szczególnych;

7) współdziała ze szkołami wyższymi oraz zakładami kształcenia nauczycieli w organizacji praktyk pedagogicznych;

8) odpowiada za właściwą organizację i przebieg sprawdzianu i egzaminów, o których mowa w art. 9 ust. 1, przeprowadzanych w szkole lub placówce;

9) (327) stwarza warunki do działania w szkole lub placówce: wolontariuszy, stowarzyszeń i innych organizacji, w szczególności organizacji harcerskich, których celem statutowym jest działalność wychowawcza lub rozszerzanie i wzbogacanie form działalności dydaktycznej, wychowawczej i opiekuńczej szkoły lub placówki;

10) (328) odpowiada za realizację zaleceń wynikających z orzeczenia o potrzebie kształcenia specjalnego ucznia.

4) Ustawa z dnia 26 .01. 1982 r. Karta Nauczyciela

Art. 7. 1. Szkołą kieruje dyrektor, który jest jej przedstawicielem na zewnątrz, przełożonym służbowym wszystkich pracowników szkoły, przewodniczącym rady pedagogicznej. Dyrektor sprawuje opiekę nad dziećmi i młodzieżą uczącą się w szkole.

2. Dyrektor szkoły odpowiedzialny jest w szczególności za:

1) dydaktyczny i wychowawczy poziom szkoły;

2) realizację zadań zgodnie z uchwałami rady pedagogicznej i rady szkoły, podjętymi w ramach ich kompetencji stanowiących, oraz zarządzeniami organów nadzorujących szkołę;

3) tworzenie warunków do rozwijania samorządnej i samodzielnej pracy uczniów i wychowanków;

4) zapewnienie pomocy nauczycielom w realizacji ich zadań i ich doskonaleniu zawodowym;

5) zapewnienie w miarę możliwości odpowiednich warunków organizacyjnych do realizacji zadań dydaktycznych i opiekuńczo-wychowawczych;

6) zapewnienie bezpieczeństwa uczniom i nauczycielom w czasie zajęć organizowanych przez szkołę.

Obowiązki (uprawnienia) pedagoga szkolnego:

Rozporządzenie Ministra Edukacji Narodowej z dnia 30.04. 2013 r. **w sprawie zasad udzielania i organizacji pomocy psychologiczno-pedagogicznej w publicznych przedszkolach, szkołach i placówkach.**

§ 23. Do zadań pedagoga i psychologa w przedszkolu, szkole i placówce należy w szczególności:

1) prowadzenie badań i działań diagnostycznych uczniów, w tym diagnozowanie indywidualnych potrzeb rozwojowych i edukacyjnych oraz możliwości psychofizycznych uczniów w celu określenia przyczyn niepowodzeń edukacyjnych oraz wspierania mocnych stron uczniów;

2) diagnozowanie sytuacji wychowawczych w przedszkolu, szkole lub placówce w celu rozwiązywania problemów wychowawczych oraz wspierania rozwoju uczniów;

3) udzielanie pomocy psychologiczno-pedagogicznej w formach odpowiednich do rozpoznanych potrzeb;

4) podejmowanie działań z zakresu profilaktyki uzależnień i innych problemów dzieci i młodzieży;

5) minimalizowanie skutków zaburzeń rozwojowych, zapobieganie zaburzeniom zachowania oraz inicjowanie różnych form pomocy w środowisku szkolnym i pozaszkolnym uczniów;

6) inicjowanie i prowadzenie działań mediacyjnych i interwencyjnych w sytuacjach kryzysowych;

7) pomoc rodzicom i nauczycielom w rozpoznawaniu i rozwijaniu indywidualnych możliwości, predyspozycji i uzdolnień uczniów;

8) wspieranie nauczycieli, wychowawców grup wychowawczych i innych specjalistów w udzielaniu pomocy psychologiczno-pedagogicznej.

