BEZPIECZNA SZKOŁA

ZAGROŻENIA I ZALECANE DZIAŁANIA PROFILAKTYCZNE W ZAKRESIE BEZPIECZEŃSTWA FIZYCZNEGO I CYFROWEGO UCZNIÓW

niepodległa | POLSKA STULECIE ODZYSKANIA NIEPODLEGŁOŚCI

MINISTERSTWO EDUKACJI NARODOWEJ

niepodległa | POLSKA STULECIE ODZYSKANIA NIEPODLEGŁOŚCI

MINISTERSTWO EDUKACJI NARODOWEJ

BEZPIECZNA SZKOŁA

ZAGROŻENIA I ZALECANE DZIAŁANIA PROFILAKTYCZNE W ZAKRESIE BEZPIECZEŃSTWA FIZYCZNEGO I CYFROWEGO UCZNIÓW

Ministerstwo Edukacji Narodowej
Warszawa 2020

Instytucje współpracujące przy tworzeniu IV wydania poradnika:
Ministerstwo Cyfryzacji, Ministerstwo Spraw Wewnętrznych i Administracji,
Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy,
Ośrodek Rozwoju Edukacji

Opracowanie redakcyjne i graficzne: Ośrodek Rozwoju Edukacji

ISBN 978-83-66047-91-4
Warszawa 2020
Wydanie IV uaktualnione

Ministerstwo Edukacji Narodowej
00-918 Warszawa
al. J. Ch. Szucha 25

Spis treści

Słowo wstępne 7

Słownik pojęć 11

Rozdział I
Bezpieczeństwo fizyczne w szkole 23

1. Zagrożenia zewnętrzne i procedury reagowania w razie wystąpienia zagrożenia 23
   1.1. Pożar w szkole. Ewakuacja w trakcie lekcji i przerwy – zasady postępowania po ogłoszeniu alarmu w szkole i placówce oświatowej 23
   1.2. Wtargnięcie napastnika (terrorysty) do szkoły – postepowanie nauczyciela, współpraca z policją 27
   1.3. Podłożenie ładunku wybuchowego – postępowanie w wyniku zamachu bombowego 29
   1.4. Podłożenie podejrzanego pakunku – postępowanie w sytuacji kryzysowej oraz uruchomienie procedury działań 30
   1.5. Skażenie chemiczne lub biologiczne szkoły – procedury postępowania w przypadku uwolnienia się niebezpiecznych dla ludzi i środowiska substancji chemicznych oraz zastosowania broni biologicznej 33
   1.6. Epidemia; kataklizm – procedury postepowania przypadku wystąpienia sytuacji nadzwyczajnych 40
2. Zagrożenia wewnętrzne i procedury reagowania w przypadku wystąpienia zagrożenia 41
   2.1. Agresywne zachowania w szkole lub zjawisko tzw. fali – procedury postępowania w przypadku wystąpienia na terenie szkoły zachowań agresywnych, tj. agresji fizycznej i słownej ucznia lub nauczyciela 41
   2.2. Substancje psychoaktywne – procedura postępowania w przypadku znalezienia w szkole substancji psychoaktywnych 46
   2.3. Kradzież; wymuszanie – procedura postępowania w przypadku wystąpienia w szkole kradzieży bądź wymuszenia pieniędzy lub przedmiotów wartościowych 49
   2.4. Pedofilia i uwodzenie – procedura postępowania w przypadku wystąpienia zjawiska pedofilii w szkole 50
   2.5. Pornografia – procedury postępowania w przypadku rozpowszechniania przez ucznia pornografii w szkole 51

2.6. Nieprawidłowe zachowania psychoseksualne w szkole – procedury postępowania w przypadku wystąpienia prostytucji ... 52
2.7. Procedura postępowania w sytuacji wystąpienia niepokojących zachowań seksualnych uczniów w szkole ... 53
2.8. Wypadek ucznia w szkole – procedury postępowania pracowników szkoły gwarantujące poszkodowanemu w wypadku uczniowi należytą opiekę i niezbędną pomoc ... 54
2.9. Czyn karalny popełniony przez ucznia – procedury postępowania w przypadku popełnienia przez ucznia czynu karalnego oraz udzielania pomocy uczniowi będącemu sprawcą czynu karalnego ... 58
2.10. Ofiara czynu karalnego – procedury postępowania w przypadku zidentyfikowania w szkole ucznia będącego ofiarą czynu karalnego oraz udzielania pomocy uczniowi będącemu ofiarą czynu karalnego ... 59

Rozdział II
Bezpieczeństwo cyfrowe ... 61

1. Zagrożenia w świecie cyfrowym – procedury reagowania w przypadku wystąpienia zagrożenia cyfrowego ... 61
   1.1. Rekomendacje strategiczne i profilaktyczne ... 62
2. Podstawowe działania na rzecz bezpieczeństwa cyfrowego w szkole ... 72
   2.1. Obligatoryjne działania interwencyjne ... 72
   2.2. Działania szkoły adresowane do instytucji i organizacji zewnętrznych ... 74
   2.3. Dostęp do treści szkodliwych, niepożądanych, nielegalnych – procedura reagowania ... 75
   2.4. Zagrożenia prywatności ... 80
   2.5. Nadmierne korzystanie z internetu – procedura reagowania ... 82
   2.6. Dezinformacja, bezkrytyczna wiara w treści zamieszczone w internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, w tym szkodliwość reklam – procedury reagowania ... 84
   2.7. Cyberprzemoc – procedura reagowania ... 85
   2.8. Seksting – procedura reagowania ... 89
   2.9. Bezprawne użycie cudzego wizerunku w sieci – procedura reagowania ... 92
   2.10. Niebezpieczne kontakty w internecie – procedura reagowania ... 95
   2.11. Łamanie prawa autorskiego – procedura reagowania ... 97

Rozdział III
Bezpieczeństwo techniczne sieci i sprzętu IT ... 101

1. Rodzaje zagrożeń ... 101
2. Procedury reagowania w przypadku wystąpienia incydentu zagrożenia cyberbezpieczeństwa w szkole/placówce oświatowej ... 105
3. Cyberbezpieczeństwo w Ogólnopolskiej Sieci Edukacyjnej ... 106
4. Instytucje wspierające cyberbezpieczeństwo ... 109
5. Linki do stron oraz telefony do instytucji ... 110

Rekomendacje podsumowujące ... 111

Słowo wstępne

Szanowni Państwo,

1 września uczniowie wracają do szkół i tradycyjnych stacjonarnych zajęć. Ponieważ jesteśmy w sytuacji szczególnej z uwagi na stan epidemii COVID-19, robimy wszystko, by uczniowie, nauczyciele i inni pracownicy systemu oświaty uczyli się i pracowali w bezpiecznych warunkach. Przygotowaliśmy rozwiązania – wytyczne sanitarne i akty prawne, które pozwolą odpowiednio zareagować i podjąć właściwe decyzje, gdyby pojawiło się ognisko zakażenia. Wszelkie decyzje w sprawie przygotowania szkół do właściwego i przede wszystkim bezpiecznego ich funkcjonowania w nowym roku szkolnym są podejmowane z uwzględnieniem aktualnej sytuacji epidemicznej oraz w porozumieniu z Głównym Inspektorem Sanitarnym i Ministrem Zdrowia – dla dobra uczniów oraz nauczycieli.

5 sierpnia br. przedstawiłem *Wytyczne dla publicznych i niepublicznych szkół i placówek*, które będą obowiązywały od 1 września 2020 r. Zalecenia będą miały zastosowanie w organizacji pracy szkoły dla dzieci i młodzieży w systemie stacjonarnym. Zostały one opublikowane na stronie internetowej Ministerstwa Edukacji Narodowej:
https://www.gov.pl/web/edukacja/bezpieczny-powrot-do-szkol-dzialania-men-w-organizacji-roku-szkolnego-20202021-w-warunkach-epidemii.

Dodatkowo przygotowano zalecenia dla dyrektorów publicznych i niepublicznych szkół i placówek zlokalizowanych w strefie czerwonej/żółtej, dostępne także na stronie resortu edukacji:
https://www.gov.pl/web/edukacja/organizacja-ksztalcenia-zalecenia-dla-dyrektorow.

12 sierpnia br. podpisałem 5 rozporządzeń, które pozwolą szkołom i placówkom w razie zagrożenia epidemicznego zastosować odpowiednie, dostosowane do sytuacji rozwiązania. Dzięki wprowadzonym zmianom dyrektorzy szkół i placówek otrzymali narzędzia pozwalające na odpowiednią organizację zajęć w szkole – szczególnie, jeśli sytuacja epidemiologiczna zagrozi zdrowiu uczniów i nauczycieli oraz pozostałych pracowników. Po otrzymaniu

pozytywnej opinii powiatowego inspektora sanitarnego i zgody organu prowadzącego będą oni mogli elastycznie wprowadzać model mieszany pracy szkoły i placówki – z kształceniem na odległość dla grupy uczniów (np. zawiesić zajęcia grupy, grupy wychowawczej, oddziału, klasy, etapu edukacyjnego bądź całej szkoły lub placówki, w zakresie wszystkich lub poszczególnych zajęć) lub wprowadzić kształcenie na odległość dla wszystkich uczniów.

W obecnym stanie prawnym organ prowadzący przedszkole, szkołę lub placówkę (dalej określane jako: szkoła) odpowiada za jej działalność. Do jego zadań należy w szczególności zapewnienie warunków działania szkoły, w tym bezpieczeństwa i higieny nauki, wychowania i opieki, oraz jej wyposażenie w sprzęt niezbędny do pełnej realizacji programów nauczania, programów wychowawczo-profilaktycznych i wykonywania innych zadań statutowych. Dodatkowo dyrektor szkoły, kierując jej działalnością, wykonuje obowiązki związane z zapewnieniem bezpieczeństwa uczniom i nauczycielom w czasie zajęć organizowanych przez szkołę, w tym sprawuje opiekę nad uczniami oraz stwarza warunki harmonijnego rozwoju psychofizycznego poprzez aktywne działania prozdrowotne.

Aby wesprzeć realizację powyższych zadań, oddaję do Państwa rąk poradnik, który stanowi kompendium wiedzy na temat rozpoznawania sytuacji zagrożeń i reagowania na nie – przeznaczony dla dyrektorów szkół, nauczycieli, rodziców i uczniów.

Szkoła jest miejscem nie tylko intelektualnego rozwoju uczniów, ale i kształtowania postaw, umiejętności i relacji. Relacje te dotyczą kontaktów zarówno pomiędzy uczniami, jak i pomiędzy uczniami a rodzicami oraz nauczycielami. Szkoła to także otoczenie fizyczne ucznia, w którym przebywa on w zróżnicowanej grupie przez wiele godzin tygodniowo.

Bezpieczeństwo dzieci i młodzieży w szkole oraz podczas zajęć organizowanych przez nią stanowi istotny obszar zainteresowania wszystkich partnerów szkoły. Jest pierwszoplanową wartością nie tylko dla władz szkoły, ale przede wszystkim dla rodziców uczniów, którzy do niej uczęszczają. Zatem właściwa reakcja wychowawcy, pedagoga, dyrektora szkoły, organu prowadzącego – adekwatna do zaistniałego zdarzenia (zagrożenia) – oraz powiadomienie odpowiednich instytucji są nie tylko oczekiwane, ale dają gwarancję, że podjęte działania będą skuteczne.

Tematyka wzmacniania bezpieczeństwa uczniów w szkołach znajduje swoje odzwierciedlenie także w kierunkach polityki oświatowej określanych przez Ministra Edukacji Narodowej oraz stanowi priorytet w działaniach resortu edukacji.

Przygotowany poradnik składa się z części poświęconych odrębnym tematom związanym z szeroko rozumianą problematyką bezpieczeństwa. Wyodrębnienie w tekście zagadnień bezpieczeństwa fizycznego (zagrożenia zewnętrzne i wewnętrzne), bezpieczeństwa cyfrowego wraz z bezpieczeństwem technicznym sieci i sprzętu IT pozwoli zainteresowanym nie tylko na łatwe odnalezienie kompleksowych informacji dotyczących występowania danego

zagrożenia, ale przede wszystkim wskaże, w jaki sposób reagować na to zjawisko i gdzie zwrócić się o pomoc.

Bezpieczeństwo w szkole jest pojęciem szerokim. Obejmuje wiele obszarów, w tym: stan techniczny budynków szkoły i jej otoczenia, wewnątrzszkolne przepisy i ich znajomość wśród nauczycieli, uczniów i rodziców, klimat społeczny, a także różnorodne programy i zajęcia adresowane do poszczególnych grup szkolnej społeczności. Ważne jest identyfikowanie zarówno zagrożeń, jak i zasobów umożliwiających prowadzenie efektywnych działań dydaktycznych, wychowawczych i profilaktycznych.

Od ponad dekady żyjemy w społeczeństwie informacyjnym, dla którego technologie informatyczne stanowią niezastąpione narzędzie nauki, pracy, rozrywki oraz komunikacji. Większość polskiego społeczeństwa funkcjonuje w świecie cyfrowych treści i usług, przenikających codzienność w stopniu niemającym odzwierciedlenia w żadnej technologii z przeszłości. Polska szkoła musi zatem w pełni bezpiecznie działać w środowisku cyfrowym, wykorzystując edukacyjne zasoby dostępne online – multimedialne treści, aplikacje, platformy i skojarzone z nimi interaktywne metody nauczania.

Oprócz omówienia problematyki bezpieczeństwa niniejszy dokument zawiera także opis usług bezpieczeństwa oferowanych w ramach Ogólnopolskiej Sieci Edukacyjnej (OSE). Jest to program publicznej sieci telekomunikacyjnej, która zapewnia szkołom dostęp do szybkiego, bezpłatnego i bezpiecznego internetu.

Intencją autorów opracowania jest stworzenie zwięzłego poradnika, zawierającego pakiet zadań rekomendowanych do zrealizowania w szkole, a w kwestiach szczegółowych odsyłającego do rozwiązań, materiałów szkoleniowych, dokumentów i multimediów edukacyjnych, które pozwolą nauczycielom i dyrektorom szkół podnieść swoje kompetencje służące zapewnieniu uczniom bezpieczeństwa, w tym w cyberprzestrzeni, a także usystematyzować już posiadaną wiedzę.

Należy pamiętać, że każda szkoła ma własną specyfikę, zróżnicowane grono uczniów, pracowników, infrastrukturę, wyposażenie itp. Zatem publikacja nie zastąpi opracowania w szkołach adekwatnych indywidualnych rozwiązań. Ponieważ poradnik wskazuje pakiet działań na rzecz zapewnienia bezpieczeństwa uczniów w środowisku szkolnym, powinien być również uzupełniany przez szkoły o indywidualnie zdiagnozowane ryzyka oraz wiedzę wynikającą z dotychczasowych doświadczeń.

Proponowane w publikacji działania opiekuńcze, wychowawcze i profilaktyczne mogą mieć charakter prewencyjny. Są również odpowiedzią na obowiązki szkoły – m.in. w zakresie upowszechniania wśród dzieci i młodzieży wiedzy o bezpieczeństwie oraz kształtowania właściwych postaw wobec zagrożeń, w tym związanych z korzystaniem z technologii informacyjno-komunikacyjnych – które nakłada na szkoły *Ustawa Prawo oświatowe*.

Opracowanie zawiera słownik pojęć, który ułatwi jego odbiorcom rozumienie terminologii, zwłaszcza cyfrowej. Autorzy rekomendują przydatne linki kierujące do instytucji wspierających cyberbezpieczeństwo oraz polecają dobre praktyki szkół i organizacji pozarządowych. Podmioty te wypracowały model działania, który przyczynił się do podniesienia poziomu bezpieczeństwa dzieci i młodzieży w szkole i poza nią.

Poradnik został opracowany w Ministerstwie Edukacji Narodowej we współpracy z organizacjami pozarządowymi, innymi resortami i instytucjami odpowiedzialnymi za bezpieczeństwo, w tym Ministerstwem Cyfryzacji, Ministerstwem Spraw Wewnętrznych i Administracji, Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym oraz Ośrodkiem Rozwoju Edukacji.

Dziękuję za zaangażowanie i pomoc w przygotowaniu publikacji.

Dariusz Piontkowski
Minister Edukacji Narodowej

Słownik pojęć

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.

Bezpieczeństwo cyfrowe

Patrz: cyberbezpieczeństwo.

Blog

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

BYOD

Ang. *bring your own device* – przynieś własne urządzenie; przynieś własną technologię, przynieś własny telefon, swój komputer, co oznacza, że w trakcie np. procesu nauczania można korzystać z własnego urządzenia.

Chmura obliczeniowa

Chmura obliczeniowa, przetwarzanie w chmurze – model przetwarzania danych oparty na użytkowaniu usług dostarczonych przez usługodawcę. Chmura to rozległa sieć serwerów zdalnych znajdujących się w różnych miejscach na świecie. Serwery są połączone i działają jako jeden system. Pełnią różne funkcje: przechowują dane i umożliwiają zarządzanie nimi, obsługują aplikacje oraz dostarczają zawartość lub usługi takie jak strumieniowe przesyłanie materiałów wideo, poczta internetowa, oprogramowanie biurowe i sieci społecznościowe. Zamiast korzystać z danych i plików na jednym komputerze

lokalnym lub osobistym, można uzyskiwać dostęp do nich z dowolnego urządzenia połączonego z internetem, wówczas informacje są dostępne w dowolnym miejscu i czasie.

Cyberbezpieczeństwo

Cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[1].

Cyberbezpieczeństwo może być rozumiane różnie, zależnie od tego, do kogo lub do czego się odnosi. Inne znaczenie ma dla pojedynczych użytkowników internetu, inne dla przedsiębiorstw, a jeszcze inne dla państw oraz całych narodów. Niezależnie jednak od punktu odniesienia istotę cyberbezpieczeństwa stanowi zbiór działań i zasobów, które umożliwiają obywatelom, przedsiębiorstwom i państwom osiągnięcie bezpieczeństwa, odporności i niezawodności działania systemów informatycznych.

Cyberprzemoc

Cyberprzemoc – rodzaj przemocy, której akty dokonywane są przy użyciu nowych technologii (mediów elektronicznych) w internecie. Do kategorii takich zjawisk zaliczamy: wyzywanie, straszenie, prześladowanie, oczernianie lub poniżanie. 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 także przybierać formę podszywania się pod inną osobę za pomocą przechwyconego profilu lub poczty, jak również celowego ignorowania aktywności ofiary w sieci. Akty cyberprzemocy należy rozpatrywać zarówno w kontekście ofiary (osoby poszkodowanej), jak i sprawcy (osoby lub grupy osób) oraz świadków zdarzenia. Cechą charakterystyczną cyberprzemocy jest wyższy stopień anonimowości niż w tradycyjnej formie przemocy. 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, a także ich dostępnością.

Najczęściej w przypadkach cyberprzemocy dochodzi do naruszeń: art. 190 kk[2] – groźba karalna, art. 190a kk – uporczywe nękanie (stalking), podszywanie się, art. 191 kk – zmuszenie do określonego działania, art. 191a kk – naruszenie intymności seksualnej, utrwalenie wizerunku nagiej osoby bez jej zgody, art. 212 kk – zniesławienie, art. 216 kk – zniewaga, art. 267 kk – bezprawne uzyskanie informacji, art. 268 kk – utrudnianie zapoznania się z informacją, art. 268a kk – niszczenie danych informatycznych, art. 269 kk – uszkodzenie danych informatycznych, art. 269a kk – zakłócanie systemu

[1] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, Dz.U. 2018, poz. 1560, z późn. zm.
[2] *Kodeks karny*, Dz.U. 1997, Nr 88, poz. 553, z późn. zm.

komputerowego, art. 287 kk – oszustwo komputerowe, art. 107 kw[3] – dokuczenia lub złośliwe wprowadzanie w błąd.

Czat

Czat, również **chat**, z ang. *chat* – pogawędka. 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 zaczęła być wykorzystywana do prowadzenia wideokonferencji.

Dane osobowe

Dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej[4].

Dzień Bezpiecznego Internetu (ang. *Safer Internet Day*)

„Dzień Bezpiecznego Internetu" – projekt, który ma na celu inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych, zaznajomienie rodziców, nauczycieli i wychowawców z problematyką bezpieczeństwa online oraz promocję pozytywnego wykorzystywania internetu. Kluczowe działania projektu to organizacja konferencji z okazji DBI oraz koordynacja lokalnych inicjatyw szkolnych na rzecz propagowania bezpieczeństwa w internecie. Organizatorem wydarzenia w Polsce od 2005 roku jest Polskie Centrum Programu Safer Internet (PCPSI), które tworzą Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy oraz Fundacja Dajemy Dzieciom Siłę[5].

DoS lub DDoS

Ataki typu DoS (ang. *denial of service* – odmowa usługi) lub DDoS (ang. *distributed denial of service* – rozproszona odmowa usługi) – działania, których celem jest blokowanie konkretnego serwisu internetowego, czyli dostępu do strony www. Ataki typu DoS są przeprowadzane z jednego komputera, zaś typu DDoS – z wielu komputerów na raz.

[3] *Kodeks wykroczeń*, Dz.U. 1971, Nr 12, poz. 114, z późn. zm.
[4] Art. 4. *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych – RODO).
[5] https://www.saferinternet.pl/dbi/o-dbi.html [dostęp: 20.08.2020 r.].

Dyżurnet.pl

Dyżurnet.pl[6] – zespół ekspertów Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, działający jako punkt kontaktowy (*hotline*) do zgłaszania nielegalnych i szkodliwych treści w internecie. Aktywność zespołu Dyżurnet.pl skupia się przede wszystkim na działaniach na rzecz usunięcia z sieci materiałów służących seksualnemu wykorzystywaniu dzieci. Zespół Dyżurnet.pl analizuje treści wskazane przez użytkowników, wykonuje dokumentację techniczną, przesyła informacje do policji, prokuratury, administratorów serwisów internetowych oraz zagranicznych punktów kontaktowych zrzeszonych w sieci INHOPE, skupiającej działania wszystkich tego rodzaju punktów w UE i krajach stowarzyszonych. Zespół Dyżurnet.pl 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, których celem jest bezpieczeństwo dzieci w internecie, kierowane do różnych grup użytkowników.

Edukacja medialna

Kształtowanie umiejętności świadomego, krytycznego, odpowiedzialnego i selektywnego korzystania ze środków masowego przekazu, tworzenia i nadawania przekazów medialnych. Inne stosowane określenia to *media literacy*, kompetencje medialne, umiejętności elektroniczne.

E-dziennik

Dziennik elektroniczny to program komputerowy lub serwis internetowy służący do rejestracji przebiegu nauczania. W wielu szkołach jest często stosowany jako dodatkowy element kontaktu z rodzicami. Zakres informacji przechowywanych w dziennikach elektronicznych jest przeważnie większy niż w tradycyjnych szkolnych dziennikach.

E-learning

E-learning lub e-nauczanie – nauczanie lub kształcenie przy użyciu technologii informatycznych. Oznacza wspomaganie procesu dydaktycznego za pomocą komputerów osobistych, smartfonów, tabletów i internetu. Dzięki takiej formie edukacji możliwe jest ukończenie kursu, szkolenia, czy edukacji formalnej bez konieczności fizycznej obecności w sali wykładowej.

Firewall

Zapora sieciowa (ang. *firewall* – ściana ogniowa) – jeden ze sposobów zabezpieczania sieci i systemów przed intruzami. Termin ten może odnosić się zarówno do sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do komputera, który zabezpiecza. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz,

[6] https://dyzurnet.pl/ [dostęp: 20.08.2020 r.].

tzn. sieci publicznych, internetu, chroni też przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz.

Forum dyskusyjne

Forma grupy dyskusyjnej działającej 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.

Incydent zagrożenia bezpieczeństwa cyfrowego

Zdarzenie, które może mieć niekorzystny wpływ na cyberbezpieczeństwo organizacji.

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.

Laptop

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

Login

Identyfikator użytkownika wymagany, aby uzyskać dostęp (zalogować się) do danego systemu informatycznego.

Media społecznościowe

Media społecznościowe (ang. *social media*) – forma przekazu informacji następująca za pośrednictwem stron bądź aplikacji działających w sieci internetowej, w ramach społeczności tworzonych poprzez użytkowników tych serwisów. Przykładem jest Facebook.

Multimedia

Media, które stanowią połączenie kilku 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.