Załącznik nr 8.
Najważniejsze zagrożenia w świetle obowiązujących przepisów

Cyberprzemoc i cyberprzestępczość - formy:

1. Włamanie i wprowadzenie zmian na koncie mailowym, na profilu w serwisie społecznościowym, czacie, forum, blogu itp.

Ochrona prawna: Art. 267 i 268 Kodeksu karnego

Art. 267. §1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.

Art. 268a. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych,

podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Co robić:

1. Powiadomić administratora sieci, strony internetowej itp.
2. Złożyć wniosek o ściganie na policję lub do prokuratury.

2.Naruszenie czci, dóbr osobistych w sieci: znieważenie, zniesławienie, naruszenie wizerunku.

„Cześć, dobre imię, dobra sława człowieka są pojęciami obejmującymi wszystkie dziedziny jego życia osobistego, zawodowego i społecznego. Naruszenie czci może więc nastąpić zarówno przez pomówienie o ujemne postępowanie w życiu osobistym i rodzinnym, jak i przez zarzucenie niewłaściwego postępowania w życiu zawodowym, naruszające dobre imię danej osoby i mogące narazić ją na utratę zaufania potrzebnego do wykonywania zawodu lub innej działalności" - tak wskazał Sąd Najwyższy w wyroku z dnia 29.10.1971r., sygn. akt II CR 455/71).

Ochrona prawna: art. 23 i 24 Kodeksu cywilnego oraz art. 212 i 216 Kodeksu karnego

Kodeks cywilny:

Art. 23. Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.

Art. 24. § 1. Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny.

§ 2. Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych.

§ 3. Przepisy powyższe nie uchybiają uprawnieniom przewidzianym w innych przepisach, w szczególności w prawie autorskim oraz w prawie wynalazczym.

Kodeks karny:

Art. 212. § 1. Kto pomawia inną osobę, grupę osób, instytucję, osobę prawną lub jednostkę organizacyjną niemającą osobowości prawnej o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności,

podlega grzywnie albo karze ograniczenia wolności.

§ 2. Jeżeli sprawca dopuszcza się czynu określonego w § 1 za pomocą środków masowego komunikowania,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 3. W razie skazania za przestępstwo określone w § 1 lub 2 sąd może orzec nawiązkę na rzecz pokrzywdzonego, Polskiego Czerwonego Krzyża albo na inny cel społeczny wskazany przez pokrzywdzonego.

§ 4. Ściganie przestępstwa określonego w § 1 lub 2 odbywa się z oskarżenia prywatnego.

Art. 216. § 1. Kto znieważa inną osobę w jej obecności albo choćby pod jej nieobecność, lecz publicznie lub w zamiarze, aby zniewaga do osoby tej dotarła,

podlega grzywnie albo karze ograniczenia wolności.

§ 2. Kto znieważa inną osobę za pomocą środków masowego komunikowania,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 3. Jeżeli zniewagę wywołało wyzywające zachowanie się pokrzywdzonego albo jeżeli pokrzywdzony odpowiedział naruszeniem nietykalności cielesnej lub zniewagą wzajemną, sąd może odstąpić od wymierzenia kary.

§ 4. W razie skazania za przestępstwo określone w § 2 sąd może orzec nawiązkę na rzecz pokrzywdzonego, Polskiego Czerwonego Krzyża albo na inny cel społeczny wskazany przez pokrzywdzonego.

§ 5. Ściganie odbywa się z oskarżenia prywatnego

Co robić:

1.Zwrócić się do administratora sieci, strony internetowej itp. do usunięcia lub zablokowania wpisów.

2. Złożyć wniosek o ściganie na policję lub do prokuratury.

3. Złożyć pozew cywilny o odszkodowanie.

3. Używanie wulgaryzmów w celu obrażenia drugiej osoby albo grupy ludzi lub używane w celu wyrażenia lekceważenia czegoś lub kogoś,

Ochrona prawna: art. 141 Kodeksu wykroczeń

Art. 141 Kto w miejscu publicznym umieszcza nieprzyzwoite ogłoszenie, napis lub rysunek albo używa słów nieprzyzwoitych, podlega karze ograniczenia wolności, grzywny do 1.500 złotych albo karze nagany.

Co robić:

1. Zwrócić się do administratora sieci, strony internetowej itp. do usunięcia lub zablokowania wpisów.

2. Powiadomić policję o popełnieniu wykroczenia.

4. Nękanie, czyli uporczywe, złośliwe nękanie kogoś przy użyciu min. narzędzi dostępnych w Internecie.

Ochrona prawna: art. 190 a Kodeksu karnego i art. 107 Kodeksu wykroczeń

Kodeks karny: Art. 190a. (245) § 1. Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność,

podlega karze pozbawienia wolności do lat 3.

§ 2. Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej.

§ 3. Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca.

podlega karze pozbawienia wolności od roku do lat 10.

§ 4. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Kodeks wykroczeń: Art. 107. Kto w celu dokuczenia innej osobie złośliwie wprowadza ją w błąd lub w inny sposób złośliwie niepokoi, podlega karze ograniczenia wolności, grzywny do 1.500 złotych albo karze nagany.

Co robić:

1. Zwrócić się do administratora sieci, strony internetowej itp. do usunięcia lub zablokowania wpisów.
2. Powiadomić policję o popełnieniu wykroczenia.
3. Powiadomić policję lub prokuraturę o popełnieniu przestępstwa.

5. Zjawisko groomingu, czyli nagabywanie w sieci dzieci do celów seksualnych

Grooming, wiąże się z zachęcaniem dziecka do udziału w czynności seksualnej, np. przez obietnicę nagrody, dyskutowanie na temat intymnych zachowań, prezentowanie treści o charakterze pornograficznym w celu przełamania oporu czy też zahamowań dotyczących sfery seksualnej"

Ochrona prawna: 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.

Co robić:

1. Powiadomić administratora sieci, strony internetowej itp.

2.Powiadomić policję lub prokuraturę o popełnieniu przestępstwa.

6. Publikacja materiałów pornograficznych

Ochrona prawna: art. 202 Kodeksu karnego.

Art. 202. § 1. Kto publicznie prezentuje treści pornograficzne w taki sposób, że może to narzucić ich odbiór osobie, która tego sobie nie życzy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. (uchylony),

§ 3. Kto w celu rozpowszechniania produkuje, utrwala lub sprowadza, przechowuje lub posiada albo rozpowszechnia lub prezentuje treści pornograficzne z udziałem małoletniego albo treści pornograficzne związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem, podlega karze pozbawienia wolności od lat 2 do 12.

§ 4. Kto utrwala treści pornograficzne z udziałem małoletniego, podlega karze pozbawienia wolności od roku do lat 10.

§ 4a. Kto przechowuje, posiada lub uzyskuje dostęp do treści pornograficznych z udziałem małoletniego,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4b. Kto produkuje, rozpowszechnia, prezentuje, przechowuje lub posiada treści pornograficzne przedstawiające wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 4c. Karze określonej w § 4b podlega, kto w celu zaspokojenia seksualnego uczestniczy w prezentacji treści pornograficznych z udziałem małoletniego.

§ 5. Sąd może orzec przepadek narzędzi lub innych przedmiotów, które służyły lub były przeznaczone do popełnienia przestępstw określonych w § 1-4b, chociażby nie stanowiły własności sprawcy.

Co robić:

1. Powiadomić administratora sieci, strony internetowej itp.

2. Powiadomić policję lub prokuraturę o popełnieniu przestępstwa.

7. Utrwalenie wizerunku bez zgody utrwalenie wizerunku nagiej osoby bez jej zgody, naruszenie intymności seksualnej

Ochrona prawna: art. 191a Kodeksu karnego, art. 23 i 24 Kodeksu cywilnego, art. 81 Ustawy o prawie autorskim i prawach pokrewnych

Kodeks karny:

Art. 191a§ 1. Kto utrwala wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej, używając w tym celu wobec niej przemocy, groźby bezprawnej lub podstępu, albo wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody rozpowszechnia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Ściganie następuje na wniosek pokrzywdzonego.

Kodeks cywilny:

Art. 23. Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.