Nadużywanie internetu

Inaczej „siecioholizm", „infoholizm", czy „uzależnienie od internetu". Nadużywanie sieci związane jest z ilością czasu spędzanego w internecie oraz intensywnością korzystania z niego, przy równoczesnym zaniedbywaniu innych aktywności. W wielu przypadkach

stan taki ma znaczący wpływ na pogorszenie funkcjonowania człowieka w różnych sferach: fizycznej, psychicznej, społecznej, ekonomicznej, interpersonalnej.

Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB)

NASK to akronim od nazwy Naukowa i Akademicka Sieć Komputerowa. Państwowy Instytut Badawczy prowadzący działalność naukową i badawczo-wdrożeniową w dziedzinie sieci teleinformatycznych. W strukturach Instytutu działa CSIRT NASK – jeden z trzech krajowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego wchodzący w skład krajowego systemu cyber-bezpieczeństwa[7]. NASK-PIB jest również operatorem Ogólnopolskiej Sieci Edukacyjnej (OSE)[8]. W działalności NASK-PIB szczególną rolę pełni edukacja społeczna oraz rozwój społeczeństwa informacyjnego. Od lat realizowane są projekty promujące bezpieczne korzystanie z nowych technologii i internetu wśród dzieci i młodzieży. Od 2005 roku NASK-PIB jest koordynatorem Polskiego Centrum Programu „Safer Internet", dedykowanego bezpieczeństwu dzieci w sieci. W NASK-PIB funkcjonuje również Zespół Dyżurnet.pl – punkt kontaktowy do zgłaszania nielegalnych treści internetowych, szczególnie związanych z seksualnym wykorzystywaniem dzieci.

Netykieta

Zbiór zasad określających właściwe zachowania w internecie, np. unikanie pisania wielkimi literami, będącego synonimem krzyku.

Niebezpieczne kontakty/uwodzenie w internecie

Uwodzenie dzieci w internecie (ang. *child grooming*) to rodzaj relacji tworzonej za pośrednictwem internetu między osobą dorosłą a osobą małoletnią (poniżej 15. r.ż. w rozumieniu przepisów *Kodeksu karnego*), 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 jego późniejsze wykorzystanie seksualne. 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 czatów 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, m.in. poprzez poruszanie tematów związanych z seksem. Kolejny etap polega na zachęcaniu dziecka do podejmowania czynności intymnych przy jednoczesnym naleganiu , by utrzymywało tajemnicę dotyczącą relacji. Podczas procesu uwodzenia sprawca stosuje różne techniki manipulacji, używa również szantażu czy groźby. Ryzyko podejmowania niebezpiecznych

[7] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, Dz.U. 2018, poz. 1560.
[8] *Ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej*, Dz.U. 2017, poz. 2184.

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*.

Online

Słowo *online* (z ang. na linii) określa status osoby, serwera lub innego podmiotu związanego z dostępem do internetu, informuje o dostępności/aktywności. Przeciwieństwem trybu online jest tryb offline – poza linią, czyli poza zasięgiem.

Ogólnopolska Sieć Edukacyjna (OSE)

Program publicznej sieci telekomunikacyjnej dającej szkołom dostęp do szybkiego, bezpłatnego i bezpiecznego internetu. Program został zaprojektowany przez Ministerstwo Cyfryzacji we współpracy z Ministerstwem Edukacji Narodowej na mocy *Ustawy o Ogólnopolskiej Sieci Edukacyjnej*[9]. Operatorem OSE jest Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, nadzorowany przez Ministerstwo Cyfryzacji.

Phishing

Jeden z najpopularniejszych typów ataku, oparty na wiadomości e-mail lub SMS. Wykorzystuje inżynierię społeczną, czyli technikę polegającą na tym, że przestępcy internetowi próbują oszukać użytkownika sieci i spowodować, aby podjął działanie zgodnie z ich zamierzeniami. Cyberprzestępcy, podszywając się m.in. pod firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych, czy nawet znajomych użytkowników, starają się wyłudzić ich dane do logowania, np. do kont bankowych lub używanych przez nich kont społecznościowych czy systemów biznesowych.

Nazwa *phishing* budzi dźwiękowe skojarzenia z *fishingiem* – czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują odpowiednio przygotowaną „przynętę". Do tego wykorzystują najczęściej sfałszowane e-maile i SMS-y. Coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społecznościowych (np. poprzez „metodę na BLIK-a"). 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.

[9] *Ustawa o Ogólnopolskiej Sieci Edukacyjnej z dnia 27 października 2017 r.*, Dz.U. 2017, poz. 2184; 2019, poz. 1815; 2020, poz. 695.

Pornografia dziecięca – materiały przedstawiające seksualne wykorzystanie dzieci

Określenie materiałów (tekstu, filmu, zdjęć, zapisów audio), które powstały podczas seksualnego wykorzystania dziecka. Termin „materiały przedstawiające seksualne wykorzystanie dzieci" jest bardziej poprawny niż termin „pornografia dziecięca", ponieważ odzwierciedla charakter przestępstwa dokonanego na dziecku. Art. 202 *Kodeksu karnego* 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.

Poczta elektroniczna

Usługa internetowa służąca do przesyłania wiadomości tekstowych, tzw. e-maili, czyli listów elektronicznych.

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 Dajemy Dzieciom Siłę oraz Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy. Centrum podejmuje szereg kompleksowych działań na rzecz bezpieczeństwa dzieci i młodzieży, korzystających z internetu i nowych technologii. W ramach programu „Safer Internet" (saferinternet.pl) realizowane są 3 projekty: pomoc telefoniczna i online – telefon zaufania dla dzieci i młodzieży: 116 111 – https://116111.pl/ oraz telefon dla rodziców i nauczycieli w sprawach bezpieczeństwa dzieci: 800 100 100 – https://800100100.pl/, a także Dyżurnet.pl – punkt kontaktowy, tzw. *hotline*, do którego można anonimowo zgłaszać przypadki występowania w internecie treści zabronionych prawem, takich jak: materiały przedstawiające seksualne wykorzystanie dzieci, pedofilia, treści o charakterze rasistowskim i ksenofobicznym.

Prawa autorskie

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

Prywatność

Prawo przysługujące każdemu człowiekowi. W kontekście internetu jest to umiejętność dbania o ochronę swoich danych, właściwego kontrolowania informacji na własny temat umieszczanych samodzielnie oraz publikowanych przez innych w sieci.

Router

Sieciowe urządzenie trasujące (przekaźnik), odpowiedzialne za przesyłanie pakietów informacji między dwoma odległymi od siebie komputerami. Router (lub routery – gdyż

im większe odległości między komunikującymi się komputerami, tym więcej tego typu urządzeń pośredniczy w przekazywaniu informacji) łączy daną sieć komputerową WAN/LAN z inną, tworząc pomost dla przesyłanych informacji. Z uwagi na to, że w dużych sieciach droga z jednego komputera do drugiego (i z powrotem) może przebiegać przez wiele różnych alternatywnych ścieżek, router ma za zadanie skierować nadchodzący pakiet zawsze tą ścieżką, która w danej chwili rokuje najszybszy i/lub najlepszy transfer do miejsca docelowego lub następnego węzła komunikacyjnego – routera. Tablice routingu, monitorujące na bieżąco wszystkie połączenia, zawierają nieustannie aktualizowane dane o stanie połączonych sieci, na podstawie których router dokonuje wyboru dalszej drogi dla nadchodzącego pakietu. Routerem może być zarówno komputer z zainstalowanym odpowiednim oprogramowaniem, jak i opracowane specjalnie do tego celu urządzenie elektroniczne.

Seksting

Seksting to przesyłanie za pomocą internetu i urządzeń mobilnych 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, że materiały przekazywane w prywatnej korespondencji trafiają do publicznego dostępu, stając się niekiedy przyczyną tragedii. Zjawisko sekstingu może w niektórych przypadkach stanowić naruszenie prawa. W polskim prawie istnieje szereg przepisów, które można odnosić do tego zagadnienia. *Kodeks karny* (art. 202) 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 w wyniku użycia wobec niej przemocy, groźby bezprawnej lub podstępu oraz rozpowszechnianie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody (art. 191a).

Serwer

System oprogramowania biorący udział w udostępnianiu zasobów. Przykładami udostępnianych zasobów są pliki, bazy danych, łącza internetowe, a także urządzenia peryferyjne, jak drukarki i skanery. Serwerem nazywa się często również komputer świadczący takie usługi, sprowadzające się zazwyczaj do udostępniania pewnych zasobów innym komputerom lub pośredniczący w przekazywaniu danych między komputerami. Serwerem może być zwykły komputer, jednak w celu pełnego wykorzystania możliwości,

jakie daje oprogramowanie serwerowe, powinna to być maszyna przeznaczona do tej roli. Maszyny takie są przystosowane do pracy ciągłej, wyposaża się je w duże i szybkie dyski twarde lub SSD, dużą ilość pamięci RAM oraz wydajne wielordzeniowe procesory serwerowe.

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.

Strona internetowa

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

Szkodliwe oprogramowanie

Każdy system oparty na pracy komputerów oraz wykorzystujący aplikacje może zostać zainfekowany szkodliwym oprogramowaniem (*malware*). Istnieje wiele typów takich zagrożeń: wirusów komputerowych, „koni trojańskich", oprogramowania szpiegującego. Szkodliwe programy mogą wnikać do urządzenia poprzez połączenia z internetem, być przenoszone na nośnikach pamięci USB, a także przenosić się w czasie synchronizacji urządzeń (np. telefonu z komputerem). Brak aktualizacji oprogramowania zwiększa prawdopodobieństwo infekcji, a brak systemów antywirusowych (*antymalware*) czy zapory *firewall* powoduje całkowitą ekspozycję na zagrożenia bezpieczeństwa.

Tablet

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

Tablica multimedialna

Inaczej tablica interaktywna – urządzenie przypominajcie duży biały monitor lub tablicę. Reaguje na dotyk i umożliwia współdziałanie z podłączonym do niej komputerem oraz projektorem multimedialnym. W zależności od technologii, w której tablica została wykonana, do pisania na niej 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.

Telefon komórkowy

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

Telefon zaufania

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

Telefon zaufania dla dzieci i młodzieży

Ogólnopolski, bezpłatny i anonimowy telefon zaufania oraz portal https://116111.pl/ przeznaczony dla dzieci i młodzieży, czynny całodobowo. Dostępny jest pod zharmonizowanym w Europie numerem 116 111, połączenie nie jest widoczne na rachunkach ani na billingach większości sieci.

Terrorysta

Osoba posługująca się bronią, eliminująca lub próbująca wyeliminować osoby znajdujące się na określonym obszarze, w obiekcie lub budynku.

Treści nielegalne

Treści 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), także treści znieważających o charakterze rasistowskim i ksenofobicznym (art. 257 kk). Nielegalność treści może wynikać z ujawniania każdej informacji, której upublicznienie jest niezgodne z prawem (np. dane osobowe).

Treści pornograficzne

W polskim prawie nie istnieje definicja terminu „treści pornograficzne". Ocena zależy więc od sądu, który może powołać 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). *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 kk, który zabrania prezentowania treści pornograficznych dzieciom do lat 15.

Treści szkodliwe

Treści, które mogą wywołać negatywne emocje u odbiorcy, treści promujące niebezpieczne zachowania i dlatego nieodpowiednie dla szerokiego odbiorcy. Do szkodliwych treści zalicza się m.in: treści obrazujące przemoc, obrażenia fizyczne bądź śmierć (np. zdjęcia/filmy prezentujące ofiary wypadków), okrucieństwo wobec zwierząt, nawołujące do samookaleczeń lub samobójstw, zachowań szkodliwych dla zdrowia czy zażywania niebezpiecznych substancji; treści dyskryminacyjne, prezentujące postawy wrogości a nawet nienawiści; treści pornograficzne. Treściami szkodliwymi mogą być materiały dozwolone przez prawo oraz regulamin danego serwisu internetowego lecz pozbawione odpowiedniej klauzuli. Zaleca się, aby treści, które nie są przeznaczone dla osób poniżej 18. r.ż., opatrzone były ostrzeżeniem oraz wyraźną informacją o ich charakterze.

Wirus

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

Zagrożenie

Wszelkie okoliczności lub zdarzenia, które mogą mieć negatywny wpływ na operacje, zasoby organizacji lub osoby fizycznej za pośrednictwem systemu informatycznego poprzez nieuprawniony dostęp do danych, zniszczenie, ujawnienie, modyfikację informacji i/lub odmowę usług.

Rozdział I
Bezpieczeństwo fizyczne w szkole

Bezpieczeństwo w szkole – uczniów, kadry nauczycielskiej i innych pracowników – stanowi kluczowe zagadnienie polityki oświatowej. Jego zapewnienie należy do najważniejszych obowiązków dyrektorów, nauczycieli i opiekunów. Czynności związane z konkretnymi zadaniami z obszaru bezpieczeństwa powinny mieć określonych realizatorów, aby w czasie wystąpienia sytuacji kryzysowej każdy z nauczycieli i innych pracowników szkoły wiedział, jakie działania pozostają w jego kompetencji (jaką przydzielono mu funkcję).

1. Zagrożenia zewnętrzne i procedury reagowania w razie wystąpienia zagrożenia

Do najczęściej występujących zewnętrznych zagrożeń fizycznych należą: wybuch pożaru, podejrzenie podłożenia ładunku wybuchowego, otrzymanie podejrzanej przesyłki, wtargnięcie terrorysty do szkoły, zagrożenie skażeniem niebezpiecznymi środkami chemicznymi lub biologicznymi, epidemia i kataklizm.

W niemal każdym z powyższych przypadków dochodzi do ogłoszenia **alarmu i ewakuacji** uczniów oraz personelu szkoły. Sposób ich przeprowadzenia powinien być znany wszystkim, a ćwiczenia w przeprowadzaniu ewakuacji powinny odbywać się raz w roku szkolnym.

1.1. Pożar w szkole. Ewakuacja w trakcie lekcji i przerwy – zasady postępowania po ogłoszeniu alarmu w szkole i placówce oświatowej

Alarm lokalny w szkole ma na celu zapewnienie bezpieczeństwa w razie zagrożenia życia i zdrowia uczniów przebywających na terenie szkoły. Najważniejszym działaniem, jakie należy podjąć w przypadku stwierdzenia zagrożenia, jest jak najszybsze powiadomienie o niebezpieczeństwie wszystkich osób znajdujących się w strefie zagrożenia i natychmiastowe

podjęcie działań mających na celu ratowanie zdrowia i życia osób zagrożonych. W tym celu należy wykorzystać **sygnał alarmu lokalnego, którym w szkole są trzy sygnały dzwonka, trwające około 10 sekund każdy, następujące bezpośrednio po sobie.**

Ważne!
Alarm lokalny w szkole jest sygnałem, który powinien być znany wszystkim uczniom i pracownikom szkoły. Tylko w przypadku, gdy nastąpiło bezpośrednie zagrożenie życia, nauczyciel sam podejmuje decyzję o ewakuacji, nie czekając na ogłoszenie alarmu.

Zasady postępowania po ogłoszeniu alarmu w szkole/placówce oświatowej:

1. O ewakuacji decyduje dyrektor, który po otrzymaniu meldunku od nauczyciela lub innej osoby zgłaszającej zagrożenie oraz rozpoznaniu sytuacji podejmuje decyzję o zawiadomieniu służb (policja, straż pożarna) i ogłoszeniu alarmu.
2. W sytuacji braku prądu sygnał alarmowy może być ogłaszany za pomocą gwizdka lub dzwonka ręcznego, z jednoczesnym komunikatem słownym podawanym przez osoby ogłaszające alarm. Jest to sygnał do natychmiastowego działania dla wszystkich pracowników szkoły oraz bezwzględnego wykonywania poleceń nauczycieli przez uczniów.
3. Niezbędne jest wezwanie odpowiednich służb drogą telefoniczną.
   Procedura wezwania powinna być realizowana następująco:

➡ Wybranie numeru odpowiedniej służby:
- policja 997;
- straż pożarna 998;
- pogotowie ratunkowe 999;
- europejski telefon alarmowy (obowiązujący na terenie całej Unii Europejskiej) 112;
- pogotowie energetyczne 991;
- pogotowie gazowe 992;
- pogotowie ciepłownicze 993;
- pogotowie wodno-kanalizacyjne 994;
- wojewódzkie centrum zarządzania kryzysowego 987;
- infolinia policji (połączenie bezpłatne) 800 120 226.

➡ Po zgłoszeniu się dyżurnego operatora danej służby podanie następujących informacji:
- rodzaj stwierdzonego zagrożenia;
- nazwa i adres szkoły;
- imię i nazwisko oraz pełniona funkcję;
- telefon kontaktowy;
- zrealizowane dotąd działania w reakcji na zagrożenie.

➡ Potwierdzenie przyjęcia zgłoszenia i zapisanie danych przyjmującego zgłoszenie.

4. Wszystkie działania od tej chwili mają prowadzić do jak najszybszej ewakuacji wszystkich osób znajdujących się na terenie szkoły. Wszyscy powinni bezwzględnie podporządkować się poleceniom osób funkcyjnych. W przypadku uczniów taką osobą jest nauczyciel, z którym w danym momencie mają zajęcia.
5. Akcją nie może kierować wiele osób, by nie doprowadzić do dezorientacji i wybuchu paniki.
6. Po rozpoznaniu zagrożenia i dokonaniu oceny sytuacji nauczyciel decyduje o możliwej najkrótszej drodze ewakuacji z budynku.
7. Uczniowie na polecenie nauczyciela ustawiają się w szeregu i w sposób zorganizowany kierują się do wskazanego wyjścia ewakuacyjnego.
8. Należy poruszać się po prawej stronie korytarzy i klatek schodowych, wykonując polecenia osób funkcyjnych.
9. Jeżeli alarm zostanie ogłoszony w czasie przerwy, uczniowie powinni skupić się wokół najbliżej stojącego nauczyciela.
10. Nauczyciele i uczniowie, którzy mają lekcje na wyższych kondygnacjach, schodzą po stwierdzeniu, że uczniowie z niższych kondygnacji opuścili już budynek i drogi ewakuacyjne są wolne.
11. Po opuszczeniu budynku uczniowie wraz z nauczycielem udają się na miejsce zbiórki.
12. Jeżeli alarm zostaje ogłoszony w czasie przerwy, uczniowie natychmiast udają się (jeżeli tylko nie zagraża to ich bezpieczeństwu) pod salę, w której mają mieć zajęcia i stamtąd pod opieką nauczyciela przemieszczają się tak, jak to opisano wyżej.
13. Zbiórka na placu alarmowym służy sprawdzeniu obecności uczniów klas i ustaleniu liczby osób nieobecnych. Jest to bardzo istotne dla prowadzenia przez wezwane służby akcji ratunkowej.

Najważniejsze zasady, o których powinien pamiętać każdy uczeń i przestrzegać ich od chwili ogłoszenia w szkole alarmu:

1. Słuchaj i wykonuj dokładnie polecenia nauczyciela.
2. Zachowaj spokój.
3. Po przerwaniu zajęć udaj się wraz z klasą na miejsce zbiórki drogą wskazywaną przez nauczyciela.
4. Pomagaj osobom słabszym.
5. Nie lekceważ zagrożenia nawet wówczas, gdy nie jest ono bezpośrednie.

Bezpieczna ewakuacja osób z niepełnosprawnością

W przypadku osób z niepełnosprawnością bezpieczna ewakuacja powinna uwzględniać rodzaj oraz stopień niepełnosprawności, wiek wychowanków i ewentualne wykorzystanie na potrzeby ewakuacji pomocy ze strony innych osób (pracowników, uczniów). Aby ułatwić ewakuację osób z niepełnosprawnościami, należy:

1. Sporządzić listę uczniów z różnymi rodzajami niepełnosprawności.
2. Rozplanować zajęcia klas, w których uczą się osoby z niepełnosprawnością, w taki sposób, by nie musiały one przemieszczać się pomiędzy piętrami budynku.

3. Przystosować drogi ewakuacyjne do poruszania się osób z niepełnosprawnościami;
4. Wyznaczyć opiekunów osób z niepełnosprawnością na czas ewakuacji.
5. W miarę możliwości wcześniej przeszkolić opiekunów osób z niepełnosprawnością w zakresie technik ewakuacji.

Osoby niepełnosprawne ruchowo często są w stanie samodzielnie pokonać drogę tylko do tzw. bezpiecznego miejsca, co może opóźniać czas ewakuacji całej placówki. Jest to szczególnie istotne w pierwszej fazie opuszczania budynku. Warto uwzględnić konieczność przepuszczenia przed osobę niepełnosprawną strumienia ewakuowanych. Bezpieczne, docelowe miejsce ewakuacji nie zawsze znajduje się poza budynkiem szkolnym. W przypadku osób poruszających się na wózkach inwalidzkich miejsce takie powinno mieć odpowiednie wymiary (co najmniej 900 x 1400 mm). Jego położenie w pobliżu pionowej drogi ewakuacyjnej (schodów) wpłynie na podniesienie bezpieczeństwa osoby ewakuowanej.

Samodzielne pokonywane dróg ewakuacyjnych przez **osoby niewidome i niedowidzące** może wiązać się z ogromnym stresem. Pomóc im mogą wprowadzone w placówce rozwiązania łagodzące stres:

- poziome znaki fluorescencyjne na podłogach i ścianach;
- podświetlone poręcze schodów, progi i przeszkody w kolorach kontrastujących z barwą ścian i otoczenia oraz oświetlenie ewakuacyjne;
- organizowanie tzw. grup pomocy koleżeńskiej oraz przydzielanie opiekunów uczniom niewidomym lub niedowidzącym.

W przypadkach pozostałych niepełnosprawności aspekt przystosowania dróg ewakuacyjnych należy rozpatrywać indywidualnie.

Przykłady technik ewakuacji osób z niepełnosprawnościami:

1. Wykorzystanie krzesełka lub wózka inwalidzkiego – ratownicy umieszczają na nim osobę wymagającą pomocy, a następnie chwytają za nóżki oraz oparcie.
2. Chwyt strażacki – ratownik przekłada swoją rękę między nogami osoby ratowanej, zaciskając ją na nadgarstku zwisającej ręki ratowanego, ratowanego kładzie sobie na barkach.
3. Chwyt kończynowy – jeden ratownik staje za głową ratowanego i chwyta go pod pachy, drugi ratownik jest odwrócony do ratowanego plecami i chwyta go pod kolana.
4. Chwyt „na barana" – ratowany znajduje się na plecach ratownika, który podtrzymuje go obiema rękami za uda.
5. Chwyt kołyskowy – klasyczny sposób przenoszenia małych dzieci.
6. Wykorzystanie koca lub innego podobnego rozmiarami materiału – koc owija się wokół rąk i głowy.
7. Ratowanie w sposób umożliwiający ciągnięcie osoby ratowanej po płaskiej, równej powierzchni (szczególnie przydatne przy ewakuacji osób o dużej masie ciała, nieprzytomnych oraz w przestrzeni zadymionej, gdzie nie ma możliwości przyjęcia postawy wyprostowanej).