Art. 24. § 1. Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny.

§ 2. Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych.

§ 3. Przepisy powyższe nie uchybiają uprawnieniom przewidzianym w innych przepisach, w szczególności w prawie autorskim oraz w prawie wynalazczym.

Ustawa o prawie autorskim i prawach pokrewnych

Art. 81.

„Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie."

Co robić:

1. Zwrócić się do administratora sieci, strony internetowej itp. do usunięcia lub zablokowania dostępu do zdjęcia (wizerunku).
2. Złożyć wniosek o ściganie na policję lub do prokuratury.
3. Złożyć pozew cywilny o odszkodowanie.

8. Zakłócanie pracy systemu komputerowego

Ochrona prawna: art. 268 a, 269 a, 269 b Kodeksu karnego, art. 415 Kodeksu cywilnego

Kodeks karny:

Art. 268a. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Art. 269a. Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 269b. § 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej,podlega karze pozbawienia wolności do lat 3.

§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

Kodeks cywilny:

Art. 415

Kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia.

Co robić?

1. Złożyć wniosek o ściganie na policję lub do prokuratury,
2. Złożyć pozew cywilny o naprawienie szkody.

Załącznik nr 9. Uwarunkowania planowania i wdrożenia koncepcji BYOD w instytucjach edukacyjnych

Dzisiejsi uczniowie to obywatele świata cyfrowego, żyją na co dzień w świecie multimediów, preferują wizualne techniki uczenia się i oczekują kreatywności. Najsprawniej uczą się metodą prób i błędów, są stale podłączeni do sieci i współpracują, odwołują się do informacji, które są żywe i powiązane odsyłaczami. Uczniowie oczekują nowoczesnych metod nauczania z wygodnym dostępem do zasobów internetowych w procesie edukacyjnym. Najwygodniejszą formą dostępu jest korzystanie w instytucji oświatowej z własnego smartfonu bądź tabletu, nazywane koncepcją BYOD.

Podstawowe zalety i wyzwania koncepcji BYOD można zestawić następująco:

- dostęp do zasobów w dowolnym miejscu i czasie, w tym w szkole,
- finansowanie urządzeń przez rodziców,
- zawsze nowoczesne spersonalizowane urządzenia,
- bez kosztów aktualizacji i napraw,

ale zarazem:

- wyzwanie różnorodności urządzeń i systemów,
- wymóg kontrolowalności dostępu do Internetu z pośrednictwem sieci instytucji,
- bardzo istotnie zwiększone wymagania co do konfigurowalności i przepływności infrastruktury sieciowej, większe nakłady na infrastrukturę sieciową,
- ograniczenia urządzeń mobilnych, które przeważnie nadają się jedynie do konsumpcji treści, o ile nie posiadają fizycznych klawiatur, w ograniczonym stopniu do wytwarzania treści.

BYOD, trudne pytania:

1. Jak spowodować, by uczniowie nie rozpraszali się dostępnością urządzeń?
2. Jak ograniczyć korzystanie przez uczniów z niewłaściwych stron?
3. Jak poradzić sobie z różnorodnością narzędzi?
4. Czy użyteczne edukacyjnie oprogramowanie będzie działać na smartfonach czy tabletach?
5. Co z uczniami, których nie stać na własne urządzenia?
6. Czy koncepcja BYOD nie zwiększy problemów z kradzieżami w szkole?
7. Jestem zainteresowany wdrożeniem koncepcji BYOD, ale jak zacząć - przeraża mnie wizja całkowitej zmiany sposobu nauczania?

Rozwiązanie BYOD trzeba rozpatrywać w wielu płaszczyznach:

- finansowej,
- pedagogicznej,
- technicznej,
- polityki równych szans (bez preferencji dla zamożnych).