1.2. Wtargnięcie napastnika (terrorysty) do szkoły – postepowanie nauczyciela, współpraca z policją

Postępowanie nauczyciela w przypadku wtargnięcia napastnika z niebezpiecznym narzędziem lub bronią, który strzela do osób znajdujących się na korytarzu i w salach lekcyjnych, tzw. aktywnego strzelca:

1. **Jeżeli nie miałeś szansy na ucieczkę, ukryj się, zamknij drzwi na klucz** (zabarykaduj się) – szybkie zamknięcie drzwi może uniemożliwić napastnikowi wejście do pomieszczenia.
2. **Wycisz i uspokój uczniów** – wszelkie dźwięki wydostające się z sal lekcyjnych mogą przyciągnąć uwagę i sprowokować próbę wejścia napastnika do pomieszczenia lub ostrzelanie sali lekcyjnej przez drzwi czy ścianę.
3. **Zaopiekuj się uczniami ze SPE i uczniami, którzy potrzebują pomocy** – zwróć szczególną uwagę na uczniów, którzy specyficznie reagują na stres i mogą mieć problemy z opanowaniem emocji.
4. **Każ bezwzględnie wyciszyć, wyłączyć telefony** – niespodziewane sygnały telefonów mogą zdradzić obecność osób wewnątrz zamkniętych pomieszczeń i zachęcić napastnika do wejścia.
5. **Poinformuj policję, wysyłając informację tekstową SMS o zaistniałej sytuacji** – w przypadku wtargnięcia napastnika do szkoły niezbędne jest natychmiastowe przekazanie informacji policji.
6. **Zasłoń okno, zgaś światło** – należy zaciemnić salę, aby utrudnić obserwowanie osób zabarykadowanych w salach lekcyjnych przez osoby współpracujące z napastnikami, a znajdujące się na zewnątrz budynku.
7. **Nie przemieszczaj się** – przemieszczanie się powoduje hałas lub powstanie cienia, który może zostać zauważony przez napastników.
8. **Stań poniżej linii okien, zejdź ze światła drzwi** – przebywanie w świetle drzwi rzuca cień i może zostać zauważone przez napastników.
9. **Zejdź z linii strzału, połóż się na podłodze** – z reguły napastnicy strzelają na wysokości około 1 do 1,5 m. Strzały z broni palnej bez problemu przebijają drzwi i mogą zranić osoby znajdujące się wewnątrz.
10. **Jeżeli usłyszysz strzały, nie krzycz** – napastnicy, oddając na ślepo strzały przez zamknięte drzwi, chcą sprowokować krzyki przerażonych osób i upewnić się, czy w salach rzeczywiście nikogo nie ma.
11. **Nie otwieraj nikomu drzwi** – interweniujące oddziały policji w razie takiej konieczności same otworzą drzwi. Napastnicy mogą zmusić osoby funkcyjne (np. dyrektora) do przekazania komunikatu, który ma spowodować otwarcie drzwi.
12. **W przypadku wtargnięcia napastnika do pomieszczenia podejmij walkę, która może być ostatnią szansą na uratowanie życia** – celem aktywnego strzelca jest zabicie jak największej liczby ludzi. W takiej sytuacji podjęcie walki może dać jedyną szansę na uratowanie życia.

Postepowanie nauczyciela w przypadku bezpośredniego kontaktu z napastnikami, którzy dążą do przejęcia kontroli nad szkołą:

1. **Wykonuj bezwzględnie polecenia napastnika** – wszelkie próby oporu mogą sprowokować napastnika do impulsywnych zachowań lub zostać uznane za akt agresji i zakończyć się śmiercią zakładników.
2. **Nie udawaj bohatera** – osoby stawiające opór napastnikom giną pierwsze.
3. **Na żądanie terrorystów oddaj im przedmioty osobiste, np. telefon** – wszelkie próby oszukania napastników mogą zakończyć się śmiercią osoby oszukującej.
4. **Poinformuj, że nie możesz wykonać jakiegoś polecenia** – w takim przypadku ewentualne niewykonanie polecenia napastników nie zostanie potraktowane jako próba oporu.
5. **Nie patrz terrorystom w oczy, unikaj kontaktu wzrokowego** – patrzenie w oczy może zostać uznane za akt prowokacji i agresji.
6. **Nigdy nie odwracaj się plecami do napastnika** – odwracanie plecami może zostać uznane za akt agresji bądź lekceważenia, wywołuje złość lub niepokój napastnika.
7. **Nie zwracaj na siebie uwagi** – niezwracanie na siebie uwagi może zwiększyć szansę na uratowanie życia w przypadku, gdy zamachowcy zdecydują się zabić kogoś dla przykładu.
8. **Nie lekceważ napastnika i nie bądź agresywny** – brak szacunku i agresja mogą zostać ukarane przez zamachowców.
9. **Nie oszukuj terrorysty** – oszustwo może zostać uznane za brak szacunku czy agresji i zostać ukarane.
10. **Uspokój uczniów, zawsze zwracaj się do nich po imieniu** – zwracanie się do uczniów po imieniu pozwala na ich upodmiotowienie, co może spowodować łagodniejsze ich traktowanie przez zamachowców.
11. **Poinformuj napastnika o uczniach ze schorzeniami** – wiedza ta w konsekwencji obniży agresję ze strony zamachowców wobec dzieci, których zachowanie może być nietypowe.
12. **Pytaj zawsze o pozwolenie, np. gdy chcesz się zwrócić do uczniów** – każda aktywność podjęta bez zgody zamachowców może zostać potraktowana jako akt oporu czy agresji i w konsekwencji ukarana.
13. **Zawsze korzystaj z dobrej woli terrorysty, zapytaj o możliwość np. napicia się wody** – nigdy nie wiadomo, kiedy kolejny raz będzie można napić się czy zjeść posiłek.

Postępowanie nauczyciela w przypadku działań antyterrorystycznych podjętych przez policję:

1. **Nie uciekaj z miejsca zdarzenia, nie wykonuj gwałtownych ruchów, bo możesz zostać uznany za terrorystę** – policja w trakcie operacji odbijania zakładników nie jest w stanie odróżnić napastników od ofiar.
2. **Nie próbuj pomagać służbom ratowniczym, dyskutować z nimi** – próba pomocy siłom bezpieczeństwa bez ich wyraźnej zgody czy prośby może zostać potraktowana jako utrudnianie działania służb lub nawet uznana za akt agresji.

3. **Połóż się na podłodze, trzymaj ręce z otwartymi dłońmi, najlepiej na wysokości głowy** – taka pozycja pozwala widzieć ewentualne niebezpieczne narzędzia będące w posiadaniu zamachowców, którzy wtopili się w szeregi zakładników.
4. **Słuchaj poleceń i instrukcji grupy antyterrorystycznej, poddawaj się jej działaniom** – postawa taka ułatwia działania policji, a także identyfikację zamachowców, którzy próbują się wtopić w szeregi napastników.
5. **Odpowiadaj konkretnie na pytania policjantów** – nie zmyślaj, jeśli czegoś nie wiesz lub nie pamiętasz, powiedz to wyraźnie; służby interwencyjne potrzebują faktów, żeby uratować ludzkie życie.
6. **Nie trzyj oczu w przypadku użycia gazów łzawiących** – tarcie oczu tylko pogarsza skutki użycia gazu łzawiącego.
7. **Pytaj o pozwolenie zaopiekowania się swoimi uczniami** – wszelkie samowolne działania mogą utrudnić akcję ratunkową.
8. **Odpowiadaj na pytania funkcjonariuszy** – policja zbiera kluczowe informacje mające się przyczynić do skutecznej akcji uwolnienia zakładników i identyfikacji zamachowców.
9. **Bądź przygotowany na traktowanie ciebie jako potencjalnego terrorysty dopóki twoja tożsamość nie zostanie potwierdzona** – w pierwszej fazie operacji odbijania zakładników policja nie jest w stanie odróżnić zakładników od napastników, którzy często próbują się wtopić w tłum i uciec z miejsca ataku.
10. **Po wydaniu polecenia wyjścia opuść pomieszczenie jak najszybciej, oddal się we wskazanym kierunku** – w przypadku interwencji sił bezpieczeństwa należy wykonać polecenia dokładnie tak, jak tego chcą siły interwencyjne.
11. **Nie zatrzymuj się w celu zabrania rzeczy osobistych, zawsze istnieje ryzyko wybuchu lub pożaru** – najważniejsze jest uratowanie życia i zdrowia, a dopiero później ratowanie dóbr materialnych.

1.3. Podłożenie ładunku wybuchowego – postępowanie w wyniku zamachu bombowego

Ofiarami zamachu bombowego mogą być wszyscy – zarówno „swoi", jak i „obcy", inaczej niż w przypadku porwania lub użycia broni palnej, które dotyczą konkretnych osób. Przez materiał wybuchowy rozumiemy związek chemiczny lub mieszaninę kilku związków chemicznych, która jest zdolna w odpowiednich warunkach do gwałtownej reakcji chemicznej i której towarzyszy wydzielenie ogromnej ilości produktów gazowych w postaci wybuchu (detonacji lub deflagracji). Określenie: ładunek materiału wybuchowego oznacza określoną ilość materiału wybuchowego przygotowanego do wysadzenia.

Czynności pracownika oświaty po otrzymaniu informacji o podłożeniu ładunku wybuchowego:

1. **Prowadząc rozmowę z osobą informującą o podłożeniu ładunku wybuchowego, zapamiętaj jak największą ilość szczegółów** – uzyskane informacje mogą być istotne dla policji w celu identyfikacji sprawcy zagrożenia.

2. **Zapisz natychmiast wszystkie uzyskane lub zapamiętane informacje** – w przypadku stresującej sytuacji po pewnym czasie możesz mieć problemy z przypomnieniem sobie istotnych informacji.
3. **Poinformuj niezwłocznie o otrzymaniu zgłoszenia osobę odpowiedzialną w szkole za uruchomienie działań** – może ona zarządzić ewakuację szkoły.
4. **Po usłyszeniu sygnału o podłożeniu ładunku wybuchowego rozpocznij ewakuację zgodnie z planem ewakuacji** – ewakuacja musi być rozpoczęta niezwłocznie po ogłoszeniu odpowiedniego sygnału. Ma ona na celu ochronę wszystkich osób przebywających w szkole przed skutkami ewentualnej eksplozji ładunku.
5. **Nie używaj telefonu komórkowego** – eksplozja ładunku może zostać zainicjowana falami emitowanymi przez telefon komórkowy.
6. **Wychodząc z sali, sprawdź, jeżeli możesz, czy w klasie pozostały przedmioty, które nie należą do jej wyposażenia** – stwierdzenie obecności nieznanego przedmiotu w klasie może przyspieszyć akcję policji i zminimalizować skutki ewentualnej eksplozji.
7. **Bezwzględnie wykonuj polecenia osoby kierującej sytuacją kryzysową lub funkcjonariuszy służb** – w trakcie uruchomienia procedury niezbędna jest dyscyplina i niezwłoczne wykonywanie wszystkich poleceń osoby kierującej sytuacją kryzysową.
8. **W miejscu ewakuacji policz wszystkich uczniów i poinformuj osobę odpowiedzialną za kierowanie działaniami kryzysowymi** – szybkie sprawdzenie obecności dzieci i młodzieży oraz pracowników ułatwi zakończenie ewakuacji szkoły.
9. **Poinformuj rodziców o miejscu odbioru ich dzieci i drodze dojazdu** – informacja ta pozwoli rodzicom na sprawny odbiór dzieci i nie spowoduje blokowania dróg ewakuacyjnych.

1.4. Podłożenie podejrzanego pakunku – postępowanie w sytuacji kryzysowej oraz uruchomienie procedury działań

Podejrzanym pakunkiem nazywamy przedmiot mogący zawierać ładunek wybuchowy lub nieznaną substancję.

Działania nauczyciela w przypadku podejrzenia, że w szkole znajduje się ładunek wybuchowy:

1. **Odizoluj miejsce zlokalizowania podejrzanego pakunku** – należy założyć, że podejrzany pakunek jest ładunkiem wybuchowym, dopóki taka ewentualność nie zostanie wykluczona.
2. **Nie dotykaj, nie otwieraj i nie przesuwaj podejrzanego pakunku** – ładunek wybuchowy może eksplodować w trakcie próby manipulowania nim.
3. **Okryj podejrzany pakunek w razie stwierdzenia, że wydobywa się z niego inna substancja (tylko jeżeli czas na to pozwala)** – okrycie pakunku w przypadku wycieku nieznanej substancji może ograniczyć jej rozprzestrzenianie się.
4. **Poinformuj o zauważeniu pakunku osobę odpowiedzialną za uruchomienie procedury** – osoba ta może zarządzić ewakuację uczniów i wszystkich pracowników szkoły.

5. **Po usłyszeniu sygnału o podłożeniu ładunku wybuchowego rozpocznij ewakuację zgodnie z planem ewakuacji** – ewakuacja musi zostać rozpoczęta niezwłocznie po ogłoszeniu odpowiedniego sygnału. Ewakuacja ma na celu ochronę uczniów i wszystkich pracowników szkoły przed skutkami ewentualnej eksplozji ładunku.
6. **Nie używaj telefonu komórkowego** – fale emitowane przez telefon komórkowy mogą zainicjować eksplozję ładunku.
7. **Bezwzględnie wykonuj polecenia osoby kierującej sytuacją kryzysową lub funkcjonariuszy służb** – w trakcie uruchomienia procedury niezbędna jest dyscyplina i niezwłoczne wykonywanie wszystkich poleceń osoby kierującej sytuacją kryzysową.
8. **W miejscu ewakuacji policz wszystkich uczniów i pracowników szkoły i poinformuj osobę odpowiedzialną za kierowanie działaniami kryzysowymi** – szybkie sprawdzenie obecności ułatwi zakończenie ewakuacji szkoły.
9. **Jeśli jest to możliwe, poinformuj rodziców o miejscu odbioru ich dzieci i drodze dojazdu do szkoły** – informacja ta pozwoli rodzicom na sprawny odbiór dzieci i nie spowoduje blokowania dróg ewakuacyjnych.

Instrukcja postępowania w przypadku podejrzenia podłożenia na terenie szkoły ładunku wybuchowego lub podejrzanego pakunku

Osoby odpowiedzialne za zarządzanie Dyrektor placówki lub w przypadku jego nieobecności wicedyrektor; w przypadku ich nieobecności – osoba przez nich wcześniej upoważniona.	
Otrzymanie informacji o podłożeniu ładunku wybuchowego	**Zauważenie podejrzanego pakunku**
Prowadząc rozmowę z osobą informującą o podłożeniu ładunku wybuchowego, zapamiętać jak największą ilość szczegółów.	Odizolować miejsce zlokalizowania podejrzanego pakunku.
Zapisać natychmiast wszystkie uzyskane lub zapamiętane informacje.	Nie dotykać, nie otwierać i nie przesuwać podejrzanego pakunku.
Poinformować niezwłocznie o otrzymaniu zgłoszenia osobę odpowiedzialną za uruchomienie procedury.	Okryć pakunek w przypadku stwierdzenia wydobywania się z niego innej substancji (tylko jeżeli czas na to pozwala).
Po usłyszeniu sygnału o podłożeniu ładunku wybuchowego rozpocząć ewakuację zgodnie z planem ewakuacji.	Poinformować o zauważeniu pakunku osobę odpowiedzialną za uruchomienie czynności.
Nie używać telefonu komórkowego.	Po usłyszeniu sygnału o podłożeniu ładunku wybuchowego rozpocząć ewakuację zgodnie z planem ewakuacji.

Wychodząc z sali, sprawdzić w miarę możliwości, czy w klasie pozostały przedmioty, które nie należą do jej wyposażenia.	Nie używać telefonu komórkowego.
Bezwzględnie wykonywać polecenia osoby kierującej sytuacją kryzysową lub funkcjonariuszy służb.	Bezwzględnie wykonywać polecenia osoby kierującej sytuacją kryzysową lub funkcjonariuszy służb.
W miejscu ewakuacji policzyć wszystkich uczniów i poinformować osobę odpowiedzialną za kierowanie działaniami kryzysowymi.	W miejscu ewakuacji policzyć wszystkich uczniów i poinformować osobę odpowiedzialną za kierowanie działaniami kryzysowymi.
Poinformować rodziców o miejscu odbioru ich dzieci i drodze dojazdu.	Poinformować rodziców o miejscu odbioru dzieci i drodze dojazdu.

Sposób prowadzenia ewakuacji	Ewakuację można przeprowadzić tylko na wyraźną komendę administratora budynku (wyznaczonej osoby odpowiedzialnej za uruchomienie procedury) lub sił interweniujących i zgodnie z ich wskazówkami.
Telefony alarmowe	Policja 997; europejski telefon alarmowy 112
Sposób powiadamiania służb	Wybierz jeden z ww. numerów. Po zgłoszeniu się dyżurnego operatora danej służby podaj następujące informacje: • nazwa i adres szkoły • rodzaj stwierdzonego zagrożenia • własne imię i nazwisko oraz pełniona funkcja • telefon kontaktowy • zrealizowane działania. Potwierdź przyjęcie zgłoszenia i zapisz dane przyjmującego zgłoszenie.
Sposób postępowania z uczniami ze SPE	Nauczyciele odpowiedzialni za opiekę nad osobami niepełnosprawnymi dbają o zachowanie uczniów odpowiadające potrzebom danej sytuacji. W przypadku konieczności ewakuacji zapewniają pomoc, zgodnie z wcześniejszymi ustaleniami.
Zarządzanie w przypadku sytuacji kryzysowej	Czynnościami prowadzonymi w trakcie realizacji procedury kieruje dyrektor placówki, wicedyrektor lub osoba przez niego wyznaczona.

Obowiązki pracowników

- zapoznanie się z czynnościami realizowanymi w trakcie uruchamiania procedury;
- branie udziału w treningach i szkoleniach z zakresu stosowania procedury;
- znajomość sygnału uruchamiającego procedurę;
- posiadanie spisu numerów telefonu osób odpowiedzialnych za uruchomienie procedury i koordynację ewakuacji osób niepełnosprawnych;
- znajomość własnych zadań w przypadku uruchomienia procedury;
- znajomość miejsca ewakuacji;
- szkolenie uczniów w zakresie postępowania w przypadku uruchomienia procedury;
- stosowanie się do poleceń osoby zarządzającej sytuacja kryzysową.

1.5. Skażenie chemiczne lub biologiczne szkoły – procedury postępowania w przypadku uwolnienia się niebezpiecznych dla ludzi i środowiska substancji chemicznych oraz zastosowania broni biologicznej

Przez zagrożenie chemiczne rozumiemy uwolnienie niebezpiecznych dla ludzi i środowiska substancji chemicznych, mieszanin lub roztworów występujących w środowisku naturalnym lub powstałych w wyniku działalności człowieka. Zagrożenie może wynikać także z zastosowania broni biologicznej (broń B, broń bakteriologiczna). W broni B ładunki bojowe wypełnione są mikroorganizmami chorobotwórczymi: bakteriami (wąglik, bruceloza etc.), wirusami (ospa, gorączka krwotoczna, zapalenie mózgu, wirus HIV), toksynami (rycyna, dioksyna, toksyna otulinowa), grzybami lub pierwotniakami.

Sytuacja, w której mogło nastąpić skażenie szkoły (np. szkoła otrzymuje informację o możliwym skażeniu substancją chemiczną/biologiczną)

A. Skażenie otoczenia szkoły (np. pożar sąsiadującego ze szkołą magazynu z oponami lub środkami chemicznymi) – należy uciec do budynku, zamknąć okna.

   Należy wówczas:

   1. **Zaalarmować wszystkich przebywających na terenie szkoły, a osoby przebywające na zewnątrz ewakuować do budynku szkoły, przemieszczając się pod wiatr oraz poprzecznie do kierunku wiatru.**
   2. **Natychmiast po ogłoszeniu alarmu powiadomić odpowiednie służby** – policję, straż pożarną, pogotowie ratunkowe, kładąc szczególny nacisk na zawarcie w tym powiadomieniu informacji o charakterze potencjalnego ataku.
   3. **W budynku szkoły zamknąć i uszczelnić okna, drzwi, otwory wentylacyjne, wyłączyć klimatyzację.**
   4. **W miarę możliwości zgromadzić podręczne środki ratownicze i „odtrutki"** – maski pyłowe, gazę, watę, kwas octowy, sok cytrynowy, oliwę jadalną, wodę, wodę utlenioną, mydło, olej parafinowy, środki pobudzające krążenie, spirytus do przemywania skóry.

5. **Przygotować wilgotne tampony, np. z gazy, do ochrony dróg oddechowych, na wypadek przeniknięcia środka biologicznego lub chemicznego do wnętrza pomieszczeń** – częsta zmiana kompresu/gazy lub nawilżanie go wodą zabezpiecza przed nadmiernym pochłanianiem substancji przez osobę, która ją wdycha.
6. **Powstrzymać się od picia, spożywania posiłków, palenia papierosów oraz czynności wymagających dużego wysiłku.**
7. **Do chwili odwołania alarmu lub zarządzenia ewakuacji nie opuszczać uszczelnionych pomieszczeń, nie przebywać w pobliżu okien i innych otworów wentylacyjnych.**
8. **Oczekiwać na pojawienie się odpowiednich służb i postępować zgodnie z otrzymanymi od nich wytycznymi.**

B. Wewnętrzne skażenie budynku szkoły – należy ewakuować osoby przebywające w szkole, otwierając okna wszędzie, gdzie jest to możliwe, żeby wymusić cyrkulację powietrza. (Substancje toksyczne, np. gazy, mogą być lżejsze od powietrza (amoniak, chlor) lub cięższe od powietrza – np. tlenek węgla, azot).

Należy wówczas:

1. **Zaalarmować wszystkich przebywających na terenie szkoły, a osoby przebywające wewnątrz ewakuować z budynku szkoły.**
2. **Natychmiast po ogłoszeniu alarmu powiadomić odpowiednie służby** – policję, straż pożarną, pogotowie ratunkowe, kładąc szczególny nacisk na zawarcie w tym powiadomieniu informacji o charakterze potencjalnego ataku.
3. **W budynku szkoły otworzyć okna, drzwi, otwory wentylacyjne, włączyć klimatyzację.**
4. **W miarę możliwości zgromadzić podręczne środki ratownicze i „odtrutki"** – maski pyłowe, gazę, watę, kwas octowy, sok cytrynowy, oliwę jadalną, wodę, wodę utlenioną, mydło, olej parafinowy, środki pobudzające krążenie, spirytus do przemywania skóry.
5. **Przygotować wilgotne tampony, np. z gazy, do ochrony dróg oddechowych** – częsta zmiana kompresu/gazy lub nawilżanie go wodą zabezpiecza przed nadmiernym pochłanianiem substancji osobę, która ją wdycha.
6. **Powstrzymać się od picia, spożywania posiłków, palenia papierosów oraz czynności wymagających dużego wysiłku.**
7. **Do chwili odwołania alarmu lub zarządzenia ewakuacji nie wchodzić do pomieszczeń, przebywać w pobliżu okien i innych otworów wentylacyjnych.**
8. **Oczekiwać na pojawienie się odpowiednich służb i postępować zgodnie z otrzymanymi od nich wytycznymi.**

Sytuacja, w której szkoła została skażona substancją chemiczną/biologiczną, a zagrożenie wykryto natychmiast lub szybko po jego pojawieniu się

Należy wówczas:

1. **Powstrzymać się od dotykania i wąchania podejrzanych przedmiotów, sprzątania proszku, ścierania cieczy.**
2. **Aby zapobiec rozprzestrzenianiu się substancji, przykryć ją np. kocem.**
3. **Pozamykać okna oraz drzwi i wyłączyć klimatyzację, nie dopuścić do przeciągów.**
4. **Opuścić pomieszczenie, w którym wykryto obecność podejrzanej substancji i uniemożliwić dostęp do niego.**
5. **Powiadomić osobę odpowiedzialną za zarządzanie kryzysowe w szkole** – dyrektora, zastępcę dyrektora, osobę upoważnioną przez dyrekcję.
6. **Zaalarmować wszystkie osoby przebywające na terenie szkoły i skierować je w rejon ewakuacji, przemieszczając się pod wiatr oraz poprzecznie do kierunku wiatru** – rejonów ewakuacji powinno być kilka i powinny znajdować się w różnych kierunkach od szkoły, gdyż nie znamy kierunku wiatru w czasie przedmiotowego zagrożenia; rejonem ewakuacji powinien być budynek/budynki, a nie otwarta przestrzeń.
7. **Natychmiast po ogłoszeniu ewakuacji powiadomić odpowiednie służby** – policję, straż pożarną, pogotowie ratunkowe, kładąc szczególny nacisk na zawarcie w tym powiadomieniu informacji o charakterze potencjalnego zagrożenia.
8. **Jeśli miał miejsce kontakt z substancją: umyć dokładnie ręce wodą i mydłem, zdjąć ubranie, które miało kontakt z podejrzaną substancją, i włożyć je do plastikowego worka.**
9. **Po kontakcie z substancją nie wolno: jeść, pić, palić papierosów do czasu uzyskania zgody odpowiednich służb** – policji, straży pożarnej, wyspecjalizowanej jednostki zwalczania skażeń i zakażeń.
10. **Sporządzić listę osób (imię, nazwisko), które miały kontakt z podejrzaną substancją albo znalazły się w odległości ok. 5 m od niej; listę przekazać policji.**
11. **W miarę możliwości gromadzić podręczne środki ratownicze i „odtrutki"** – maski pyłowe, gazę, watę, kwas octowy, sok cytrynowy, oliwę jadalną, wodę, wodę utlenioną, mydło, olej parafinowy, środki pobudzające krążenie, spirytus do przemywania skóry.
12. **Przygotować wilgotne tampony do ochrony dróg oddechowych, na wypadek przeniknięcia środka biologicznego lub chemicznego do wnętrza pomieszczeń** – częsta zmiana kompresu/gazy lub nawilżanie go wodą zabezpiecza przed nadmiernym pochłanianiem substancji.
13. **Powstrzymać się od picia, spożywania posiłków, palenia papierosów oraz prac wymagających dużego wysiłku.**
14. **Oczekiwać na pojawienie się odpowiednich służb i postępować zgodnie z otrzymanymi od nich wytycznymi.**

Sytuacja, w której szkoła została skażona substancją chemiczną/biologiczną, a zagrożenie wykryto późno, np. gdy pojawiły się objawy reakcji na substancję lub/i ogniska zachorowań

Należy wówczas:

1. **Powstrzymać się od dotykania i wąchania podejrzanych przedmiotów, sprzątania proszku, ścierania cieczy.**
2. **Powiadomić osobę odpowiedzialną w szkole za zarządzanie kryzysowe** – dyrektora, zastępcę dyrektora, osobę upoważnioną przez dyrekcję.
3. **Przykryć substancję np. kocem, aby zapobiec jej rozprzestrzenianiu się,**
4. **Opuścić pomieszczenie, w którym wykryto obecność podejrzanej substancji i uniemożliwić dostęp do niego.**
5. **Ogłosić alarm i ewakuować do wnętrza szkoły wszystkich uczniów, nauczycieli oraz pracowników znajdujących się bezpośrednio poza budynkiem, a przebywających na terenie szkoły.**
6. **Natychmiast po ogłoszeniu alarmu powiadomić odpowiednie służby** – policję, straż pożarną, pogotowie ratunkowe, kładąc szczególny nacisk na zawarcie w tym powiadomieniu informacji o charakterze potencjalnego zagrożenia.
7. **Zamknąć i uszczelnić okna, drzwi, otwory wentylacyjne, wyłączyć klimatyzację, a budynek szkoły wraz ze wszystkimi obecnymi wewnątrz osobami odizolować od bezpośredniego otoczenia, przygotowując się do ewentualnej kwarantanny.**
8. **Oczekiwać na pojawienie się odpowiednich służb i postępować zgodnie z otrzymanymi od nich wytycznymi**.

Instrukcja postępowania w przypadku skażenia substancją chemiczną lub biologiczną terenu szkoły oraz zagrożenia skażeniem ww. substancjami

Osoby odpowiedzialne za zarządzanie Dyrektor lub wicedyrektor szkoły; w przypadku ich nieobecności – osoba przez nich upoważniona.	
Otrzymanie przez szkołę informacji o możliwym skażeniu substancją chemiczną/biologiczną – mogło nastąpić skażenie placówki	Zaalarmować wszystkich przebywających na terenie szkoły, osoby przebywające na zewnątrz ewakuować do budynku szkoły, przemieszczając się pod wiatr oraz poprzecznie do kierunku wiatru.
	Natychmiast po ogłoszeniu alarmu powiadomić odpowiednie służby.
	W budynku szkoły zamknąć i uszczelnić okna, drzwi, otwory wentylacyjne, wyłączyć klimatyzację.
	W miarę możliwości gromadzić podręczne środki ratownicze.
	Przygotować wilgotne tampony do ochrony dróg oddechowych, na wypadek przeniknięcia środka biologicznego lub chemicznego do wnętrza pomieszczeń.
	Powstrzymać się od picia, spożywania posiłków, palenia papierosów oraz prac wymagających dużego wysiłku.
	Do chwili odwołania alarmu lub zarządzenia ewakuacji nie opuszczać uszczelnionych pomieszczeń, nie przebywać w pobliżu okien i innych otworów wentylacyjnych.
	Oczekiwać na pojawienie się odpowiednich służb i postępować zgodnie z otrzymanymi od nich wytycznymi.
Skażenie szkoły substancją chemiczną/biologiczną – zagrożenie wykryto natychmiast lub szybko po jego pojawieniu się	Nie dotykać i nie wąchać podejrzanych przedmiotów, nie sprzątać proszku, nie ścierać cieczy.
	Aby zapobiec rozprzestrzenianiu się substancji, przykryć ją np. kocem.
	Pozamykać okna oraz drzwi i wyłączyć klimatyzację, nie dopuścić do przeciągów.
	Opuścić pomieszczenie, w którym wykryto obecność podejrzanej substancji i nie wpuszczać do niego innych osób.
	Powiadomić administratora.

Skażenie szkoły substancją chemiczną/biologiczną – zagrożenie wykryto natychmiast lub szybko po jego pojawieniu się	Zaalarmować wszystkie osoby przebywające na terenie szkoły i skierować je w rejon ewakuacji, przemieszczając się pod wiatr oraz poprzecznie do kierunku wiatru.
	Natychmiast po ogłoszeniu ewakuacji powiadomić odpowiednie służby.
	Jeśli miał miejsce kontakt z substancją, należy: umyć dokładnie ręce wodą i mydłem, zdjąć ubranie, które miało kontakt z podejrzaną substancją, i włożyć je do plastikowego worka.
	Po kontakcie z substancją nie wolno: jeść, pić, palić papierosów do czasu uzyskania zgody odpowiednich służb.
	W obiekcie – budynku, do którego nastąpiła ewakuacja, zamknąć i uszczelnić okna, drzwi, otwory wentylacyjne, wyłączyć klimatyzację.
	Sporządzić listę osób, które miały kontakt z podejrzaną substancją albo znalazły się w odległości ok. 5 m od niej. Listę przekazać policji.
	W miarę możliwości gromadzić podręczne środki ratownicze i odtrutki.
	Przygotować wilgotne tampony do ochrony dróg oddechowych, na wypadek przeniknięcia środka biologicznego lub chemicznego do wnętrza pomieszczeń.
	Powstrzymać się od picia, spożywania posiłków, palenia papierosów oraz prac wymagających dużego wysiłku.
	Oczekiwać na pojawienie się odpowiednich służb i postępować zgodnie z otrzymanymi od nich wytycznymi.
Skażenie szkoły substancją chemiczną/biologiczną – zagrożenie wykryto późno, np. gdy pojawiły się objawy reakcji na substancję lub/i ogniska zachorowań	Nie dotykać i nie wąchać podejrzanych przedmiotów, nie sprzątać proszku, nie ścierać cieczy.
	Powiadomić kierownictwo szkoły.
	Aby zapobiec rozprzestrzenianiu się substancji, przykryć ją np. kocem.
	Pozamykać okna oraz drzwi i wyłączyć klimatyzację, nie dopuścić do przeciągów.

Skażenie szkoły substancją chemiczną/biologiczną – zagrożenie wykryto późno, np. gdy pojawiły się objawy reakcji na substancję lub/i ogniska zachorowań	Opuścić pomieszczenie, w którym wykryto obecność podejrzanej substancji i nie wpuszczać do niego innych osób.
	Ogłosić alarm i ewakuować do wnętrza szkoły wszystkich uczniów, nauczycieli oraz pracowników znajdujących się bezpośrednio poza budynkiem, a przebywających na terenie szkoły.
	Natychmiast po ogłoszeniu alarmu powiadomić odpowiednie służby.
	Zamknąć i uszczelnić okna, drzwi, otwory wentylacyjne, wyłączyć klimatyzację, a budynek szkoły wraz ze wszystkimi obecnymi wewnątrz osobami odizolować od bezpośredniego otoczenia, przygotowując się do ewentualnej kwarantanny.
	Oczekiwać na pojawienie się odpowiednich służb i postępować zgodnie z otrzymanymi od nich wytycznymi.
Sposób prowadzenia ewakuacji	Ewakuację można przeprowadzić tylko na wyraźną komendę sił interweniujących i zgodnie z ich wskazówkami.
Sposób reakcji na sygnał dźwiękowy	W zależności od sytuacji: ewakuacja; wejście do budynku i pozostanie w nim.
Telefony alarmowe	Policja 997; straż pożarna 998; pogotowie ratunkowe 999; europejski telefon alarmowy 112
Sposób powiadamiania służb	Wybierz jeden z ww. numerów. Po zgłoszeniu się dyżurnego operatora danej służby podaj następujące informacje: • nazwa i adres szkoły • rodzaj stwierdzonego zagrożenia • własne imię i nazwisko oraz pełniona funkcja • telefon kontaktowy • zrealizowane działania. Potwierdź przyjęcie zgłoszenia i zapisz dane przyjmującego zgłoszenie
Sposób postępowania z uczniami ze SPE	Nauczyciele odpowiedzialni za opiekę na osobami niepełnosprawnymi dbają o zachowanie się dzieci zgodnie z potrzebami danej sytuacji. W przypadku konieczności ewakuacji zapewniają pomoc zgodnie z wcześniejszymi ustaleniami.

Zarządzanie w przypadku sytuacji kryzysowej	Czynnościami realizowanymi w trakcie procedury kieruje dyrektor placówki, wicedyrektor lub osoba przez niego wyznaczona.
Obowiązki pracowników: • zapoznanie się z czynnościami realizowanymi w trakcie uruchamiania procedury; • branie udziału w treningach i szkoleniach z zakresu stosowania procedury; • znajomość sygnału uruchamiającego procedurę; • posiadanie listy numerów telefonu osób odpowiedzialnych za uruchomienie procedury i koordynację ewakuacji osób niepełnosprawnych; • znajomość własnych zadań w przypadku uruchomienia procedury; • znajomość miejsca ewakuacji. • szkolenie uczniów w zakresie postępowania w przypadku uruchomienia procedury; • stosowanie się do poleceń osoby zarządzającej sytuacją kryzysową.	

1.6. Epidemia; kataklizm – procedury postepowania przypadku wystąpienia sytuacji nadzwyczajnych

Stan nadzwyczajny to sytuacja szczególnego zagrożenia, którego nie da się usunąć za pomocą narzędzi już funkcjonujących. Wymaga on sięgnięcia po szczególne środki prawne. Do stanów nadzwyczajnych zaliczamy stan wojenny, stan wyjątkowy oraz stan klęski żywiołowej.

W przypadku wystąpienia kataklizmu, epidemii, pandemii lub innego poważnego zagrożenia dla zdrowia i życia ludzkiego Rada Ministrów na wniosek właściwego wojewody lub z własnej inicjatywy, w drodze rozporządzenia, wprowadza stan klęski żywiołowej.

W czasie stanu klęski żywiołowej właściwy miejscowo wójt (burmistrz, prezydent miasta) kieruje działaniami prowadzonymi na obszarze gminy w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia.

W razie niezdolności do kierowania lub niewłaściwego kierowania działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia wojewoda z inicjatywy własnej lub na wniosek starosty może zawiesić uprawnienia wójta (burmistrza, prezydenta miasta) i wyznaczyć pełnomocnika do kierowania tymi działaniami.

Dyrektor szkoły, jego zastępca lub osoba wyznaczona przez dyrektora szkoły postępuje zgodnie z wytycznymi, które są mu przekazywane przez właściwy organ działający w celu zapobieżenia skutkom klęski żywiołowej.

2. Zagrożenia wewnętrzne i procedury reagowania w przypadku wystąpienia zagrożenia

2.1. Agresywne zachowania w szkole lub zjawisko tzw. fali – procedury postępowania w przypadku wystąpienia na terenie szkoły zachowań agresywnych, tj. agresji fizycznej i słownej ucznia lub nauczyciela

Do najważniejszych zagrożeń wewnętrznych w szkole należą: agresywne zachowania ucznia oraz zjawisko tzw. fali, korzystanie przez uczniów z substancji psychoaktywnych, kradzież, wymuszenia pieniędzy lub przedmiotów wartościowych, pedofilia i uwodzenie, pornografia, nieprawidłowe zachowania psychoseksualne, czyn karalny dokonany przez ucznia.

Zagrożeniom w szkole zwykle towarzyszą poprzedzające je lub towarzyszące im widoczne symptomy zachowań uczniów, na podstawie których można je rozpoznać. Ofiary negatywnych działań w szkole zwykle skarżą się na bóle głowy czy brzucha lub na brak apetytu. Często pojawia się u nich niechęć do chodzenia do szkoły (wagary) lub całkowita absencja. W rodzinie występują agresja wobec rodzeństwa i rodziców, widoczny niepokój, rozdrażnienie lub lękowe reagowanie na różne sytuacje. Uczniowie tacy izolują się i szukają samotności. Odbija się to negatywnie na ich wynikach w nauce. Nauczyciele i rodzice powinni zauważyć te zachowania i rozpocząć wyjaśnianie ich przyczyn. Należy pamiętać, że uczniowie na ogół ukrywają, iż stali się ofiarami czynów zabronionych, wstydzą się, nie chcą martwić nauczycieli lub rodziców. Niekiedy przypisują sobie winę za to, co ich spotkało.

Niewłaściwe zachowania uczniów stanowiące zagrożenie dla bezpieczeństwa w szkole mają wiele przyczyn:

1. Uwarunkowania osobowościowe sprawcy – np. zaburzenia rozwoju emocjonalnego, słabo rozwinięte kompetencje społeczne, nieumiejętność radzenia sobie z problemami w sposób konstruktywny; wpływ środowiska pozaszkolnego – otoczenia ucznia, uwarunkowań społeczno-rodzinnych.
2. Wpływ telewizji, internetu, gier komputerowych.
3. Oddziaływanie środowiska szkolnego: konflikty między rówieśnikami, negatywna dominacja starszych kolegów, próba zdobycia kontroli nad rówieśnikami, chęć imponowania, wyróżnienia się wśród społeczności szkolnej.
4. Funkcjonowanie szkoły – duża liczba uczniów, hałas, anonimowość uczniów, brak współpracy z rodzicami, policją, nieumiejętność zagospodarowania czasu wolnego uczniów czy brak zajęć pozalekcyjnych.
5. Błędy popełnianie przez nauczycieli w procesie kształcenia, wychowania i opieki – brak dbałości o pozytywny klimat w klasie, problemy w komunikacji z uczniem, niereagowanie na zachowania niewłaściwe.

Źródłem problemów w szkole może być też zestresowany i przemęczony nauczyciel, niepotrafiący poradzić sobie z agresją dzieci.

Zagrożenia wynikające z niewłaściwego funkcjonowania uczniów przejawiają się jako:

1. Systematyczne dokuczanie, wyśmiewanie, ośmieszanie, przezywanie, robienie sobie żartów, bicie, popychanie i kopanie.
2. Dominacja nad innymi, chęć podporządkowania ich sobie, używanie gróźb i siły.
3. Spadek zainteresowania szkołą.
4. Niechęć do podejmowania aktywności na rzecz społeczności lokalnej.
5. Niekontrolowane wybuchy gniewu, impulsywność.
6. Nastawienie „na nie " i agresja wobec dorosłych (w tym nauczycieli).
7. Brak poczucia winy i wstydu, a nawet zadowolenie z własnych negatywnych zachowań.
8. Zachowania aspołeczne: kradzież, wandalizm, picie alkoholu, przyjmowanie narkotyków.
9. Agresja w stosunku do zwierząt.
10. Fascynacja sytuacjami ukazującymi sceny przemocy, inicjowanie rozmów na tematy związane z używaniem niebezpiecznych narzędzi.
11. Ekspresja wyrażana w pracach szkolnych, ukierunkowana na zjawiska związane z przemocą, prace plastyczne obrazujące sceny agresji.
12. Nadmierne zainteresowanie funkcjonowaniem grup przestępczych (próby nawiązania kontaktu).
13. Rozmowy na tematy związane z bronią, przynoszenie na teren szkoły niebezpiecznych narzędzi (m.in. noży, broni palnej, materiałów wybuchowych).

Przyczyną zagrożeń mogą być niewłaściwe postawy i zachowania nauczycieli, takie jak:

1. Drwina i złośliwość wobec uczniów.
2. Wywieranie presji psychicznej, ośmieszanie, lekceważenie uczniów.
3. Agresja słowna – dokuczanie, wyśmiewanie.
4. Naruszanie nietykalności cielesnej.
5. Groźby w stosunku do ucznia.
6. Źle rozumiana solidarność zawodowa – nauczyciele bronią siebie nawzajem, by zachować dobre imię, nie ujawniając przypadków niewłaściwego traktowania ucznia przez innych nauczycieli.

Rekomendowane działania w szkole
Każdy sygnał świadczący o zaistnieniu zagrożenia należy traktować z powagą i przeciwdziałać mu na możliwie wczesnym etapie jego powstawania.
Należy dać uczniowi możliwość poinformowania nauczyciela lub pedagoga o zaistniałej sytuacji związanej z czynnością niebezpieczną, budując atmosferę zaufania.
Należy zawsze wyciągać konsekwencje w stosunku do osób dopuszczających się czynów zabronionych.
W ramach działań profilaktycznych podczas lekcji wychowawczych, we współpracy z ekspertami i specjalistami, należy informować uczniów o konsekwencjach związanych z zagrożeniami w szkole, jak i poza nią.
Należy tworzyć przyjazne środowisko pracy i nauki – klimat społeczny – poprzez sprawiedliwe ocenianie, jasne, czytelne normy, przyjazny nadzór nad uczniami, sprawną organizację życia szkolnego.
Należy podejmować działania integrujące zespoły klasowe, poznawanie się uczniów, sprzyjające budowaniu pozytywnych relacji w klasie.
Należy budować dobre relacje nauczyciela z uczniami, np.: jasno określać zasady pracy i wymagania wobec uczniów, szanować ucznia i udzielać mu wsparcia, sprawować kontrolę w klasie i interweniować w razie zachowania naruszającego normy.
Należy diagnozować sytuacje w szkole w kontekście występowania zagrożeń wewnętrznych, przeciwdziałania im i usuwania ich oraz monitorować postępy i efekty wprowadzonych działań.
Niezbędna jest edukacja, kierowana do nauczycieli, osób współpracujących z uczniami i rodziców w zakresie rozwiązywania problemów.
Należy organizować w szkole zajęcia profilaktyczne dla rodziców.

Niektóre z czynów stanowiących fizyczne zagrożenie wewnętrzne w szkole noszą znamiona czynów zabronionych. Należy pamiętać, że na zasadach określonych w *Kodeksie karnym* odpowiada osoba, która popełniła czyn zabroniony po ukończeniu 17 lat. Określa to art. 10 § 1 *Kodeksu karnego*. Także niektóre czyny osoby, która ukończyła 15 lat rozpatrywane są jako przestępstwa – określa je szczegółowo art. 10 § 2 kk. Nie oznacza to jednak, że odpowiedzialności nie mogą podlegać osoby młodsze. Odpowiedzialność przed sądem rodzinnym i dla nieletnich ponoszą osoby, które w chwili popełnienia czynu ukończyły 13 lat, jednak taki czyn nie stanowi przestępstwa, a jedynie jest klasyfikowany jako czyn karalny zaś, sprawca podlega stosowaniu środków wychowawczych przewidzianych w *Ustawie o postępowaniu w sprawach nieletnich*.

Procedury postępowania w przypadku najczęściej występujących fizycznych zagrożeń wewnętrznych

Agresywne zachowania ucznia w szkole lub przypadki tzw. fali	
Cel uruchomienia procedury	Zapewnienie bezpieczeństwa fizycznego w szkole na wypadek wystąpienia na jej terenie zachowań agresywnych, tj. agresji fizycznej i agresji słownej ucznia wobec ucznia lub wobec nauczyciela.
Osoby odpowiedzialne za zarządzanie	Procedura postępowania jest uruchamiana przez osobę, która zauważyła przedmiotowe zachowanie lub której je zgłoszono. O stopniu zaawansowania procedury i podejmowanych krokach decyduje dyrektor placówki, a w przypadku jego nieobecności wicedyrektor lub pedagog szkolny. Czynnościami podejmowanymi w trakcie realizacji procedury kieruje dyrektor placówki, wicedyrektor lub osoba przez niego wyznaczona.
Sposób postępowania	**1. Agresja fizyczna** • Należy bezzwłocznie podjąć działania mające na celu powstrzymanie i wyeliminowanie tego zjawiska. Obowiązkiem każdego pracownika szkoły, który zaobserwował atak agresji fizycznej lub został o nim poinformowany, jest przerwanie tego zachowania. Pracownik szkoły powinien w sposób stanowczy i zdecydowany przekazać uczestnikom zdarzenia, że nie wyraża zgody na takie zachowanie. Należy mówić dobitnie, głośno, stanowczo, używać krótkich komunikatów. W razie potrzeby należy zadbać o rozdzielenie bijących się uczniów i uniemożliwienie im dalszego kontaktu. • W przypadku zagrożenia życia (gdy osoba poszkodowana jest nieprzytomna) pielęgniarka, pedagog/psycholog lub dyrektor szkoły wzywa natychmiast karetkę pogotowia, nawet bez uzyskania zgody rodziców (opiekunów prawnych). • Opiekę nad uczniem podczas udzielania pomocy medycznej, ale bez możliwości udzielenia zgody na operację, sprawuje osoba wyznaczona przez dyrektora szkoły. • Decyzję o dalszym leczeniu dziecka podejmują rodzice/opiekunowie prawni poszkodowanego. • Pedagog/psycholog szkolny i wychowawcy klas przeprowadzają rozmowy z rodzicami/opiekunami prawnymi obydwu stron oraz ze sprawcą i ofiarą. Z rozmów sporządzają notatkę.

Sposób postępowania	• Pedagog/psycholog szkolny powinien udzielić specjalistycznej pomocy ofierze przemocy oraz wskazać, jak należy radzić sobie w podobnych sytuacjach. • Należy przeprowadzić rozmowę ze świadkami zdarzenia, wyjaśnić im pojęcia: emocje, agresja, przemoc, przypomnieć normy postępowania i sposoby reagowania. • Należy ustalić działania w podobnych przypadkach oraz zweryfikować stosowane w szkole narzędzia i metody pracy wychowawczej, opiekuńczej i profilaktycznej. • W przypadku przeprowadzenia przez agresora kolejnych ataków – z widocznymi skutkami pobicia – szkoła kieruje sprawę na policję, od której postępowania zależą dalsze losy sprawcy przemocy. Wobec agresora stosuje się konsekwencje przewidziane w statucie i/lub regulaminie szkoły. **2. Agresja słowna** • Należy bezzwłocznie podjąć działania mające na celu powstrzymanie i wyeliminowanie tego zjawiska. • Należy powiadomić wychowawcę klasy i/lub dyrektora, pedagoga/psychologa. • Wychowawca (pedagog lub psycholog) przeprowadza z uczniem rozmowę mającą na celu wyjaśnienie okoliczności zdarzenia. Rozmowy z ofiarą i agresorem należy przeprowadzić osobno. • Wychowawca (pedagog/psycholog) przeprowadza rozmowy ze sprawcą i ofiarą w celu ustalenia okoliczności zdarzenia, uzgadnia wraz ze sprawcą formę zadośćuczynienia. • O zaistniałym zdarzeniu należy poinformować rodziców/opiekunów prawnych uczestników zdarzenia. • Pedagog/psycholog szkolny powinien udzielić pomocy specjalistycznej ofierze przemocy, wskazać, jak należy radzić sobie w podobnych sytuacjach. • Należy przeprowadzić rozmowę ze świadkami zdarzenia, wyjaśnić im pojęcia: emocje, agresja, przemoc, przypomnieć normy postępowania i sposoby reagowania. • W poważnych przypadkach, np. uzyskania informacji o popełnieniu przestępstwa ściganego z urzędu lub przestępstwa ściganego na wniosek poszkodowanego, powiadamiana jest policja. • Wobec ucznia przejawiającego zachowania agresywne stosuje się konsekwencje przewidziane w statucie lub regulaminie szkoły. • Należy zweryfikować stosowane w szkole narzędzia i metody pracy wychowawczej, opiekuńczej i profilaktycznej.

Obowiązki pracowników	• zapoznanie się z czynnościami realizowanymi w trakcie uruchamiania procedury; • branie udziału w szkoleniach z zakresu stosowania procedury; • posiadanie listy numerów telefonu osób odpowiedzialnych za uruchomienie procedury; • znajomość własnych zadań w przypadku uruchomienia procedury; • szkolenie uczniów w zakresie działań prowadzonych w ramach procedury; • stosowanie się do poleceń osoby zarządzającej sytuacją trudną lub kryzysową.