Projektując w sieci rozwiązanie typu BYOD należy przede wszystkim odpowiedzieć sobie na pytanie, jakie ma być przeznaczenie tego rozwiązania. Zasadniczo rozpatruje się dwa podstawowe uzasadnienia:

1. Udostępnienie wydajnej i taniej dla użytkownika infrastruktury dostępowej do sieci internet urządzeniom końcowym pracowników i uczniów. To uzasadnienie nie przekłada się bezpośrednio na usprawnienie bądź urozmaicenie procesu dydaktycznego, jakkolwiek nadal może stanowić istotny aspekt w instytucjach oświatowych prowadzących swoją działalność edukacyjną albo w obszarach niezamożnych albo dla niezamożnych grup społecznych. Wtedy koncepcja BYOD może stanowić element działań przeciwdziałających wykluczeniu cyfrowemu.

2. Usprawnienie i urozmaicenie procesu dydaktycznego. Dostosowanie metod nauczania do realiów społeczeństwa informacyjnego. Z punktu widzenia ekonomicznego nie ma oczywistej odpowiedzi na pytanie, czy dopuszczenie urządzeń własnych użytkowników podnosi czy obniża koszty prowadzenia działalności edukacyjnej. Z jednej strony wykorzystywanie urządzeń własnych zmniejsza zapotrzebowanie na dużą bazę urządzeń w posiadaniu szkoły oraz zmniejsza koszty związane z koniecznością cyklicznego odświeżania parku technologicznego urządzeń końcowych, a ten starzeje się stosunkowo szybko. Z drugiej jednak strony dopuszczenie obcych urządzeń do infrastruktury technicznej instytucji niesie ze sobą bardzo poważne dodatkowe nakłady na bezpieczeństwo oraz konieczność wzmożonej nieustannej troski i nakładów na dbanie o odpowiedni poziom bezpieczeństwa w trakcie eksploatacji systemu. Użytkownikom może być wygodniej i przyjemniej, ale instytucja ponosi dodatkowy koszt.

Wykorzystywanie własnych urządzeń w infrastrukturze technicznej instytucji musi niezbędnie być obudowane formalnie. W szczególności jedną z regulacji wewnętrznych instytucji powinna być polityka akceptowalnego wykorzystywania urządzeń mobilnych w sieci szkoły (instytucji oświatowej).

Kontekst uzasadniający konieczność wprowadzania polityki akceptowalnego wykorzystywania urządzeń mobilnych przez uczniów w szkole obejmuje między innymi następujące zagadnienia:

- urządzenie mobilne jako potencjalne źródło rozrywki odrywające uwagę od prowadzonych zajęć,
- oczekiwania rodziców dotyczące dostępności natychmiastowej komunikacji z dziećmi w sytuacji dostępności urządzeń mobilnych,
- zagadnienia zarządzania i ochrony prywatności informacji przechowywanych na urządzeniach mobilnych,
- potencjalne nasilenie zjawiska cyberbullingu jako efekt łatwej dostępności urządzeń mobilnych w trakcie zajęć,
- problem wykorzystywania urządzeń mobilnych do oszukiwania w trakcie testów wiedzy.

Celem wytworzenia polityki BYOD to przede wszystkim:

- zapewnienie zgodności z obowiązującym prawem i regulacjami wewnętrznymi instytucji oświatowej,
- zwiększenie świadomości zagrożeń towarzyszących korzystaniu z urządzeń własnych i generalnie zasobów teleinformatycznych w jednostce,
- udostępnienie możliwości korzystania z internetu oraz korzystania z zasobów edukacyjnych użytkownikom mobilnym,
- troska o ochronę informacji wrażliwych instytucji.

Wyzwania techniczne z jakimi musi sobie poradzić instytucja aspirująca do wdrożenia rozwiązania BYOD obejmują między innymi:

- zwiększone prawdopodobieństwo przeciążenia sieci komputerowej – ryzyko niedostatecznie pojemnej (w liczbie klientów i oferowanej przepływności) infrastruktury sieci bezprzewodowej,
- istotnie zwiększone wymagania i nakłady na właściwy poziom bezpieczeństwa i zarządzania rozbudowaną infrastrukturą i informacjami o kontach przypisanych do użytkowników,
- wyzwanie różnorodności urządzeń przyłączanych do sieci.