2.2. Substancje psychoaktywne – procedura postępowania w przypadku znalezienia w szkole substancji psychoaktywnych

Znalezienie w szkole substancji psychoaktywnych	
Cel uruchomienia procedury	Zapewnienie zdrowia i bezpieczeństwa fizycznego, psychicznego i emocjonalnego uczniów przebywających w szkole/placówce w sytuacji zagrożeń wewnętrznych związanych z rozprowadzaniem niebezpiecznych środków odurzających oraz odurzeniem alkoholem, narkotykami lub „dopalaczami".
Osoby odpowiedzialne za zarządzanie	Dyrektor szkoły, pedagog/psycholog szkolny.
Podstawy uruchomienia procedury	Wystąpienie zagrożenia: (1) rozpowszechnianiem środków odurzających (narkotyków, dopalaczy) lub alkoholu, (2) zdrowia ucznia po użyciu środka odurzającego lub spożycia alkoholu oraz (3) zdrowia ucznia w wyniku wypadku w szkole lub poza nią.
Sposób postępowania	**1. W przypadku znalezienia podejrzanej substancji odurzającej na terenie szkoły, należy**: • zachować szczególne środki ostrożności; • zabezpieczyć substancję przed dostępem do niej uczniów oraz jej ewentualnym zniszczeniem; • powiadomić dyrektora szkoły, który zawiadamia policję; • ustalić (jeżeli to możliwe), do kogo należy znaleziona substancja; • przekazać policji zabezpieczoną substancję oraz informację o zaistniałej sytuacji; • opracować i przeprowadzić projekty edukacyjne dotyczące ww. problematyki oraz wdrożyć profilaktykę uzależnień.

Sposób postępowania	2. **W przypadku podejrzenia ucznia o posiadanie środków odurzających należy**: • odizolować podejrzanego od pozostałych uczniów w klasie; • powiadomić pedagoga/psychologa szkolnego; • powiadomić dyrektora szkoły, który zawiadomi policję; • zażądać od ucznia, w obecności innej osoby/pedagoga, przekazania posiadanej substancji i/lub pokazania zawartości plecaka oraz kieszeni; • powiadomić rodziców/prawnych opiekunów ucznia; • poinformować rodziców o procedurach obowiązujących w szkole/placówce; • przeprowadzić z uczniem w obecności jego rodziców/opiekunów prawnych rozmowę o złamaniu obowiązujących zasad szkolnych, a następnie objąć ucznia działaniami profilaktycznymi; wsparcia należy udzielić również rodzicom/opiekunom prawnym ucznia; • zaproponować rodzicom/opiekunom prawnym działania profilaktyczne w zakresie rozpoznawania sygnałów ostrzegawczych oraz posiadania i rozprowadzania środków odurzających, bądź specjalistyczne, np. uczestnictwo w warsztatach umiejętności wychowawczych.
	3. **W przypadku rozpoznania u ucznia stanu odurzenia alkoholem należy**: • powiadomić wychowawcę klasy ucznia; • odizolować ucznia od pozostałych uczniów w klasie; • powiadomić pedagoga/psychologa szkolnego; • przekazać ucznia pod opiekę pielęgniarki/pedagoga szkolnego/psychologa szkolnego; • powiadomić dyrektora szkoły o zaistniałej sytuacji; • powiadomić rodziców/opiekunów prawnych ucznia oraz prosić ich o przybycie do szkoły/placówki; • poinformować rodziców/opiekunów prawnych o obowiązującej w szkole procedurze postępowania w przypadku znalezienia w szkole substancji psychoaktywnych, a następnie objąć ucznia działaniami profilaktycznymi; wsparcia udzielić również rodzicom/opiekunom prawnym ucznia; • przeprowadzić rozmowę z rodzicami, opisując zagrożenie zdrowia dziecka, wskazać instytucje, które mogą służyć pomocą w zaistniałej sytuacji; • w przypadku wystąpienia stanu nagłego zagrożenia zdrowia powiadomić jednostkę państwowego ratownictwa medycznego.

Sposób postępowania	4. **W przypadku rozpoznania stanu odurzenia ucznia narkotykami, w tym „dopalaczami”**: • przekazać uzyskaną informację wychowawcy klasy; • poinformować pielęgniarkę/pedagoga szkolnego/psychologa szkolnego; • w momencie rozpoznania odizolować ucznia od pozostałych rówieśników w klasie; • przekazać ucznia pod opiekę pielęgniarki/pedagoga szkolnego/psychologa szkolnego; • poinformować dyrektora szkoły o zaistniałej sytuacji; • wezwać do szkoły rodziców/opiekunów prawnych ucznia; • przekazać rodzicom informację o obowiązującej procedurze postępowania; • przeprowadzić rozmowę z rodzicami/opiekunami prawnymi oraz z uczniem; • zobowiązać rodziców/opiekunów prawnych do pomocy dziecku w zaprzestaniu odurzania się, wskazać działania i instytucje mogące służyć pomocą w zaistniałej sytuacji; • opracować działania profilaktyczne do zrealizowania z uczniem; • uwzględnić w programie wychowawczo-profilaktycznym zdiagnozowane obszary; • monitorować i ewaluować efekty oddziaływań profilaktycznych; • w przypadku wystąpienia stanu nagłego zagrożenia zdrowia powiadomić jednostkę państwowego ratownictwa medycznego.
	5. **W przypadku odmowy współpracy rodziców/opiekunów prawnych**: • szkoła pisemnie powiadamia o zaistniałej sytuacji sąd rodzinny lub policję oraz pomoc społeczną; • szkoła współpracuje z instytucjami w zakresie pomocy i wsparcia ucznia na mocy obowiązujących przepisów prawa.
Obowiązki pracowników	• zapoznanie się ze skutecznymi działaniami profilaktycznymi; • umiejętność rozpoznawania rodzajów i wyglądu środków odurzających; • znajomość symptomów wskazujących na odurzenie narkotykiem; • znajomość symptomów nadużycia alkoholu; • regularne prowadzenie zajęć profilaktycznych dotyczących zagrożenia zdrowia substancjami psychoaktywnymi; • systematyczne prowadzenie zajęć na temat stosowania obowiązującego prawa, dotyczących zdrowia i bezpieczeństwa uczniów;

Obowiązki pracowników	• realizowanie z uczniami projektów edukacyjnych na temat współczesnych zagrożeń; • prowadzenie cyklicznych szkoleń dla rodziców na temat zagrożeń zdrowia dzieci; • prowadzenie ciągłej obserwacji uczniów w zakresie ich zdrowia i bezpieczeństwa; • opracowanie listy instytucji pomocowych zajmujących się uzależnieniami, dostępnych w lokalnym środowisku; • zapoznawanie się z bazą programów rekomendowanych i wdrażanie ich zgodnie z potrzebami w swojej szkole (www.programyrekomendowane.pl).

2.3. Kradzież; wymuszanie – procedura postępowania w przypadku wystąpienia w szkole kradzieży bądź wymuszenia pieniędzy lub przedmiotów wartościowych

Kradzież bądź wymuszenie pieniędzy lub przedmiotów wartościowych	
Cel uruchomienia procedury	Określenie sposobu postępowania w przypadkuk stwierdzenia w szkole kradzieży bądź wymuszenia pieniędzy lub przedmiotów wartościowych, dokonanych przez ucznia.
Osoby odpowiedzialne za zarządzanie	Za uruchomienie i anulowanie procedury oraz kierowanie koniecznymi działaniami odpowiadają kolejno: dyrektor placówki, w przypadku jego nieobecności wicedyrektor, a w przypadku jego nieobecności pedagog/psycholog szkolny.
Sposób postępowania	• bezzwłoczne podjęcie działań mających na celu powstrzymanie i niwelowanie tego zjawiska; • bezzwłoczne powiadomienie dyrektora przez osobę, która wykryła kradzież; • zażądanie, aby podejrzewany uczeń pokazał zawartość torby szkolnej oraz kieszeni we własnej odzieży lub przekazał skradzioną rzecz, w obecności innej osoby, np. wychowawcy klasy, pedagoga szkolnego, psychologa, dyrektora lub innego pracownika szkoły (należy pamiętać, że pracownik szkoły nie ma prawa samodzielnie wykonać czynności przeszukania odzieży ani plecaka ucznia – może to zrobić tylko policja; • zabezpieczenie dowodów, tj. przedmiotów pochodzących z kradzieży lub wymuszenia i przekazanie ich policji; • przekazanie sprawcy czynu (o ile jest znany i przebywa na terenie szkoły) pod opiekę pedagoga szkolnego lub dyrektora szkoły;

Sposób postępowania	• ustalenie we współpracy z pedagogiem szkolnym okoliczności czynu i ewentualnych świadków zdarzenia; • wezwanie przez dyrektora rodziców/opiekunów prawnych sprawcy i przeprowadzenie rozmowy z uczniem w ich obecności; należy sporządzić notatkę z tej rozmowy, podpisaną przez rodziców/opiekunów prawnych; • doprowadzenie do zadośćuczynienia przez sprawcę, w porozumieniu z jego rodzicami, poszkodowanemu w kradzieży; • powiadomienie policji; • podjęcie innych czynności w zależności od regulacji zawartych w statucie szkoły.
Obowiązki pracowników	• zapoznanie się z czynnościami realizowanymi w trakcie uruchamiania procedury; • wzięcie udziału w treningach i szkoleniach z zakresu stosowania procedury; • posiadanie listy numerów telefonu osób odpowiedzialnych za uruchomienie procedury; • znajomość własnych zadań w przypadku uruchomienia procedury; • stosowanie się do poleceń osoby zarządzającej procedurą.

2.4. Pedofilia i uwodzenie – procedura postępowania w przypadku wystąpienia zjawiska pedofilii w szkole

Pedofila jest przestępstwem przeciwko wolności seksualnej i obyczajności. W myśl *Kodeksu karnego*, art. 200 § 1: „Kto obcuje płciowo z małoletnim poniżej lat 15 lub dopuszcza się wobec takiej osoby innej czynności seksualnej lub doprowadza ją do poddania się takim czynnościom albo do ich wykonania, podlega karze pozbawienia wolności od lat 2 do 12."

Wystąpienie zjawiska pedofilii w szkole	
Cel uruchomienia procedury	Zapewnienie bezpieczeństwa fizycznego, psychicznego i emocjonalnego uczniów w przypadku wystąpienia zagrożenia wewnętrznego, wynikającego z pojawienia się osób psychicznie i fizycznie molestujących dzieci lub nakłaniających je do wykonywania czynności seksualnych.
Osoby odpowiedzialne za zarządzanie	Dyrektor lub wicedyrektor szkoły; w przypadku ich nieobecności – osoba przez nich upoważniona.

Sposób postępowania	• bezzwłoczne podjęcie działań mających na celu powstrzymanie tego zjawiska; • po stwierdzeniu zagrożenia powiadomienie dyrektora oraz pedagoga/psychologa szkolnego; • w przypadku potwierdzenia informacji o pojawianiu się osób obcych, zaczepiających uczniów, bezzwłoczne powiadomienie policji; • przekazanie przez dyrektora wszystkim pracownikom szkoły informacji o stwierdzonym zagrożeniu; • podjęcie przez wychowawców oraz pedagoga/psychologa szkolnego działań profilaktycznych skierowanych do uczniów w celu omówienia potencjalnego zagrożenia oraz wskazania możliwych form przekazywania pracownikom szkoły informacji o osobach, które mogą stwarzać zagrożenie; • w przypadku stwierdzenia, że uczeń był molestowany, bezzwłoczne powiadomienie rodziców/prawnych opiekunów ucznia oraz policji w celu przeprowadzenia czynności sprawdzających, które umożliwią ustalenie sprawcy; • wezwanie do szkoły rodziców/prawnych opiekunów ucznia przez dyrektora; • przeprowadzenie przez pedagoga/psychologa szkolnego indywidualnej rozmowy z uczniem – omówienie w obecności rodziców przyczyn i okoliczności zdarzenia; • ustalenie przez dyrektora, w porozumieniu z rodzicami/prawnymi opiekunami ucznia oraz pedagogiem/psychologiem szkolnym, dalszych działań mających na celu zapewnienie uczniowi właściwej opieki.
Podstawy prawne uruchomienia procedury	*Kodeks karny*: art. 197 § 3; art. 200; art. 200a; art. 200b.

2.5. Pornografia – procedury postępowania w przypadku rozpowszechniania przez ucznia pornografii w szkole

Przypadek rozpowszechniania pornografii w szkole przez ucznia	
Cel uruchomienia procedury	Zapewnienie bezpieczeństwa fizycznego, psychicznego i emocjonalnego uczniów na wypadek zagrożenia wewnętrznego, związanego z rozpowszechnianiem materiałów o charakterze pornograficznym.
Osoby odpowiedzialne za zarządzanie	Dyrektor lub wicedyrektor szkoły; w przypadku ich nieobecności – osoba przez nich upoważniona.

Sposób postępowania	• w przypadku otrzymania przez nauczyciela/rodzica lub inną osobę informacji o rozpowszechnianiu przez ucznia pornografii w internecie lub szkole bezzwłoczne powiadomienie dyrektora szkoły oraz administratora sieci o zaistniałym zdarzeniu; • w przypadku, gdy uczeń przekazuje informację o osobach, które pokazywały materiały pornograficzne, zapewnienie mu anonimowości w celu uniknięcia ewentualnych konsekwencji związanych z przemocą skierowaną wobec tego ucznia ze strony sprawców zdarzenia; • przekazanie przez dyrektora pracownikom szkoły informacji o stwierdzonym zagrożeniu bez wskazywania konkretnego ucznia; • podjęcie przez wychowawcę klasy i pedagoga/psychologa szkolnego działań profilaktycznych wśród uczniów w celu omówienia zagrożeń, jakie niesie za sobą upublicznianie materiałów o charakterze pornograficznym, oraz wskazania możliwych konsekwencji tego typu działań; • wezwanie przez dyrektora do szkoły rodziców/prawnych opiekunów ucznia, który rozpowszechniał materiały pornograficzne; • przeprowadzenie przez wychowawcę lub pedagoga, psychologa szkolnego rozmowy z rodzicami/prawnymi opiekunami ucznia sprawcy na temat zdarzenia.

2.6. Nieprawidłowe zachowania psychoseksualne w szkole – procedury postępowania w przypadku wystąpienia prostytucji

Przypadek prostytucji wśród uczniów	
Cel uruchomienia procedury	Zapewnienie bezpieczeństwa fizycznego, psychicznego i emocjonalnego uczniów w przypadku zagrożenia wewnętrznego, związanego z prostytucją w szkole lub wśród uczniów.
Osoby odpowiedzialne za zarządzanie	Dyrektor lub wicedyrektor szkoły; w przypadku ich nieobecności – osoba przez nich upoważniona.
Sposób postępowania	• w przypadku otrzymania informacji o sytuacji, w której uczeń był świadkiem czynności noszących znamiona prostytucji, powiadomienie o zaistniałym wydarzeniu dyrektora szkoły przez nauczyciela przyjmującego zgłoszenie; • w przypadku stwierdzenia przez pracownika/nauczyciela, że uczeń świadomie lub nie, dopuszczał się czynności, które mogłyby być uznane za prostytuowanie się, wezwanie do szkoły rodziców/prawnych opiekunów ucznia;

Sposób postępowania	• przeprowadzenie przez wychowawcę rozmowy z rodzicami/opiekunami prawnymi oraz z uczniem w ich obecności; w przypadku potwierdzenia informacji zobowiązanie ucznia do zaniechania negatywnego postępowania, zaś rodziców/opiekunów prawnych – bezwzględnie do szczególnego nadzoru nad jego zachowaniem (w toku interwencji profilaktycznej ewentualne skierowanie do specjalistycznej placówki i udział ucznia w programie terapeutycznym); • jeżeli rodzice/opiekunowie prawni ucznia odmawiają współpracy lub nie stawiają się do szkoły, a nadal z wiarygodnych źródeł napływają informacje o przejawach demoralizacji ich dziecka, pisemne powiadomienie przez dyrektora szkoły o zaistniałej sytuacji sądu rodzinnego lub policji (specjalisty ds. nieletnich); • w sytuacji, gdy szkoła wykorzystała wszystkie dostępne jej środki oddziaływań wychowawczo-profilaktycznych (rozmowa z rodzicami, ostrzeżenia ucznia, spotkania z pedagogiem, psychologiem itp.), a ich zastosowanie nie przynosi oczekiwanych rezultatów, powiadomienie przez dyrektora szkoły sądu rodzinnego lub policji (dalszy tok postępowania leży w kompetencji tych instytucji); • ustalenie przez dyrektora szkoły, w porozumieniu z rodzicami/prawnymi opiekunami dalszych działań z udziałem psychologa w celu zapewnienia opieki uczniowi, który świadomie lub nie dopuścił się czynności, które mogłyby być uznane za prostytuowanie się.
Podstawa prawna	*Kodeks karny*: art. 18 § 3; art. 203; art. 204.

2.7. Procedura postępowania w sytuacji wystąpienia niepokojących zachowań seksualnych uczniów w szkole

Niepokojące zachowania seksualne uczniów w szkole	
Cel uruchomienia procedury	Zapewnienie bezpieczeństwa fizycznego, psychicznego i emocjonalnego uczniów w przypadku zagrożenia wewnętrznego, związanego z zachowaniami uczniów o charakterze seksualnym.
Osoby odpowiedzialne za zarządzanie	Dyrektor lub wicedyrektor szkoły; w przypadku ich nieobecności – osoba przez nich upoważniona.

Sposób postępowania	• powiadomienie przez nauczyciela lub innego pracownika szkoły wychowawcy klasy i/lub pedagoga/psychologa szkolnego o przypadkach niepokojących zachowań seksualnych uczniów w szkole (gdy uczeń przekazuje nauczycielowi informację o niepokojących zachowaniach seksualnych innego ucznia, konieczne jest zapewnienie mu anonimowości w celu uniknięcia ewentualnej przemocy/odwetu); • przeprowadzenie przez wychowawcę lub pedagoga/psychologa szkolnego rozmowy z uczniem oraz poinformowanie o zaistniałym zdarzeniu rodziców ucznia; • zobowiązanie rodziców przez wychowawcę lub pedagoga/psychologa szkolnego do szczególnego nadzoru nad dzieckiem oraz ustalenie z nimi dalszego postępowania, w przypadku gdy rozmowa z uczniem okazuje się niewystarczająca do zmiany jego zachowania; • w sytuacji, kiedy rodzice odmawiają współpracy lub nie reagują na wezwanie do pojawienia się w szkole, a szkoła wykorzystała dostępne jej metody oddziaływań i zachowanie ucznia nie zmienia się, pisemne powiadomienie przez dyrektora szkoły wydziału rodzinnego i nieletnich sądu rejonowego oraz wydziału ds. nieletnich policji; • powiadomienie przez pedagoga/psychologa szkolnego, w porozumieniu z dyrektorem, najbliższej jednostki policji (po uprzednim zawiadomieniu o zajściu rodziców/opiekunów prawnych ucznia), w przypadku, gdy zachowanie ucznia świadczy o możliwości popełnienia przez niego przestępstwa (np. gwałtu); sporządzenie notatki służbowej na temat całego zdarzenia przez pedagoga/psychologa szkolnego.

2.8. Wypadek ucznia w szkole – procedury postępowania pracowników szkoły gwarantujące poszkodowanemu w wypadku uczniowi należytą opiekę i niezbędną pomoc

Wypadek ucznia/uczniów w szkole	
Cel uruchomienia procedury	Zapewnienie profesjonalnych działań pracowników szkoły, gwarantujących uczniowi poszkodowanemu w wypadku w szkole należytą opiekę i niezbędną pomoc.
Osoby odpowiedzialne za zarządzanie	Dyrektor lub wicedyrektor szkoły, a w przypadku ich nieobecności – osoba upoważniona przez nich.

Sposób postępowania	Wypadek ucznia jest to nagłe zdarzenie wywołane przyczyną zewnętrzną, powodujące uraz lub śmierć, które nastąpiło w czasie pozostawania ucznia pod opieką szkoły: na terenie szkoły lub poza jej terenem (w trakcie wycieczki lub wyjścia pod opieką nauczycieli).
	1. Udzielenie poszkodowanemu pierwszej pomocy przedmedycznej Pracownik szkoły, który otrzymał wiadomość o wypadku ucznia, niezwłocznie zapewnia poszkodowanemu opiekę, w szczególności sprowadzając fachową pomoc medyczną, a w miarę możliwości udzielając poszkodowanemu pierwszej pomocy. Udzielenie pierwszej pomocy w wypadkach jest prawnym obowiązkiem każdego pracownika szkoły. Jej nieudzielenie, szczególnie przez osobę odpowiedzialną za bezpieczeństwo ucznia, skutkuje sankcją karną. Gdy do wypadku ucznia dochodzi podczas lekcji nauczyciel przerywa ją, wyprowadzając uczniów z miejsca zagrożenia – jeżeli warunki w miejscu, w którym prowadzone są zajęcia, stwarzają nadal zagrożenie dla bezpieczeństwa uczniów. Pracownik zobowiązany jest do niezwłocznego powiadomienia dyrektora szkoły o sytuacji. **2. Obowiązek powiadamiania i zabezpieczenia miejsca zdarzenia** O każdym wypadku zawiadamia się niezwłocznie: rodziców/opiekunów prawnych poszkodowanego, pracownika szkoły odpowiedzialnego za bezpieczeństwo i higienę pracy, społecznego inspektora pracy, organ prowadzący szkołę lub placówkę oraz radę rodziców. O wypadku śmiertelnym, ciężkim i zbiorowym zawiadamia się niezwłocznie prokuratora. O wypadku, do którego doszło w wyniku zatrucia, zawiadamia się niezwłocznie państwowego inspektora sanitarnego. Zawiadomienia dokonuje dyrektor lub upoważniony przez niego pracownik szkoły. Fakt ten powiadamiający dokumentuje w sposób ustalony w danej szkole (podając datę i godzinę powiadomienia rodziców/opiekunów prawnych ucznia o wypadku). W niegroźnych przypadkach (brak wyraźnych obrażeń – np. widoczne tylko lekkie zaczerwienienie, zadrapanie, lekkie skaleczenie), po udzieleniu pierwszej pomocy poszkodowanemu uczniowi, nauczyciel/wychowawca ustala potrzebę wezwania pogotowia ratunkowego oraz potrzebę wcześniejszego przyjścia rodzica/opiekuna prawnego i godzinę odbioru dziecka ze szkoły w dniu zdarzenia.

Sposób postępowania	W przypadku wezwania pogotowia ratunkowego w szkole powinni przebywać powiadomieni przez szkołę rodzice. Jeżeli lekarz stwierdzi konieczność hospitalizacji, rodzice jadą razem z dzieckiem do szpitala. Jeżeli rodzice nie dotarli do szkoły przed odjazdem karetki pogotowia (ciężki wypadek, osoba wymagająca natychmiastowej pomocy), razem z dzieckiem jedzie do szpitala dyrektor lub pracownik wskazany przez dyrektora szkoły. Informację o powyższych ustaleniach przekazuje się rodzicom/prawnym opiekunom ucznia oraz dokumentuje. W każdym przypadku, gdy widoczne są obrażenia, urazy, niepokojące objawy, dyrektor lub upoważniona osoba wzywa pogotowie ratunkowe. Jeżeli wypadek został spowodowany niesprawnością techniczną pomieszczenia lub urządzeń, należy zabezpieczyć je nienaruszone do momentu pojawienia się odpowiednich służb. Dyrektor zabezpiecza je do czasu dokonania oględzin lub wykonania szkicu przez zespół powypadkowy. Jeżeli wypadek zdarzył się w czasie wyjścia, imprezy organizowanej poza terenem szkoły, wszystkie stosowne decyzje podejmuje opiekun grupy/kierownik wycieczki i odpowiada za nie oraz powiadamia właściwe służby (pogotowie, policję itp.). Do czasu rozpoczęcia pracy przez zespół powypadkowy dyrektor zabezpiecza miejsce wypadku w sposób wykluczający dopuszczenie osób niepowołanych. Jeżeli czynności związanych z zabezpieczeniem miejsca wypadku nie może wykonać dyrektor, wykonuje je upoważniony przez dyrektora pracownik szkoły. **3. Zespół powypadkowy** Dyrektor szkoły powołuje zespół powypadkowy. W jego skład wchodzi z zasady pracownik odpowiedzialny za bezpieczeństwo i higienę pracy oraz społeczny inspektor pracy. Jeżeli z jakichkolwiek powodów nie jest możliwy udział w pracach zespołu jednej z osób – dyrektor powołuje w jej miejsce innego pracownika szkoły lub placówki przeszkolonego w zakresie bezpieczeństwa i higieny pracy. Jeżeli w działaniach zespołu nie mogą uczestniczyć ani pracownik służby bezpieczeństwa i higieny pracy, ani społeczny inspektor pracy, w skład zespołu wchodzi dyrektor oraz pracownik szkoły przeszkolony w zakresie bhp. W działaniach zespołu może uczestniczyć przedstawiciel organu prowadzącego, kuratora oświaty lub rady rodziców. Przewodniczącym zespołu jest pracownik odpowiedzialny za bhp w szkole, a jeżeli nie ma go w składzie zespołu – społeczny inspektor pracy. Jeżeli w zespole nie ma ani pracownika służby bhp, ani społecznego inspektora pracy, przewodniczącego zespołu spośród pracowników szkoły wyznacza dyrektor.

Sposób postępowania	**4. Postępowanie powypadkowe** Zespół powypadkowy: • przeprowadza postępowanie powypadkowe i sporządza dokumentację powypadkową; • powiadamia rodziców/opiekunów prawnych o wypadku i wzywa ich do szkoły; • rozmawia z uczniem (w obecności rodzica/opiekuna prawnego lub wychowawcy/pedagoga/psychologa szkolnego) i sporządza protokół; • rozmawia ze świadkami wypadku i sporządza protokoły; jeżeli świadkami są uczniowie, rozmowa odbywa się w obecności wychowawcy lub pedagoga/psychologa szkolnego, a protokół odczytuje się w obecności ucznia – świadka – i jego rodziców/opiekunów prawnych; • sporządza szkic lub fotografię miejsca wypadku; • uzyskuje pisemne oświadczenie nauczyciela, pod opieką którego uczeń przebywał w czasie, gdy zdarzył się wypadek; • uzyskuje opinię lekarską z opisem doznanych obrażeń i określeniem rodzaju wypadku; • protokół powypadkowy sporządza się w terminie 21 dni od dnia zakończenia postępowania powypadkowego i niezwłocznie doręcza osobom uprawnionym do zaznajomienia się z materiałami tego postępowania. Przekroczenie 21-dniowego terminu może nastąpić w przypadku, gdy wystąpią uzasadnione przeszkody lub trudności uniemożliwiające sporządzenie protokołu w wyznaczonym terminie. W sprawach spornych rozstrzygające jest stanowisko przewodniczącego zespołu. Członek zespołu, który nie zgadza się ze stanowiskiem przewodniczącego, może zgłosić zdanie odrębne, które odnotowuje się w protokole powypadkowym. Jeżeli do treści protokołu powypadkowego nie zostały zgłoszone zastrzeżenia rodziców/opiekunów prawnych ucznia poszkodowanego, postępowanie powypadkowe uznaje się za zakończone. Protokół powypadkowy sporządza się w trzech egzemplarzach dla: poszkodowanego, szkoły, która przechowuje go w dokumentacji powypadkowej wypadku ucznia, oraz organu prowadzącego lub kuratora oświaty (na żądanie). Z treścią protokołu powypadkowego i innymi materiałami postępowania powypadkowego zaznajamia się poszkodowanego małoletniego i jego rodziców/opiekunów prawnych lub poszkodowanego pełnoletniego. Jeżeli poszkodowany pełnoletni zmarł lub nie pozwala mu na to stan zdrowia, z materiałami postępowania powypadkowego zaznajamia się jego rodziców/opiekunów prawnych. Protokół powypadkowy doręcza się osobom uprawnionym do zaznajomienia się z materiałami postępowania powypadkowego.

Sposób postępowania	**5. Składanie zastrzeżeń do protokołu powypadkowego** W ciągu 7 dni od dnia doręczenia protokołu powypadkowego osoby, którym go doręczono, mogą zgłosić zastrzeżenia do ustaleń protokołu (są o tym informowane podczas jego odbierania). Zastrzeżenia składa się przewodniczącemu zespołu ustnie lub na piśmie, a przewodniczący wpisuje je do protokołu. Zastrzeżenia mogą dotyczyć w szczególności: niewykorzystania wszystkich środków dowodowych niezbędnych dla ustalenia stanu faktycznego, sprzeczności istotnych ustaleń protokołu z zebranym materiałem dowodowym. Zastrzeżenia rozpatruje organ prowadzący szkołę. Po rozpatrzeniu zastrzeżeń organ prowadzący szkołę może: zlecić dotychczasowemu zespołowi powypadkowemu wyjaśnienie ustaleń protokołu lub przeprowadzenie określonych czynności dowodowych, powołać nowy zespół celem ponownego przeprowadzenia postępowania powypadkowego. **6. Dokumentacja** Dyrektor szkoły prowadzi rejestr wypadków. Dyrektor wskazuje prawidłowe zachowania i odstępstwa od niniejszej procedury, informuje o wnioskach i podjętych działaniach profilaktycznych zmierzających do zapobiegania analogicznym wypadkom.

2.9. Czyn karalny popełniony przez ucznia – procedury postępowania w przypadku popełnienia przez ucznia czynu karalnego oraz udzielania pomocy uczniowi będącemu sprawcą czynu karalnego

	Popełnienie przez ucznia czynu karalnego
Cel uruchomienia procedury	Zapewnienie bezpieczeństwa fizycznego w szkole w przypadku popełnienia przez ucznia czynu karalnego oraz udzielenie pomocy uczniowi – sprawcy czynu karalnego.
Osoby odpowiedzialne za zarządzanie	Dyrektor lub wicedyrektor szkoły, a w przypadku ich nieobecności – osoba upoważniona przez nich.
Podstawy uruchomienia działań	Przypadek może dotyczyć ucznia, który dopuścił się czynu po ukończeniu lat 13, ale nie ukończył lat 17, bądź ucznia, który nie ukończył 18. r.ż., wówczas zastosowanie mają przepisy zawarte w *Ustawie o postępowaniu w sprawach nieletnich z dnia 26 października 1982 r.*, Dz.U. 1982., Nr 35, poz. 228, z późn. zm. Przypadek może dotyczyć ucznia pełnoletniego (po 18. r.ż.), który popełnił czyn karalny, wówczas podlega on przepisom prawa ogólnie przyjętym wobec osób dorosłych.

Sposób postępowania	• osoba, która była świadkiem popełnienia czynu karalnego lub dostrzegła zagrożenie, zobowiązana jest do powiadomienia dyrektora szkoły; • dyrektor szkoły odpowiada za ustalenie okoliczności czynu i ewentualnych świadków zdarzenia; • w przypadku, gdy sprawcą jest małoletni/niepełnoletni uczeń danej szkoły przebywający na jej terenie, wyznaczone przez dyrektora osoby winny zatrzymać i przekazać go dyrektorowi szkoły lub pedagogowi/psychologowi szkolnemu pod opiekę; • dyrektor szkoły winien powiadomić rodziców/opiekunów prawnych ucznia o zaistniałej sytuacji; • dyrektor szkoły jest zobowiązany do niezwłocznego powiadomienia policji w przypadku, gdy sprawa jest poważna (np. rozbój, uszkodzenie ciała itp.) lub w przypadku, gdy sprawca jest pełnoletni bądź nie jest uczniem szkoły; do jego obowiązków należy także zabezpieczenie ewentualnych dowodów lub przedmiotów pochodzących z przestępstwa i przekazanie ich policji. • dyrektor szkoły nie ma prawa przeprowadzać czynności zarezerwowanych dla policji (np. przesłuchiwania, przeszukiwania).

2.10. Ofiara czynu karalnego – procedury postępowania w przypadku zidentyfikowania w szkole ucznia będącego ofiarą czynu karalnego oraz udzielania pomocy uczniowi będącemu ofiarą czynu karalnego

Zidentyfikowanie ucznia jako ofiary czynu karalnego	
Cel uruchomienia procedury	Zapewnienie bezpieczeństwa fizycznego w szkole w przypadku zidentyfikowania w szkole ucznia będącego ofiarą czynu karalnego oraz udzielenie pomocy uczniowi – ofierze czynu karalnego.
Osoby odpowiedzialne za zarządzanie	Dyrektor lub wicedyrektor szkoły; w przypadku ich nieobecności – osoba przez nich upoważniona.
Podstawy uruchomienia działań	Sytuacja, w której uczeń stał się ofiarą czynu karalnego zabronionego przez *Ustawę o postępowaniu w sprawach nieletnich*.
Sposób postępowania	• osoba, która była świadkiem popełnienia czynu karalnego lub dostrzegła zagrożenie, winna udzielić ofierze pierwszej pomocy (przedmedycznej) bądź zapewnić jej udzielenie poprzez wezwanie lekarza, w przypadku kiedy ofiara doznała obrażeń; • świadek powinien powiadomić o sytuacji dyrektora szkoły;

Sposób postępowania	• obowiązkiem dyrektora szkoły jest niezwłoczne powiadomienie rodziców/opiekunów prawnych ucznia – ofiary czynu karalnego; • dyrektor szkoły winien niezwłocznie wezwać policję, szczególnie w przypadku, kiedy istnieje konieczność profesjonalnego zabezpieczenia śladów przestępstwa, ustalenia okoliczności i ewentualnych świadków zdarzenia; • ofiara czynu karalnego powinna otrzymać pomoc, wsparcie psychologiczne.

Rozdział II
Bezpieczeństwo cyfrowe

1. Zagrożenia w świecie cyfrowym – procedury reagowania w przypadku wystąpienia zagrożenia cyfrowego

Większość polskiego społeczeństwa żyje w świecie cyfrowych treści i usług, przenikających codzienność jak żadna technologia w przeszłości. Polska **szkoła musi zatem w pełni, merytorycznie i bezpiecznie działać w środowisku cyfrowym,** wykorzystując edukacyjne zasoby dostępne online: multimedialne treści, aplikacje, platformy i skojarzone z nimi interaktywne metody nauczania. W pełni – to znaczy nie wybiórczo, lecz konsekwentnie w ramach wszystkich przedmiotów nauczania; merytorycznie – czyli ze zrozumieniem specyfiki zasobów i narzędzi cyfrowych online oraz ich zastosowań metodycznych, a także bezpiecznie – a zatem ze świadomością zagrożeń i wiedzą o tym, jak na nie reagować.

Badania wykazują, że zagrożeń, na które narażone są dzieci i młodzież w internecie, jest wiele, dotyczą różnych obszarów funkcjonowania człowieka w przestrzeni osobistej i społecznej. W literaturze przedmiotu można znaleźć wiele przykładów klasyfikacji zagrożeń związanych z korzystaniem z nowych technologii. Lista niebezpieczeństw, na które narażony jest młody internauta, jest stale aktualizowana ze względu na pojawiające się nowe rodzaje zagrożeń.

Niniejszy rozdział ma na celu przedstawienie pakietu **podstawowych działań na rzecz zapewnienia bezpieczeństwa uczniów w środowisku cyfrowym**, **jakie powinny zostać podjęte w każdej polskiej szkole.** Czytelnicy znajdą tu także zestaw **procedur poprawnego reagowania** w przypadku wystąpienia zagrożeń cyberbezpieczeństwa uczniów[10].

[10] Przez bezpieczeństwo cyfrowe (cyberbezpieczeństwo, bezpieczeństwo w środowisku cyfrowym) rozumie się zarówno zapewnienie bezpiecznej aktywności uczniów w środowisku cyfrowym, jak i przeciwdziałanie zagrożeniom odnoszącym się do bezpieczeństwa sieci, serwerów, danych na urządzeniach.

Proponowane działania profilaktyczne będą odpowiedzią na obowiązek: „upowszechniania wśród dzieci i młodzieży wiedzy o bezpieczeństwie oraz kształtowania właściwych postaw wobec zagrożeń, w tym związanych z korzystaniem z technologii informacyjno-komunikacyjnych", który nakłada na szkoły *Ustawa z 14 grudnia 2016 r. – Prawo oświatowe*.

Największe znaczenie dla zapewnienia podstaw bezpieczeństwa cyfrowego w szkole mają działania profilaktyczne (prewencyjne) prowadzone wobec i z udziałem wszystkich członków społeczności szkolnej: uczniów i ich rodziców, dyrektorów, nauczycieli i innych pracowników szkoły (np. psychologów, pedagogów, pracowników sekretariatu). Działania te powinny mieć charakter systemowy, ciągły, wieloletni i skoordynowany, a ich zakres należy wpisać w realizowany w szkole program wychowawczo-profilaktyczny.

1.1. Rekomendacje strategiczne i profilaktyczne

REKOMENDACJA STRATEGICZNA

Opracowanie, realizacja i aktualizacja szkolnych działań mających na celu zapewnienie bezpieczeństwa cyfrowego (np. plan, strategia)

Zainicjowanie pracy nad planem oraz opracowanie jego projektu to zadania **dyrektora szkoły**. Założenia planu winny powstać z jego inspiracji w ramach dyskusji z nauczycielami i przedstawicielami organu prowadzącego, samorządu szkolnego oraz rady rodziców lub rady szkoły. Finalna postać planu strategii powinna stanowić oficjalny dokument przyjęty do realizacji w szkole i zaakceptowany przez rodziców, nauczycieli i uczniów.

Na taki plan – obejmujący aktywności w okresie 3–4 lat, aktualizowany w trakcie realizacji – składać się będą wynikające z rekomendacji profilaktycznych niniejszego dokumentu działania o charakterze: kadrowym, edukacyjnym, wychowawczym i techniczno-inwestycyjnym. Ważną – wyróżnioną – część strategii stanowić musi tzw. **polityka bezpieczeństwa cyfrowego** w szkole (bezpiecznego korzystania z zasobów sieci oraz infrastruktury cyfrowej w szkole). Polityka bezpieczeństwa musi uwzględniać wprowadzenie standardów i procedur zgłaszania incydentów oraz podejmowania interwencji w sytuacji wystąpienia zagrożenia (określać, jak zgłaszać, do kogo, gdzie szukać pomocy itp.)[11]. Podczas jej opracowania warto skorzystać ze wsparcia eksperta. Rekomenduje się koordynację przygotowania polityk bezpieczeństwa cyfrowego w szkołach na poziomie organu prowadzącego. Punktem wyjścia do sformułowania planu jest zawsze **diagnoza sytuacji początkowej** – obejmująca ocenę potrzeb edukacyjnych uczniów i nauczycieli, analizę występujących i potencjalnych zagrożeń oraz ewaluację poziomu bezpieczeństwa infrastruktury cyfrowej.

[11] Politykę bezpieczeństwa cyfrowego w szkole należy rozumieć jako zbiór zasad obejmujący procedury działania i reagowania w sytuacjach zidentyfikowanych i sklasyfikowanych jako występujące w cyberprzestrzeni szkoły oraz pojawiające się w związku z użytkowaniem sieci przez nauczycieli, uczniów i osoby trzecie.

Internet – jego zasoby i możliwości komunikacyjne – to wielkie bogactwo, z którego korzysta na co dzień nowoczesna szkoła. Działania na rzecz zapewnienia cyberbezpieczeństwa w największym stopniu składać się muszą z aktywności, które zagwarantują wszystkim grupom budującym społeczność szkolną łatwy i bezpieczny dostęp do treści i platform edukacyjnych, a także sprzyjać będą budowaniu atmosfery zaufania między uczniami i nauczycielami oraz rodzicami poprzez wyjaśnianie i pozytywne rozwiązywanie pojawiających się problemów. Nie mogą być zatem wyłącznie zbiorem ograniczeń, zakazów i kar.

W przypadkach wystąpienia zagrożeń czy incydentów naruszenia bezpieczeństwa dzieci, w tym naruszenia prawa, działania szkoły cechować powinna otwartość postępowania oraz identyfikacja i zaproponowanie rozwiązania adekwatnego do poziomu zagrożenia. Warto przy tym podkreślić, iż nie istnieje „złota recepta", którą zastosować można we wszystkich przypadkach zagrożeń. Dyrektorzy i nauczyciele muszą uwzględniać kontekst indywidualnych przypadków, a także ich szkolne i środowiskowe tło, aby reagować adekwatnie do poziomu odpowiedzialności i winy ucznia.

REKOMENDACJA PROFILAKTYCZNA 1

Wdrożenie bezpieczeństwa na poziomie klas szkolnych

Zapewnienie uczniom bezpieczeństwa cyfrowego to zadanie dla niemal wszystkich pracowników szkoły oraz rodziców. Dzieci i młodzież korzystają bowiem z usług i treści sieci w szkole, a także – przede wszystkim – poza nią. Aby działać skutecznie, dyrektor powinien powołać spośród grona pedagogicznego **szkolnego lidera bezpieczeństwa** – osobę współodpowiedzialną wraz z nim za realizację strategii zapewnienia bezpieczeństwa cyfrowego: koordynatora i promotora działań na rzecz cyberbezpieczeństwa w szkole.

Osoby tej nie należy jednak mylić z osobą lub firmą odpowiedzialną za techniczne bezpieczeństwo sprzętu cyfrowego (komputerów stacjonarnych, laptopów, tablic multimedialnych, tabletów itp.) i sieci szkolnej. Spektrum jej zadań jest potencjalnie szersze i obejmuje: bieżącą diagnozę potrzeb szkoły w zakresie bezpieczeństwa cyfrowego, organizację procesu nabywania dziedzinowych kompetencji nauczycieli, zarządzanie szkolnymi zasobami narzędzi zapewniających cyberbezpieczeństwo, nadzorowanie pracy osób/firm odpowiedzialnych za techniczne bezpieczeństwo urządzeń cyfrowych i wewnętrznej sieci szkolnej oraz koordynację działań w przypadku wystąpienia zagrożenia. Jej zadaniem powinno być także prowadzenie działań służących rozwijaniu kompetencji medialnych i cyfrowych uczniów oraz działań adresowanych do rodziców.

Liderów należy rekrutować raczej spośród nauczycieli zaangażowanych w częste wykorzystanie technologii informacyjno-komunikacyjnych (TIK) w codziennej praktyce nauczania, pasjonatów tematyki cyfrowej, niż z grupy informatyków. Przewodzenie procesowi

cywilizacyjnej zmiany w szkole to wyzwanie niezwykle odpowiedzialne, a jednocześnie atrakcyjne i budujące pozycję nauczyciela w szkole. Bardzo ważne, żeby była to osoba, do której uczniowie mają zaufanie, aktywnie wspierająca ich w znajdowaniu rozwiązań sytuacji problemowych związanych z poruszaniem się w środowisku cyfrowym i nie tylko.

Lider bezpieczeństwa cyfrowego w szkole może być wynagradzany dodatkowo za swoją pracę niedydaktyczną, posiadać odpowiednie uprawnienia nadane mu przez dyrektora oraz narzędzia do wprowadzania niezbędnych zmian oraz koordynacji działań w przypadku wystąpienia zagrożenia. Wymagać to będzie odpowiednich decyzji organu prowadzącego szkołę, w formie uchwały o zapewnieniu środków finansowych na ten cel. Dlatego **duże znaczenie dla powodzenia działań zapewniających bezpieczeństwo cyfrowe w szkole ma przekonanie władz samorządowych o wadze i powszechności zagrożeń cyberbezpieczeństwa uczniów**. Można wyobrazić sobie, iż liderem działań na rzecz bezpieczeństwa cyfrowego w szkole jest jej wicedyrektor, którego obowiązki koncentrują się na wprowadzeniu szkoły w cyfrowy świat.

W większych szkołach opisane powyżej zadania może realizować szerszy zespół ds. bezpieczeństwa cyfrowego, powołany i koordynowany przez dyrektora szkoły. Warto rozważyć włączenie do takiego zespołu przedstawicieli uczniów i rodziców.

W polskich szkołach częstym przejawem prewencji zagrożeń cyberbezpieczeństwa lub przeciwdziałania korzystaniu przez uczniów podczas lekcji z własnych urządzeń cyfrowych (na ogół smartfonów) dla celów niezwiązanych z nauką jest **ograniczanie uczniom dostępu do internetu w przestrzeni szkolnej** (limitowany dostęp – w wybranych salach lekcyjnych) oraz wprowadzanie **zakazu korzystania z telefonów komórkowych w trakcie lekcji lub na terenie całej szkoły**[12].

Taki wzorzec (pozornego) zapewnienia bezpieczeństwa cyfrowego w środowisku szkolnym, bazujący na zakazach i ograniczeniach w korzystaniu z zasobów internetu kontrastuje z dominującym wśród uczniów modelem niemal nieograniczonej obecności w sieci oraz swobodą użytkowania jej zasobów i komunikowania się. Powoduje on, że uczniowie – „internetowi tubylcy" – traktują szkołę jako środowisko wykluczenia, restrykcji i archaiczności, przez co dystansują się wobec jej zachowawczości i technologicznego anachronizmu, co ujemnie odbija się na skuteczności ich nauki w szkole.

Dlatego realizację Szkolnego Planu Zapewnienia Bezpieczeństwa Cyfrowego należy potraktować jako inspirację do przeprowadzenia dyskusji i opracowania **szkolnego kontraktu cyfrowego** (w formie umowy), **uzgodnionego i zawartego między wszystkimi współtwórcami środowiska edukacji: uczniami i ich rodzicami oraz nauczycielami i innymi**

[12] Zakazy te wpisywane są często do statutu i/lub regulaminu szkoły lub zostają objęte specjalnymi zastrzeżeniami w ramach kontraktów zawieranych między kierownictwem szkoły, rodzicami a uczniami. Mogą być także ujęte w statucie szkoły/placówki.

pracownikami szkoły. Kontrakt taki – z dobrze zbalansowanym zestawem praw i obowiązków wszystkich sygnatariuszy – pobudza u uczniów poczucie współodpowiedzialności za sytuację w szkole i buduje w nich poczucie podmiotowości jako partnera dorosłych w życiu szkoły.

REKOMENDACJA PROFILAKTYCZNA 2

Przeprowadzenie dyskusji nad szkolnym kontraktem cyfrowym, określającym zakres i zasady korzystania z internetu w szkole. Formalne uzgodnienie kontraktu i jego okresowa aktualizacja

W powszechnej opinii ekspertów dominujące w polskich szkołach blokowanie dostępu do internetu – nie jest rozwiązaniem. Proponujemy, aby zapisy kontraktu – respektując uprawnienia szkoły do zapewnienia bezpieczeństwa cyfrowego i wykluczenia przypadków nielegalnego i wychowawczo niepożądanego korzystania z treści i usług internetu – koncentrowały się na **otwartym dostępie do infrastruktury internetowej**[13], **budowaniu atmosfery zaufania między nauczycielami a uczniami w świecie cyfrowym**, **edukacji cyfrowej i medialnej**, a także umożliwieniu – w pewnych sytuacjach – **korzystania z urządzeń cyfrowych w modelu BYOD**[14]. Celem kontraktu jest uzgodnienie i respektowanie zestawu praw i obowiązków wszystkich uczestników społeczności szkolnej, obowiązujących w relacjach ze światem cyfrowym.

W pracach nad umową ważną rolę odgrywają rodzice (poprzez udział rad rodziców lub rad szkół oraz osób zainteresowanych, w tym fachowców) i uczniowie (poprzez aktywność samorządu szkolnego i osób zainteresowanych).

W zakres tego dokumentu wchodzić powinny m.in. regulacje dotyczące: bezpiecznego dostępu uczniów do internetu w szkole, wykorzystywania TIK w trakcie zajęć, zasad korzystania z pracowni informatycznej, szkolnych zasady netykiety i tworzenia szkolnej strony internetowej.

Strategiczny cel – zapewnienie bezpieczeństwa cyfrowego dzieci i młodzieży, a także przestrzeni szkolnej – można osiągnąć głównie poprzez wychowanie i edukację, prowadzone w sposób zintegrowany tak w szkole, jak i w rodzinie. Wyjątkową rolą szkoły jest zainicjowanie takiego procesu, który połączy starania nauczycieli i rodziców w celu: (1) zapewnienia dzieciom aktualnej wiedzy na temat korzystania z zasobów internetu, (2) kształtowania postaw odpowiedzialnej aktywności w środowisku cyfrowym oraz (3)

[13] Przy założeniu zapewnienia przez infrastrukturę sieciową szkoły identyfikacji każdej osoby, każdy uczeń i inny użytkownik sieci w szkole powinien mieć indywidualny login i hasło: do sieci i do WiFi.
[14] (ang.) *Bring Your Own Device* – przynieś swoje własne urządzenie.

zapewnienia spójności prawidłowych zachowań w szkole, w przestrzeni publicznej i w domu rodzinnym.