W kontekście wykorzystywania urządzeń własnych należy rozróżnić elementy polityki BYOD odnoszące się do:

- dostępu do ogólnodostępnych zasobów internetowych, w tym kontroli i potencjalnego filtrowania treści dostępnych za pośrednictwem sieci instytucji oświatowej,
- dostępu do lokalnych zasobów wykorzystywanych w procesie edukacyjnym.

Wybrane przykładowe zapisy warte rozpatrzenia jako potencjalne elementy spisanej polityki BYOD, która powinna być przedmiotem indywidualnej potwierdzonej podpisem akceptacji warunków przed przyznaniem użytkownikowi i jego urządzeniu dostępu do sieci instytucji:

- korzystanie z urządzeń elektronicznych w trakcie zajęć jest dopuszczalne jedynie po wyraźnej zgodzie prowadzącego zajęcia nauczyciela,
- użytkownicy muszą stosować się do przyjętych w jednostce reguł postepowania z urządzeniami mobilnymi, w szczególności z przyjętą polityką dozwolonego użytkowania sieci internetowej jednostki,
- w trakcie przebywania przez ucznia w jednostce, zarówno na zajęciach i w trakcie przerw międzylekcyjnych, nauczyciel ma prawo zażądać od ucznia zaprzestania korzystania z zasobów Internetu,

- w trakcie zajęć dopuszcza się korzystanie z urządzeń jedynie w celach edukacyjnych, zabronione jest wykorzystywanie urządzeń do celów prywatnych, w tym towarzyskich,
- urządzenia nie mogą być wykorzystywane do robienia zdjęć, filmów bądź nagrywania audio, bez wyraźnej zgody osoby filmowanej bądź nagrywanej, niezależnie czy jest nauczycielem czy też uczniem.

Inne zagadnienia, które stanowią istotny kontekst w przypadku decyzji o wdrożeniu w instytucji edukacyjnej rozwiązań BYOD:

- zarządzanie tożsamością użytkowników w sieci komputerowej instytucji, konta i hasła, bezwzględnie indywidualne jedno na każdego użytkownika na potrzeby rejestrowania aktywności w sieci z wykorzystaniem infrastruktury instytucji – zmniejszenie ryzyk prawnych instytucji;
- zagadnienie filtrowania treści; infrastruktura instytucji oświatowej bezwzględnie musi mieć zainstalowane rozwiązania do filtrowania treści niedozwolonych, a być może również niepożądanych;
- zagadnienie zapisanych uprawnień nauczyciela względem ucznia i stanowiących jego własność urządzenia BYOD: nauczyciel musi mieć możliwość odłączenia/wyłączenia urządzenia/zablokowania konta, którego aktywność zaburza pracę sieci komputerowej bądź dostęp do zasobów (np. przez aktywną infekcję szkodliwym oprogramowaniem);
- zagadnienie ładowania elektrycznego urządzeń BYOD – laptopy i smartfony często wymagają ładowania, regulaminy powinny wskazywać oczekiwanie przychodzenia do szkoły z naładowanymi urządzeniami, jeżeli chce się z nich w szkole korzystać;
- zagadnienie uprawnień do drukowania: z których urządzeń i czy w ogóle można drukować na drukarkach instytucji z urządzeń własnych;
- prawo nauczyciela do przeszukiwania urządzenia, o ile urządzenie to jest podłączane do sieci instytucji;
- obowiązek dbania o bezpieczeństwo urządzenia włączanego do sieci, np. rozstrzygnięcie zakresu odpowiedzialności szkoły i ucznia w sytuacji uszkodzenia urządzenia w szkole;
- wpisane w proces powszechnego użycia w szkole ryzyko kradzieży bądź zagubienia urządzenia własnego.

Bibliografia

1. Aronson E., Pratkanis A., 2008) *Wiek propagandy*. Warszawa: Wydawnictwo Naukowe PWN.

2. Augustynek A., 2010, *Uzależnienie komputerowe. Diagnoza, rozpowszechnienie, terapi*a. Warszawa: Difin.

3. *Biuletyny bezpieczeństwa OUCH* 2014, Dostęp w: http://www.cert.pl/ouch.

4. Borkowska A., Macander D., 2009, *System reagowania w szkole na ujawnienie cyberprzemocy. Dziecko krzywdzone. Teoria, badania, praktyka*. 26(1).

5. Borkowska A., Szymańska J., Witkowska M., 2012, *Przeciwdziałanie agresji i przemocy w szkole. Poradnik dla nauczycieli.* Warszawa, Dostęp w: ORE http://www.ore.edu.pl/materialy-do-pobrania.

6. Bochenek M., Wrońska A., Silicki K., i inni 2014, Cyberprzestępczość i nadużycia w: red. Lizut J., (red.) (2014), *Zagrożenia cyberprzestrzeni kompleksowy program dla pracowników służb społec znych*. Warszawa: Wydawnictwo Wyższej Szkoły Pedagogicznej.

7. Chrzanowski M., Kruk,T. J., 2014, *Wyzwania sieciowej tożsamości – aspekty techniczne* w: red. Lizut J., Wrońska A., *E-zagrożenia nowym wyzwaniem dla służb społecznych*, Wydawnictwo WSP im. Janusza Korczaka 2014, .

8. Cialdini R., 2013, *Wywieranie wpływu na ludzi.* Gdańsk: Gdańskie Wydawnictwo Psychologiczne.

9. Gaś Z., 2006, *Profilaktyka w szkole.* Warszawa: Wydawnictwo Szkolne i Pedagogiczne.

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

11. Lizut J., Wrońska A., 2014, *E- zagrożenia nowym wyzwaniem dla służb społecznych.* Warszawa: Wydawnictwo Wyższej Szkoły Pedagogicznej.

12. Makaruk K., Wójcik S., 2013, *Nadużywanie internetu przez młodzież. Wyniki badania EU NET ADB. Dziecko krzywdzone. Teoria, badania, praktyka.*12(1).

13. Polak Z., Różycka M., Maranda M., 2013, *Zagrożenia internetowe. Wybrane zjawiska*. Warszawa: NASK.

14. R*aport roczny CERT Polska2015*, Dostpne w: http://www.cert.pl/PDF/Raport_CP_2014.pdf.

15. *Raport "The School IT Administrator" - European Schoolnet*, 2015, Dostepne w: http://www.eun.org/c/document_library/get_file?uuid=2e2dcbda-f332-4a13-90e8-58098ac8d059&groupId=43887.

16. Wrzesień-Gandolfo A. (red.), 2015, B*ezpieczeństwo dzieci online. Kompendium dla rodziców, nauczycieli i profesjonalistów.* Warszawa: NASK i Fundacja Dzieci Niczyje.

Dokumenty:

1. *Rozporządzenie Ministra Edukacji Narodowej z dnia 1 lutego 2013 r. w sprawie szczegółowych zasad działania publicznych poradni psychologiczno-pedagogicznych, w tym publicznych poradni specjalistycznych* (Dz.U. 2013 poz. 199),

2. *Ustawa z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich* (Dz. U. 1982 nr 35 poz. 228)

3. *Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń* (Dz. U. 1971 nr 12 poz. 114)

4. *Ustawa z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego* (Dz. U. 1997 nr 89 poz. 555)

5. *Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny* (Dz. U. 1997 nr 88 poz. 553)

6. *Ustawa z dnia 6 kwietnia 1990 r. o Policji* (Dz. U. 1990 nr 30 poz. 179)

7. *Ustawa z dnia 7 września 1991 r. o systemie oświaty* (Dz. U. 1991 nr 95 poz. 425),

8. *Ustawa z dnia 26 stycznia 1982 r. - Karta Nauczyciela* (Dz.U. 1982 nr 3 poz. 19)

9. *Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne* (Dz. U. 2004 nr 171 poz. 1800)

10. *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (Dz. U. 2002 nr 144 poz. 1204)

11. *Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny* (Dz. U. 1964 nr 16 poz. 93)