Współczesną polską szkołę cechuje **deficyt kompetencji uczniów w zakresie bezpieczeństwa cyfrowego**. Do każdej z grup wiekowych dzieci warto w szkole adresować działania uświadamiające, motywujące i edukacyjne o odpowiedniej skali i zakresie tematycznym. Najlepsze efekty w dziedzinie bezpieczeństwa cyfrowego szkoła osiągnie wówczas, gdy głównymi uczestnikami wszystkich działań będą właśnie uczniowie, którzy świetnie potrafią zidentyfikować wszystkie przejawy niewłaściwych zachowań. To właśnie oni mogą stworzyć, np. katalog zagrożeń – udostępniony online dla wszystkich i poparty „żywymi" przykładami ku przestrodze innych – lub listę zasad bezpiecznego i efektywnego, przynoszącego uczniom korzyści edukacyjne, korzystania z internetu.

REKOMENDACJA PROFILAKTYCZNA 3

Działania profilaktyczne i edukacyjne adresowane do uczniów

Wyniki badań z ostatnich lat wskazują, że niemal wszyscy nastolatkowie (96%) korzystają z sieci każdego dnia. Respondenci najczęściej korzystają z internetu w domu (95,4% wskazań). Aż 60% używa sieci podczas podróży, komunikacji i transportu (np. w drodze do szkoły). Niespełna połowa respondentów (41,2%) zadeklarowała, że korzysta z internetu w szkole[15]. Z uwagi na to warto, aby nauczyciele pokazali uczniom, w jaki sposób bezpiecznie poruszać się w sieci. Nauczyciele i pedagodzy szkolni mają zatem do odegrania wielką rolę przewodników w eksploracji internetu i w kształtowaniu właściwych zachowań w sieci. Aby było to możliwe, niezbędne jest ich doskonalenie w tym obszarze.

Prowadzone w sposób zrozumiały, akcentujące przewagę pozytywnych cech internetu, odnoszące się do systemu wartości akceptowanego przez uczniów działania wychowawcze i edukacyjne adresowane do uczniów są fundamentalnym sposobem zapewnienia bezpieczeństwa cyfrowego dzieci.

Proponujemy, aby w każdej ze szkół zajęcia z cyberbezpieczeństwa miały charakter zaplanowany, systematyczny w działaniach i kompleksowy w zakresie tematyki.

Na coroczny minimalny zakres zajęć profilaktycznych uświadamiających problem składać się mogą:

1. Poświęcenie tematyce jednego z aspektów bezpieczeństwa cyfrowego „**apelu szkolnego**" – spotkania całej szkolnej społeczności, przygotowanego przez uczniów (2–3 spotkania rocznie).

[15] NASK, *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów*, Warszawa: NASK, 2019.

2. Organizacja **spotkań społeczności szkolnej z ekspertem** w zakresie tematyki korzystania z internetu przez dzieci – edukatorem, nauczycielem, informatykiem, policjantem itp. (2 razy w roku).
3. Przeprowadzenie co najmniej **jednej lekcji wychowawczej kwartalnie (w zależności od zdiagnozowanych potrzeb częściej)** na temat wybranego aspektu cyberbezpieczeństwa, adekwatnego do potrzeb, wyzwań klasy i wieku uczniów. Sposób prowadzenia lekcji i ich tematyka muszą uwzględniać poziom rozwoju i doświadczenia dzieci (4–6 lekcji rocznie).
4. Organizacja **dnia bezpieczeństwa cyfrowego w szkole**, np. w ramach Dnia Bezpiecznego Internetu – wydarzenia dla całej społeczności szkolnej, otwartego na współudział rodziców/opiekunów prawnych uczniów, a także przedstawicieli lokalnego środowiska – władz oświatowych, organizacji pozarządowych czy instytucji kultury. Do współorganizacji takiego dnia dyrekcja szkoły oraz lider bezpieczeństwa cyfrowego w szkole zaprosić powinni samorząd uczniowski, przewodniczących klas, a także radę rodziców (szkoły). Bezpośrednim organizatorem może być np. samorząd uczniowski, którego działania adresowane do społeczności szkolnej byłyby lepiej ukierunkowane i skuteczniejsze. Na wydarzenie składać się mogą prelekcje i zajęcia praktyczne (warsztaty) w szkole, a także spotkania uświadamiające, dyskusje, happeningi, pikniki i inne formy popularyzacji tematyki cyberbezpieczeństwa[16] (raz w roku).
5. Zorganizowanie przez samorząd uczniowski **konkursu** – opartego na rywalizacji między klasami – na temat bezpieczeństwa cyfrowego (np. pozytywnego wykorzystania zasobów internetu, sposobów radzenia sobie w sytuacjach zagrożenia), z nagrodami ufundowanymi przez radę rodziców i sponsorów (raz w roku).
6. Organizowanie dla uczniów **zajęć pozalekcyjnych** o tematyce informatycznej (np. programowanie, robotyka, projektowanie graficzne, szkolne radio lub telewizja) z obligatoryjnym uwzględnieniem komponentu edukacji w zakresie bezpieczeństwa cyfrowego, a także kształtujących miękkie kompetencje medialne i cyfrowe (np. tworzenie własnego wizerunku cyfrowego, współpraca grupowa poprzez sieć, skuteczne szukanie informacji, odróżnianie fałszu od prawdy w sieci, prawo autorskie, bezpieczeństwo w sieci itd.). Warto zauważyć, że tematyka ta obecna jest w nowej podstawie programowej, w szczególności w ramach zajęć edukacji informatycznej oraz informatyki.
7. Realizacja **projektów edukacyjnych** uwzględniających nowe technologie informacyjno-komunikacyjne oraz tematykę bezpieczeństwa cyfrowego, finansowanych ze środków unijnych, kuratoriów i fundacji prywatnych.
8. Zaplanowanie i realizacja wybranego **programu profilaktycznego** dostosowanego do możliwości organizacyjnych i kadrowych szkoły.

[16] Organizowanie dni bezpieczeństwa cyfrowego w szkole umożliwia realizację różnorodnych aktywności, dostosowanych do potrzeb lokalnej społeczności. Bardzo wiele inspirujących przykładów takich działań w ostatnich latach zostało opisanych na portalu projektu „Cyfrowobezpieczni.pl": https://www.cyfrowobezpieczni.pl/szkoly/szkoly-cyfrowobezpieczne [dostęp: 29.08.2020 r.]. Organizację dni bezpieczeństwa cyfrowego powiązać można z uczestnictwem w europejskiej akcji Dzień Bezpiecznego Internetu (*Safer Internet Day*), realizowanej co roku w lutym – zob. https://www.saferinternet.pl/dbi/o-dbi.html [dostęp: 29.08.2020 r.].

W codziennej pracy dydaktycznej należy dążyć do włączania tematyki bezpieczeństwa cyfrowego w nauczanie przedmiotów nieinformatycznych, a także wzmacniać zainteresowanie uczniów tematyką bezpieczeństwa cyfrowego poprzez przygotowywanie ich do udziału w konkursach[17].

Spotkania społeczności szkolnych mogą też mieć służącą aktywności formę gier terenowych/miejskich, festiwali, spektakli szkolnych o tematyce bezpieczeństwa w sieci itp. Współpraca nauczycieli z uczniami w dziedzinie bezpieczeństwa cyfrowego może zostać znacznie zintensyfikowana, jeśli z ramienia samorządu uczniowskiego, w ramach realizacji planu powołana zostanie grupa „uczniowskich liderów cyberbezpieczeństwa", ściśle współpracujących z liderem bezpieczeństwa cyfrowego w szkole i czuwających nad bezpieczeństwem cyfrowym szkoły ze strony uczniów. Zdaniem praktyków w takim modelu współpracy planowane działania przyniosą lepszy skutek i zapewnią wyższy poziom bezpieczeństwa cyfrowego w szkole.

Tematyka bezpieczeństwa cyfrowego szkoły powinna się pojawić **w serwisie internetowym szkoły oraz na profilach szkoły w portalach społecznościowych jako oddzielne zagadnienie**. Szczególne znaczenie ma publikowanie w nich numerów telefonów, pod którymi można zgłosić przypadki naruszenia bezpieczeństwa cyfrowego w sposób anonimowy lub jako spersonalizowane zgłoszenie. Uczniowie w szkole powinni ponadto wiedzieć, kto pełni rolę szkolnego lidera bezpieczeństwa cyfrowego – do kogo należy zgłaszać indywidualne przypadki niedozwolonych zachowań lub działań. Proponujemy, aby uzupełnieniem informacji na ten temat w internecie była aktualizowana tablica informacyjna na korytarzu szkolnym, informująca o aktualnościach i o różnych zagadnieniach bezpieczeństwa cyfrowego czy odsyłająca do materiałów informacyjnych i edukacyjnych w sieci.

REKOMENDACJA PROFILAKTYCZNA 4

Przygotowanie grona pedagogicznego do prowadzenia zajęć w zakresie bezpieczeństwa cyfrowego

Badania wskazują na relatywnie **niski poziom wiedzy nauczycieli wszystkich typów szkół na temat różnorodnych aspektów bezpieczeństwa cyfrowego.** Wykazano w nich także, iż tylko część nauczycieli aktualizuje swoje kompetencje cyfrowe, a w szkołach osoby o średnich i wysokich umiejętnościach z zakresu wykorzystania TIK w nauczaniu stanowią zdecydowaną mniejszość.

Duże znaczenie ma realizacja postulatu objęcia szkoleniami nauczycieli wszystkich przedmiotów oraz **pedagogów** i **psychologów.** Proponujemy, aby tematyce bez-

[17] Takich jak np. Olimpiada Cyfrowa https://olimpiadacyfrowa.pl [dostęp: 29.08.2020 r.], Olimpiada Wiedzy o Mediach http://owm.edu.pl/ [dostęp: 29.08.2020 r.] i Olimpiada Informatyczna http://www.oi.edu.pl/ [dostęp: 29.08.2020 r.].

pieczeństwa cyfrowego uczniów w szkole poświęcone było co najmniej jedno posiedzenie rady pedagogicznej w roku szkolnym, zaś tematyka ta była obowiązkowo każdorazowo włączana do programu najbliższego posiedzenia rady w przypadku naruszenia cyberbezpieczeństwa w środowisku szkolnym.

Szkolenia dotyczące wybranych zagadnień bezpieczeństwa cyfrowego należy organizować obligatoryjnie, wykorzystując środki będące w dyspozycji dyrekcji szkoły na podniesienie kwalifikacji nauczycieli lub środki projektów zewnętrznych (np. unijnych, kuratoryjnych, MEN) – **w związku z zakupem nowych urządzeń cyfrowych lub instalacją/zmianami w szkolnej sieci komputerowej/internetowej**.

Nauczyciele i dyrektorzy szkół mogą także poszerzać swoją wiedzę, zapoznając się z bezpłatnymi publikacjami na temat cyberbezpieczeństwa, zamieszczonymi na stronie Naukowej i Akademickiej Sieci Komputerowej, będącej operatorem projektu Ogólnopolskiej Sieci Edukacyjnej[18]. Publikacje te obejmują zarówno raporty przedstawiające stan bezpieczeństwa polskiej części internetu, raporty z działalności zespołu Dyżurnet.pl, jak i poradniki dobrych praktyk.

REKOMENDACJA PROFILAKTYCZNA 5

Uświadamianie rodzicom i opiekunom prawnym uczniów znaczenia działań wychowawczych z zakresu bezpieczeństwa cyfrowego

Szkoła może być miejscem edukacji uczniów w zakresie cyberbezpieczeństwa, nie zastąpi jednak rodziców w ich funkcjach wychowawczych. Ponieważ w domu rodzinnym uczniowie niemal przez cały czas pozostają online, szczególne znaczenie mają świadome działania kontrolne, wychowawcze i edukacyjne prowadzone przez rodziców w omawianym zakresie. Szkoła pozostawiona z tym zadaniem sama może tylko częściowo zaspokoić potrzeby wychowawcze i edukacyjne uczniów na tym polu.

Jak pokazują badania, **na przeszkodzie w realizacji tego ważnego zadania stoi w Polsce duży deficyt kompetencji rodziców i opiekunów w zakresie bezpieczeństwa cyfrowego** oraz – zapewne z nim skojarzony – dominujący wśród nich **brak zainteresowania celami i sposobami korzystania przez dzieci z usług i treści internetu**.

Współpraca szkoły z rodzicami powinna zatem w pierwszej kolejności polegać **na uświadomieniu im znaczenia ich roli** w zakresie przygotowania dzieci do bezpiecznego korzystania z internetu. Takim działaniom towarzyszyć może wsparcie edukacyjne, np. w formie wskazywania źródeł wiedzy, popularnych multimediów edukacyjnych itp. Wartościowymi działaniami realizowanymi przez NASK i skierowanymi do ogółu społeczeństwa są: projekt OSE,

[18] https://ose.gov.pl/materialy-do-pobrania [dostęp: 29.08.2020 r.].

program Komisji Europejskiej „Safer Internet" oraz kampania Ministerstwa Cyfryzacji i NASK „Nie zagub dziecka w sieci", mające na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni. Na stronie internetowej znajduje się gotowa baza dobrych praktyk, z których mogą skorzystać zarówno rodzice, jak i uczniowie[19].

Współpracę ze środowiskiem rodziców prowadzić należy zarówno poprzez inicjatywy dyrekcji szkoły i szkolnego lidera bezpieczeństwa cyfrowego podejmowane wspólnie z radami rodziców lub radami szkoły, jak i w ramach dostępnych kanałów komunikacji z rodzicami („wywiadówki", dzienniki elektroniczne itp.).

We wszystkich tych działaniach na pierwszym miejscu stawiać należy uświadamianie rodzicom znaczenia cyfrowego świata w życiu dzieci i młodzieży, w tym skali i dotkliwości zagrożeń cyberbezpieczeństwa, przed jakimi stają ich dzieci oraz najważniejszej roli, jaką rodzice muszą odegrać w procesie kształtowania odpowiedzialnych postaw dzieci wobec świata cyfrowego.

Przykłady prowadzonych w szkole działań uświadamiających i edukacyjnych adresowanych do rodziców:

1. Organizowanie **szkolnego dnia bezpieczeństwa cyfrowego**, a w jego ramach m.in. krótkiego szkolenia dla rodziców z wykorzystaniem materiałów multimedialnych i przygotowanej w tym celu ulotki informacyjnej (w tradycyjnej lub elektronicznej formie) z podaniem źródeł przystępnie udostępnionej wiedzy (raz w roku)[20].
2. **Włączenie w tematykę spotkań z rodzicami każdej z klas w szkole tematyki bezpieczeństwa cyfrowego** – na co najmniej jednej „wywiadówce" w roku. W przypadku wystąpienia zagrożenia cyberbezpieczeństwa w klasie należy o tym powiadomić rodziców bezzwłocznie i zorganizować spotkanie specjalnie poświęcone temu incydentowi.
3. W szkołach posiadających system dziennika elektronicznego **rozesłanie za pomocą tej platformy informacji na temat potencjalnych zagrożeń wraz z linkami do materiałów edukacyjnych i multimediów oraz apelem do rodziców** o zapoznanie się z daną tematyką i rozmowę z dziećmi – możliwe rozesłanie informacji przez inne, elektroniczne kanały kontaktu (2 razy w roku).
4. Przedstawienie w trakcie uroczystości zakończenia roku szkolnego **prezentacji dotyczącej zagrożeń bezpieczeństwa cyfrowego dzieci i młodzieży**, jakie dzieci mogą napotkać w czasie wakacji, ze zwróceniem uwagi obecnych dzieci i rodziców na konieczność rozmowy na ten temat w czasie wakacji.

[19] https://.saferinternet.pl; https://akademia.nask.pl/baza-wiedzy.html; https://ose.gov.pl/materialy-do-pobrania; https://www.gov.pl/web/niezagubdzieckawsieci [dostęp: 29.08.2020 r.].

[20] Organizując takie wydarzenie w szkole, można skorzystać z materiałów informacyjnych m.in.: projektu „Cyfrowobezpieczni.pl – Bezpieczna Szkoła Cyfrowa" – www.cyfrowobezpieczni.pl [dostęp: 29.08.2020 r.], programu „Safer Internet": https://www.saferinternet.pl/menu/materialy-edukacyjne/poradniki-i-broszury.html oraz materiałów przygotowanych przez Fundację Orange: http://fundacja.orange.pl/strefa-wiedzy/materialy-edukacyjne-dla-rodzicow/, a także NASK http://akademia.nask.pl/baza-wiedzy.html [dostęp: 29.08.2020 r.].

REKOMENDACJA PROFILAKTYCZNA 6

Opracowanie i wdrożenie w praktyce szkolnej tzw. polityki bezpieczeństwa cyfrowego, ukierunkowanej na eliminację zagrożeń sieci komputerowych, systemów operacyjnych i innego oprogramowania wykorzystywanego w szkole

Zarówno sprzęt cyfrowy (komputery stacjonarne, laptopy, tablety, tablice multimedialne i inne urządzenia), jak i szkolną sieć komputerową (okablowanie, urządzenia sieciowe, zainstalowane systemy informacyjne oraz inne oprogramowanie) **należy chronić zgodnie z wytycznymi zawartymi w III rozdziale dokumentu *Bezpieczna szkoła cyfrowa. Zalecenia i rekomendacje dla samorządów – realizatorów projektów w ramach unijnej perspektywy budżetowej 2014–2020*[21].**

Inwestując w infrastrukturę cyfrową szkoły, należy dążyć do **zakupu urządzeń dostosowanych do potrzeb i specyfiki ich wykorzystywania przez uczniów** (trwałość, odporność na mobilne korzystanie) **oraz profesjonalnej rozbudowy systemu sieci internetowej w szkole** (router, firewall). Bezpieczeństwo cyfrowe jest silnie skorelowane z jakością infrastruktury. Sprzyja mu także korzystanie z zewnętrznych **platform edukacyjnych**[22] oraz rozwiązań **chmury edukacyjnej.**

Oprócz zwalczania zagrożeń związanych ze złośliwym oprogramowaniem (m.in. wirusy, robaki, oprogramowanie szpiegujące, „konie trojańskie") na poziomie technicznym należy instalować aktualizowane **systemy blokowania ruchu pod kątem filtrowania treści nieodpowiednich dla dzieci i młodzieży, niepożądanych i nielegalnych**. Należy zwrócić uwagę, że zapewnienie bezpieczeństwa sieci oraz filtrowania treści należy do obowiązków szkoły zgodnie z art. 4a *Ustawy o systemie oświaty* oraz art. 27 *Ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe*.

Zawsze należy pamiętać, iż celem cyfryzacji szkoły jest zapewnienie uczniom otwartego, ograniczonego tylko względami bezpieczeństwa dostępu do internetu, który w perspektywie najbliższych lat umożliwi korzystanie na co dzień w trakcie uczenia (się) z modelu BYOD. Wymagać to będzie jednak zabezpieczeń na wyższym niż podstawowy poziomie.

Za techniczne cyberbezpieczeństwo szkoły muszą odpowiadać specjaliści. W przypadku dużych szkół niezbędne jest zatrudnienie osoby profesjonalnie odpowiedzialnej za szkolną infrastrukturę, przy czym nie powinna ona łączyć swoich zadań z rolą nauczyciela informatyki. Jej obowiązki obejmować muszą głównie zapewnienie niezawodności i bezpieczeństwa sprzętu oraz sieci, tak aby nauczyciele i uczniowie mogli korzystać z nich, nie

[21] https://www.cyfrowobezpieczni.pl/aktualnosci/73-bezpieczna-szkola-cyfrowa-rekomendacje-dla-samorzadow [dostęp 29.08.2020 r.].
[22] Np. Zintegrowana Platforma Edukacyjna epodreczniki.pl [dostęp 29.08.2020 r.].

tracąc czasu na korekty, naprawy i instalacje. Środki na wynagrodzenie takiego specjalisty powinny zostać zapewnione przez organ prowadzący. W przypadku mniejszych szkół organ prowadzący powinien zapewnić opisane wsparcie na poziomie wszystkich szkół w gminie.

2. Podstawowe działania na rzecz bezpieczeństwa cyfrowego w szkole

Systematycznie prowadzone w szkole działania profilaktyczne w znacznej mierze ograniczają zakres zagrożeń występujących w cyberprzestrzeni, nie są jednak w stanie ich całkowicie wyeliminować. **W przypadku wystąpienia incydentu zagrożenia bezpieczeństwa, zwłaszcza wobec naruszenia prawa, działania szkoły cechować powinny: otwartość, szybka identyfikacja problemu – określenie szkodliwych lub niezgodnych z prawem zachowań – i jego rozwiązanie adekwatne do poziomu zagrożenia, jaki spowodował on w szkole.** Podobnie – bez zbędnej zwłoki, merytorycznie – z wykorzystaniem wiedzy ekspertów i dobrych praktyk z innych placówek szkoła powinna zareagować w przypadku wystąpienia problemów wynikających z deficytu wiedzy ucznia, np. na temat prawa autorskiego.

Zagrożenia bezpieczeństwa cyfrowego w szkole oraz problemy ucznia w świecie cyfrowym mogą mieć różnorodny charakter. W niniejszym opracowaniu nie podejmowano próby ich systematycznego opisu, natomiast dokonano analizy służącej określeniu procedur reagowania na występujące zagrożenia lub deficyty kompetencji, eksperci korzystali przede wszystkim z wartościowej publikacji *Standard bezpieczeństwa online placówek oświatowych*[23].

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

2.1. Obligatoryjne działania interwencyjne

Są następstwem wystąpienia zagrożenia. Podzielić je można na 3 grupy:

1. **Działania wobec aktu/zdarzenia** – opis przypadku, ustalenie okoliczności zdarzenia, zabezpieczenie dowodów oraz monitoring sytuacji szkolnej;
2. **Działania wobec uczestników zdarzenia** (ofiara – sprawca – świadek, rodzice/opiekunowie prawni);

[23] Publikacja *Standard bezpieczeństwa online placówek oświatowych* opracowana została przez zespół ekspertów Naukowej i Akademickiej Sieci Komputerowej (NASK) oraz Wyższej Szkoły Pedagogicznej im. Janusza Korczaka w Warszawie, w ramach projektu „Działania na rzecz bezpiecznego korzystania z Internetu", https://ose.gov.pl/materialy-do-pobrania/standardy-bezpieczenstwa-rekomendacje: https://akademia.nask.pl/publikacje/ost_Standard_bezpieczenstwa_online_placowek_oswiatowych.pdf oraz *Szkolne standardy bezpieczeństwa cyfrowego dzieci i młodzieży*, wydanej przez Fundację Dajemy Dzieciom Siłę w roku 2014: http://dzieckowsieci.fdn.pl/sites/default/files/file/dziecko-w-sieci/szkolne-standardy-bezpieczenstwa-online.pdf [dostęp: 28.08.2020 r.].

3. **Działania wobec instytucji/organizacji/służb pomocowych i współpracujących** – policji, wymiaru sprawiedliwości, służb społecznych.

W każdej procedurze związanej z wystąpieniem danego typu zagrożenia cyberbezpieczeństwa w szkole muszą zostać uwzględnione działania tego typu – podjęte przez dyrekcję szkoły oraz nauczycieli, pedagogów/psychologów szkolnych. Ich szczegółowy opis znajduje się w opracowaniu: *Standard bezpieczeństwa online placówek oświatowych* opracowanym przez zespół ekspertów Naukowej i Akademickiej Sieci Komputerowej (NASK) oraz Wyższej Szkoły Pedagogicznej im. Janusza Korczaka w Warszawie. Publikacja opracowana została w ramach realizowanego przez Fundację Odkrywców Innowacji[24] projektu „Działania na rzecz bezpiecznego korzystania z Internetu", zaktualizowana i uzupełniona w 2018 roku.

Działania wobec zdarzenia polegają przede wszystkim na **zachowaniu** (nieusuwaniu) **dokumentacji cyfrowej**: wiadomości sms, e-maili, nagrań z poczty głosowej telefonu, komentarzy w serwisie społecznościowym, zapisów na blogu czy plików filmów wideo. O ile to możliwe, należy także zarchiwizować treść rozmów w komunikatorach oraz linki (konkretne adresy URL), a także dane o potencjalnym sprawcy. Każde zdarzenie wymaga udokumentowania w stosownym protokole.

Działania na rzecz uczestników zdarzenia oznaczają te aktywności, które podejmowane są **wobec ofiar** (osób poszkodowanych), **sprawców** i **świadków** zdarzenia. W szkole osobami poszkodowanymi w przeważającej liczbie przypadków są dzieci (osoby nieletnie). Dlatego jako kolejną grupę pośrednich uczestników zdarzenia wyróżniamy ich rodziców/prawnych opiekunów.

Standardową procedurę reakcji w przypadku wystąpienia zagrożenia bezpieczeństwa cyfrowego prezentuje poniższy rysunek.