12. *Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych* (Dz. U. 1994 nr 24, poz. 83)

O projekcie

Projekt „Działania na rzecz bezpiecznego korzystania z internetu" był realizowany w okresie od 18.06.2015 do 15.12.2015 r. jako zadanie publiczne przez Fundację Odkrywców Innowacji oraz Fundację Drabina Rozwoju, na podstawie umowy nr 1/DSI/ZP1/2015 z dnia 30.09.2015 zawartej z Ministerstwem Administracji i Cyfryzacji. Jego celem było podniesienie świadomości na temat zagrożeń występujących w cyberprzestrzeni, przeciwdziałanie tego rodzaju zagrożeniom oraz promowanie świadomego i bezpiecznego korzystania z Internetu wśród pracowników placówek oświatowych, rodziców, dzieci i młodzieży. Produkty projektu: kwerenda (repozytorium) zintegrowanych treści nt. cyberzagrożeń, standard bezpieczeństwa online placówek oświatowych, 16 konferencji wojewódzkich i przeprowadzenia 80 szkoleń lokalnych przez Trenerów Bezpiecznego Internetu dla łącznie ponad 3500 osób. Uzupełnieniem działań adresowanych do dorosłych, jest innowacyjny mulitbook dla dzieci.

Zadanie publiczne zostało zrealizowane z dużym zaangażowaniem Zespołu Projektu i współpracujących z nim specjalistów i ekspertów, co pozwoliło opracować i dostarczyć wszystkie wymagane produkty i rezultaty zadania. Łącznie udało się włączyć w projekt aż 175 Trenerów Bezpiecznego Internetu, którzy w bardzo krótkim czasie przeszkolili łącznie 8107 osób, w tym: 5152 dzieci i młodzieży, 2115 nauczycieli i 840 rodziców (dane na 16.12.2015 r.).

Zespół Projektu:
Jerzy Nowak – Kierownik Projektu
Olga Szczekutek – Koordynator Szkoleń
Julia Trzebuchowska – Koordynator Konferencji
Dorota Zalewska – Specjalista ds. Rozliczeń

Realizatorzy projektu

FUNDACJA ODKRYWCÓW INNOWACJI

Fundacja Odkrywców Innowacji (wcześniej: Fundacja Inicjatyw Badawczo-Szkoleniowych) od 2010 r. realizuje zadania w zakresie badań społecznych, szkoleń i warsztatów dla dzieci, młodzieży, rodziców i nauczycieli. Celami Fundacji są m.in. budowanie kapitału intelektualnego dla innowacyjności ze szczególnym uwzględnieniem wyższej użyteczności publicznej, promowanie idei przedsiębiorczości, w tym promowanie działalności wspomagającej rozwój gospodarki, ekonomii społecznej i usług społecznych.

W projekcie odpowiedzialna za opracowanie standardu bezpieczeństwa online dla placówek oświatowych, opracowanie kwerendy nt. cyberzagrożeń, realizację konferencji wojewódzkich i szkoleń lokalnych realizowanych przez Trenerów Bezpiecznego Internetu.

Fundacja Drabina Rozwoju od 2006 r. tworzy i realizuje programy i multimedialne narzędzia edukacyjne skierowane do dzieci, młodzieży i dorosłych. Drabina Rozwoju symbolizuje pokonywanie kolejnych progów, poziomów, barier w rozwoju człowieka. Projekty Fundacji łączą wiedzę z różnych dziedzin: między innymi psychologię, edukację przyrodniczą, artystyczną z nowoczesnymi technologiami. W ramach swojej działalności Fundacja stworzyła m.in. gry komputerowe łączące pracę psychoedukacyjną z bajkoterapią, filmy animowane, których celem jest przeciwdziałanie zjawisku przemocy w szkole czy grę komputerową dla młodzieży usamodzielniającej się i wchodzącej na rynek pracy łączącą metodę coachingu i storytellingu. Laureat konkursu INNOWATOR EFS 2011.

W ramach projektu odpowiedzialna za opracowanie multibooka dla dzieci.