Rys 1. Standard procedury reakcji na zagrożenie bezpieczeństwa cyfrowego

Źródło: Wrońska A., Polak Z., (2018), *Standard bezpieczeństwa online placówek oświatowych*, Warszawa: NASK, s. 27.

[24] http://www.odkrywcyinnowacji.pl/

2.2. Działania szkoły adresowane do instytucji i organizacji zewnętrznych

Współpraca z zewnętrznymi instytucjami jest niezbędna w przypadku naruszenia przepisów prawa przez uczniów lub osoby spoza szkoły[25]. Należy pośród nich wyróżnić szczególnie współpracę z: (1) policją i sądami rodzinnymi, (2) służbami społecznymi i placówkami specjalistycznymi oraz (3) dostawcami usług internetowych oraz operatorami telekomunikacyjnymi[26].

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

1. Sprawca musi otrzymać od przedstawicieli szkoły komunikat o braku akceptacji dla działań, jakich dokonał. W trakcie rozmowy uczeń powinien poznać możliwe skutki swojego postępowania, a także konsekwencje, jakie mogą zostać wobec niego wyciągnięte (np. wynikające ze statutu i/lub regulaminu szkoły lub wprowadzonego kontraktu – umowy). Sprawca powinien zostać wezwany do zaprzestania podejmowania podobnych działań w przyszłości oraz usunięcia skutków swoich dotychczasowych działań (np. publikacji na portalu społecznościowym). Sprawca powinien również zostać objęty odpowiednią pomocą psychologiczno-pedagogiczną w celu zrozumienia konsekwencji swego zachowania oraz zmiany postawy i dalszego postępowania. Jeśli sprawców jest więcej, to z każdym z nich należy rozmawiać osobno.
2. Należy zadbać o to, żeby osoba reprezentująca szkołę (psycholog, pedagog, wychowawca) ograniczała się do podjęcia interwencji, a nie wymierzała karę. Decyzję o tym, jaką karę wymierzyć sprawcy, powinna podejmować rada pedagogiczna (po poznaniu wszystkich okoliczności zdarzenia), a przekazywać – dyrektor szkoły. Ważne jest zatem oddzielenie osoby pedagoga, nawiązującego relację z uczniem, od organu wymierzającego karę.

Celem sankcji wobec sprawcy jest przede wszystkim: zatrzymanie jego działań i zapewnienie poczucia bezpieczeństwa ofierze oraz zmiana postawy sprawcy. Sankcje mają na celu także pokazanie społeczności szkolnej, że działania sprawcy nie będą tolerowane i że szkoła jest w stanie skutecznie zareagować w tego rodzaju sytuacji. Podejmując decyzję o zastosowaniu sankcji, należy wziąć pod uwagę:

- **rozmiar i rangę szkody** – np. czy w przypadku cyberprzemocy materiał został upubliczniony w sposób pozwalający na dotarcie do niego wielu osobom (określa to rozmiar upokorzenia, jakiego doznaje ofiara), czy trudno jest wycofać materiał z sieci itp.;
- **czas trwania prześladowania** – czy było to długotrwałe działanie, czy pojedynczy incydent;

[25] Szczegółowy wykaz aktów prawnych związanych z bezpieczeństwem cyfrowym szkoły, działaniami podejmowanymi w szkole oraz wobec osób nieletnich znajduje się w II wydaniu publikacji *Standard bezpieczeństwa online placówek oświatowych z 2018 r.*, na stronach 111–117.

[26] Szczegółowy opis działań wobec tych podmiotów został opisany na stronach 32–36 w II wydaniu publikacji *Standard bezpieczeństwa online placówek oświatowych z 2018 r.*

- **świadomość popełnianego czynu** – czy działanie było zaplanowane, a sprawca był świadomy, że postąpił nagannie, np. czy wie, że wyrządza krzywdę koledze, jak wiele wysiłku włożył w ukrycie swojej tożsamości itp.;
- **motywacje sprawcy** – należy sprawdzić, czy działanie sprawcy nie jest działaniem odwetowym w odpowiedzi na uprzednie doświadczenia sprawcy.

Aktywność wobec sprawcy powinna także obejmować rozmowę z jego rodzicami lub opiekunami prawnymi – muszą oni zostać poinformowani o zdarzeniu, zapoznani z materiałami oraz decyzją co do dalszego postępowania ze sprawcą (np. z zastosowanymi sankcjami). Warto, aby rodzice współpracowali ze szkołą w zakresie rozwiązywania sytuacji kryzysowej, aby stali się jej sojusznikami, a nie przeciwnikami. Rodzice/opiekunowie prawni sprawcy powinni również zostać poinformowani, że rodzice ofiary mają prawo zgłosić sprawę policji.

Jeśli sprawcą jest osoba spoza szkoły, należy zapewnić bezpieczeństwo ofierze i poinformować ją (jej rodziców/opiekunów prawnych) o przysługujących jej prawach (np. zgłoszenie popełnienie przestępstwa policji). Jeśli sprawcą jest uczeń z innej szkoły, należy rozważyć nawiązanie współpracy między placówkami i wspólne rozwiązanie kryzysowej sytuacji.

2.3. Dostęp do treści szkodliwych, niepożądanych, nielegalnych – procedura reagowania

Dostęp do treści szkodliwych, niepożądanych i nielegalnych	
Podstawy prawne uruchomienia procedury	*Kodeks karny*, art. 200 § 1–5 kk, art. 200a kk, art. 200b kk, art. 202 § 1-4b, art. 256 kk, art. 257. Statut szkoły, regulamin szkoły.
Rodzaj zagrożenia objętego procedurą	Zagrożenie łatwym dostępem do treści szkodliwych, niedozwolonych, nielegalnych i niebezpiecznych dla zdrowia (pornografia, treści obrazujące przemoc, promujące działania szkodliwe dla zdrowia i życia dzieci, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawołujące do samookaleczeń i samobójstw, korzystania z narkotyków; niebezpieczeństwo werbunku dzieci i młodzieży do organizacji nielegalnych i terrorystycznych).
Telefony/kontakty alarmowe krajowe	Zgłaszanie nielegalnych treści: www.dyzurnet.pl, numer alarmowy 112 , policja 997
Sposób postępowania w przypadku wystąpienia zagrożenia	
Opis okoliczności, analiza, zabezpieczenie dowodów	Reakcja szkoły w przypadku pozyskania wiedzy o wystąpieniu zagrożenia będzie zależna od tego, czy: (1) treści te można bezpośrednio powiązać z uczniami danej szkoły, czy też (2) treści nielegalne lub szkodliwe nie mają związku z uczniami danej szkoły, lecz wymagają kontaktu szkoły z odpowiednimi służbami.

Opis okoliczności, analiza, zabezpieczenie dowodów	W pierwszej kolejności należy zabezpieczyć dowody w formie elektronicznej (pliki z treściami niedozwolonymi, zapisy rozmów w komunikatorach, e-maile, zrzuty ekranu), znalezione w internecie lub w komputerze dziecka. Zabezpieczenie dowodów jest zadaniem rodziców lub opiekunów prawnych dziecka, w czynnościach tych może wspomagać ich przedstawiciel szkoły posiadający odpowiednie kompetencje techniczne. W pierwszym przypadku (1) rozwiązanie leży po stronie szkoły, zaś w drugim należy rozważyć zgłoszenie incydentu policji oraz poinformować o nim serwis Dyżurnet (dyzurnet.pl).
Identyfikacja sprawcy(-ów)	W identyfikacji sprawców kluczową rolę odgrywają zgromadzone dowody. W procesie udostępniania nielegalnych i szkodliwych treści małoletnim biorą udział na ogół: twórca treści – np. pornograficznych – oraz osoby, które udostępniły je dziecku. Często są nimi rówieśnicy – uczniowie tej samej szkoły czy klasy, dzieci sąsiadów. Konieczne jest poinformowanie wszystkich rodziców/prawnych opiekunów dzieci uczestniczących w zdarzeniu o sytuacji i roli ich dzieci.
Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły	W przypadku udostępniania przez ucznia treści opisanych wcześniej jako szkodliwe nielegalne i niebezpieczne dla zdrowia należy przeprowadzić z nim rozmowę na temat jego postępowania i w jej trakcie uzmysłowić mu szkodliwość prowadzonych przez niego działań. Działania szkoły powinny koncentrować się jednak na aktywnościach wychowawczych. W przypadku upowszechniania przez sprawców treści nielegalnych (np. pornografii dziecięcej) należy złożyć zawiadomienie o zdarzeniu na policji.
Działania wobec ofiar zdarzenia	Dzieci – ofiary i świadków zdarzenia – należy począwszy od pierwszego etapu interwencji otoczyć opieką psychologiczno-pedagogiczną. Rozmowa z dzieckiem powinna się odbywać z uwzględnieniem jego komfortu psychicznego, z poszanowaniem poufności i podmiotowości ucznia ze względu na fakt, iż kontakt z treściami nielegalnymi może mieć bardzo szkodliwy wpływ na jego psychikę. W trakcie rozmowy należy ustalić okoliczności uzyskania przez ofiarę dostępu do ww. treści. Należy koniecznie powiadomić rodziców lub opiekunów prawnych ofiary o zdarzeniu i uzgodnić z nimi podejmowane działania i formy wsparcia dziecka. Działania szkoły w takich przypadkach powinna cechować poufność i empatia w kontaktach ze wszystkimi uczestnikami zdarzenia oraz osobami udzielającymi wsparcia. W przypadku kontaktu dziecka z treściami szkodliwymi należy dokładnie zbadać sposób, w jaki do niego doszło. Poszukiwanie przez dziecko tego typu treści w sieci lub podsuwanie ich dziecku przez innych może być oznaką niepokojących incydentów ze świata rzeczywistego, np. kontaktów z osobami handlującymi narkotykami czy udziału w procesie rekrutacji do sekty lub innej niebezpiecznej grupy.

Aktywności wobec świadków	W przypadku gdy informacja na temat zdarzenia dotrze do środowiska rówieśniczego ofiary – w klasie czy szkole – wskazane jest podjęcie działań edukacyjnych i wychowawczych.
Współpraca z policją i sądami rodzinnymi	W przypadku naruszenia prawa, np. rozpowszechniania materiałów pornograficznych z udziałem nieletniego lub prób uwiedzenia małoletniego w wieku do 15 lat przez osobę dorosłą, należy – w porozumieniu z rodzicami dziecka – niezwłocznie powiadomić policję.
Współpraca ze służbami i placówkami specjalistycznymi	Kontakt z treściami szkodliwymi lub niebezpiecznymi może wywołać potrzebę skorzystania przez ofiarę ze specjalistycznej opieki psychologicznej. Decyzja o takim kontakcie i skierowaniu na terapię musi zostać podjęta w porozumieniu z rodzicami/opiekunami prawnymi dziecka.

Rodzaje cyberzagrożeń

Eksperci wskazują takie zagrożenia związane z użytkowaniem sieci internetowej jak:

- infoholizm (siecioholizm, netoholizm);
- zaburzenia zdrowia psychicznego i fizycznego, w tym: choroby wzroku i słuchu, schorzenia układu kostno-szkieletowego, tendencje autodestrukcyjne;
- zagrożenia poznawczo-intelektualne, obejmujące między innymi trudności z aktywnym przyswajaniem wiedzy, brak umiejętności weryfikacji informacji, zamknięcie w „bańce informacyjnej";
- zagrożenia moralne, takie jak: cyberpornografia, prostytucja w sieci, sexting, sponsoring i inne;
- niebezpieczeństwa społeczno-wychowawcze dotyczące zwłaszcza postaw, zachowań, relacji i więzi, takie jak: cyberprzemoc i agresja w sieci, hazard internetowy, zaburzenie kontaktów interpersonalnych czy wykorzystywanie internetu przez sekty jako nowej, słabo nadzorowanej przestrzeni werbunkowej;
- negatywne skutki zażywania substancji chemicznych, o których źródłem wiedzy i inspiracji jest przestrzeń internetowa (narkotyki, dopalacze, leki o działaniu psychoaktywnym, sterydy i inne formy dopingu sportowego);
- ryzykowne zachowania z zakresu przestępczości teleinformatycznej, w tym: łamanie praw autorskich, hacking, bezprawne niszczenie informacji, sabotaż komputerowy, rozpowszechnianie wirusów komputerowych czy przestępstwa przeciwko wiarygodności dokumentów[27].

[27] Klasyfikacja za: Bednarek J., Andrzejewska A., (2018), *Zagrożenia dla nastolatków w społeczeństwie wiedzy*, [w:] Ratajek W. (red.), *Edukacja i człowiek w czasach technologii. Szanse, nadzieje i zagrożenia*, Wrocław: Wydawnictwo Humanistyczne Via Ferrata, s. 28–29.

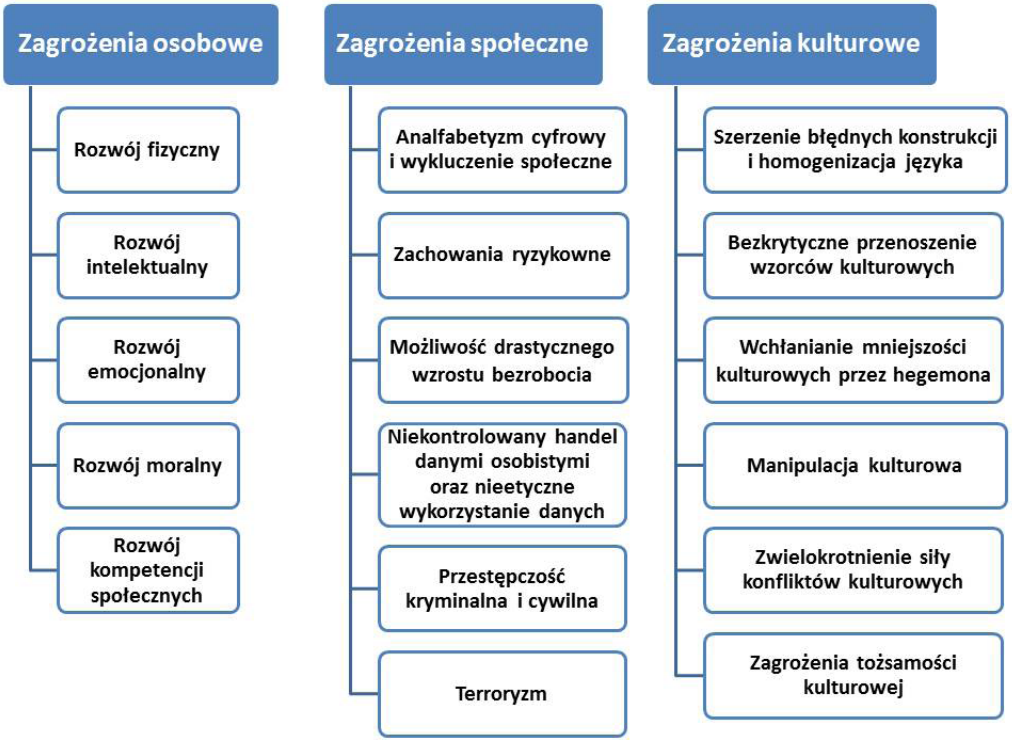
Inny podział cyberzagrożeń wyróżnia siedem podstawowych kategorii:

1. Kontakty z nieodpowiednimi treściami:
    - cyberpornografia;
    - cyberprostytucja (w tym także sexting prowadzący do osiągania korzyści materialnych);
    - treści propagujące niezdrowy tryb życia.
2. Niebezpieczne działania: cyberprzemoc, sexting, samobójstwa z inspiracji i pod wpływem sieci (w tym samobójstwa transmitowane na żywo w internecie, samobójstwa pod wpływem upokorzenia czy gnębienia doznanego w sieci, instruktaże dla samobójców, a także internetowe pakty samobójcze).
3. Niebezpieczne kontakty:
    - uwodzenie dzieci online (*child grooming*);
    - cyberpedofilia.
4. Naruszanie prywatności (*cyberstalking*).
5. Zagrożenia o charakterze seksualnym (sexting, cyberseks).
6. Zespół uzależnienia od internetu (*internet addiction disorder* – IAD), w tym od informacji, pozostawania online (*fear of missing out* – FOMO) oraz od relacji społecznych budowanych i podtrzymywanych w sieci.
7. Cyberprzestępczość i nieuczciwość w sieci:
    - zagrożenia związane z bezpieczeństwem danych przechowywanych w internecie;
    - fałszywe lajki i pliki cookies zawierające szkodliwe oprogramowanie;
    - fałszywe witryny i wyłudzenia danych;
    - ataki hakerskie na serwisy społecznościowe;
    - *tabnabbing* (fałszywe witryny internetowe, podszywające się pod inne serwisy);
    - *clickjacking* (maskowanie odnośnika w celu skłonienia użytkownika do kliknięcia w link podsunięty przez przestępcę);
    - zagrożenia dla systemów mobilnych[28].

Natomiast do zagrożeń osobowych, społecznych i kulturowych wynikających z rozwoju cyberprzestrzeni[29] należą zjawiska wskazane na poniższym schemacie:

[28] Klasyfikacja za: Bębas S., (2018), *Zagrożenia dla dzieci i młodzieży w świecie wirtualnym*, [w:] Ratajek W. (red.), *Edukacja i człowiek w czasach nowych technologii. Szanse, nadzieje i zagrożenia*, Wrocław: Wydawnictwo Humanistyczne Via Ferrata, s. 36–44.

[29] Klasyfikacja za: Tanaś M. , Galanciak S., (2019), *Dziecko w sieci zagrożeń – ryzykowne zachowania internetowe dzieci i młodzieży jako wyzwanie dla edukacji*, [w:] Wrońska A., Lew-Starowicz R., Rywczyńska A. (red.), *Edukacja – relacja – zabawa. Wieloaspektowość internetu w wymiarze bezpieczeństwa dzieci i młodzieży*, Warszawa: Fundacja Rozwoju Systemu Edukacji, s. 49.



Zapewnienie młodym użytkownikom internetu szeroko rozumianego bezpieczeństwa jest podstawowym obowiązkiem dorosłych. Nie można go jednak sprowadzać wyłącznie do tych działań i środków, które przejawiają się w minimalizowaniu skutków różnorodnych zagrożeń lub obejmują wyłącznie system ochrony czy monitoringu. Zapewnienie bezpieczeństwa należy ściśle wiązać z edukacją zarówno dzieci, jak i dorosłych – edukacją, umożliwiającą poznanie rozmaitych zagrożeń, ich źródeł, przejawów, skutków, sposobów radzenia sobie w sytuacjach trudnych, a przede wszystkim sprzyjającej rozwijaniu kompetencji cyfrowych.

2.4. Zagrożenia prywatności

Naruszenie prywatności dotyczące nieodpowiedniego bądź niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka bądź pracownika szkoły	
Podstawy prawne uruchomienia procedury	*Kodeks karny,* art. 190a, RODO[30].
Rodzaj zagrożenia objętego procedurą	Zagrożenie to polega na naruszeniu prywatności dziecka lub pracownika szkoły poprzez nieodpowiednie lub niezgodne z prawem wykorzystanie danych osobowych lub wizerunku dziecka albo pracownika szkoły. Należy zwrócić uwagę, że podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub danych osobowych w celu wyrządzenia jej szkody osobistej lub majątkowej jest w świetle polskiego prawa przestępstwem. Najczęstszymi formami wyłudzenia lub kradzieży danych jest przejęcie profilu na portalu społecznościowym w celu dyskredytacji lub naruszenia dobrego wizerunku ofiary (np. publikacja zdjęć intymnych bądź fotomontażu), szantażowania (w celu uzyskania korzyści finansowych w zamian za niepublikowanie zdjęć bądź treści naruszających reputację ofiary), dokonania zakupów i innych transakcji finansowych (np. w sklepach internetowych na koszt ofiary). Często naruszenia prywatności łączy się z cyberprzemocą.
Sposób postępowania w przypadku wystąpienia zagrożenia	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Gdy sprawcą jest uczeń – kolega ofiary ze szkoły czy klasy – uczniowie lub rodzice powinni skontaktować się z dyrektorem szkoły, wychowawcą lub osobą odpowiedzialną za koordynację działań związanych z bezpieczeństwem cyfrowym na terenie szkoły. W przypadku gdy do naruszenia prywatności poprzez kradzież, wyłudzenie danych osobowych wykorzystanie wizerunku dziecka dochodzi ze strony dorosłych osób trzecich, rodzice powinni skontaktować się bezpośrednio z policją i powiadomić o tym szkołę (zgodnie z *Kodeksem karnym* ściganie następuje wówczas na wniosek pokrzywdzonego). Istotne dla ścigania sprawcy jest uzyskanie dowodów potwierdzających, że sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej.

[30] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych), Dziennik Urzędowy Unii Europejskiej.

Opis okoliczności, analiza, zabezpieczenie dowodów	W pierwszej kolejności należy zabezpieczyć dowody nieodpowiedniego lub niezgodnego z prawem działania – w formie elektronicznej (e-mail, zrzut ekranu oraz adres strony, na której udostępniony został wizerunek dziecka, konwersacja w komunikatorze, SMS). Równolegle należy dokonać zmian tych danych identyfikujących, które zależą od ofiary, tj. haseł i loginów lub kodów dostępu do platform i portali internetowych, tak aby uniemożliwić kontynuację procederu naruszania prywatności – w działaniu tym powinna wspierać ucznia osoba dorosła. Jeśli wykradzione dane zostały wykorzystane w celu naruszenia dobrego wizerunku ofiary bądź w innych celach niezgodnych z prawem, należy dążyć do wyjaśnienia tych działań i usunięcia ich skutków, także tych widocznych w internecie. Likwidacja stron internetowych czy profili w portalach społecznościowych, która wymagać będzie interwencji w zebrane dowody, musi odbywać się za zgodą policji (o ile została powiadomiona). Szczególnej uwagi wymagają incydenty kradzieży tożsamości w celu posłużenia się nią np. podczas zakupu towarów online lub dokonania transakcji finansowych. W tym przypadku należy skontaktować się ze sklepem lub pożyczkodawcą i wyjaśnić charakter zdarzenia. O czynach niezgodnych z prawem należy powiadomić policję.
Identyfikacja sprawcy(-ów)	W przypadku gdy dowody jasno wskazują na konkretnego sprawcę oraz potwierdzają, że sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej, należy je zabezpieczyć i przekazać policji. W przypadku, gdy trudno to ustalić, identyfikacji dokonać powinna policja. W przypadku znanego sprawcy, który jednak nie działał z powyższych pobudek, szkoła powinna dążyć do rozwiązania problemu w ramach działań wychowawczo-profilaktycznych uzgodnionych z rodzicami.
Działania wobec sprawców zdarzenia ze szkoły/spoza szkoły	Gdy sprawcą incydentu jest uczeń szkoły, należy wobec niego – w porozumieniu z rodzicami – podjąć działania wychowawcze, zmierzające do uświadomienia nieodpowiedniego i nielegalnego charakteru czynów, jakich dokonał. Jednym z elementów takich działań powinno być zadośćuczynienie osobie poszkodowanej. Celem tych działań powinno być nie tylko nabycie przez ucznia odpowiedniej wiedzy na temat wagi poszanowania prywatności w codziennym życiu, ale trwała zmiana jego postawy na prezentującą szacunek wobec cudzego wizerunku i prywatności. Działania takie szkoła powinna podjąć niezależnie od powiadomienia policji/sądu rodzinnego. Dyrekcja szkoły powinna podjąć decyzję w sprawie powiadomienia o incydencie policji, biorąc pod uwagę rodzaj czynu oraz wiek sprawcy, jego dotychczasowe zachowanie, postawę po odkryciu incydentu, opinie wychowawcy i pedagoga. Dobrym rozwiązaniem jest uzyskanie interpretacji prawnej radcy prawnego.

Działania wobec ofiar zdarzenia	Nieletnią ofiarę incydentu należy otoczyć – w porozumieniu z rodzicami/opiekunami prawnymi – opieką psychologiczno-pedagogiczną (jeśli jest taka potrzeba) i powiadomić o działaniach podjętych w celu usunięcia skutków działania sprawcy (np. usunięcie z internetu intymnych zdjęć ofiary, zablokowanie dostępu do konta w portalu społecznościowym). Jeśli kradzież tożsamości bądź naruszenie dobrego imienia ofiary jest znane tylko jej i rodzicom, szkoła powinna zapewnić poufność działań, tak aby informacje narażające ofiarę na naruszenie wizerunku nie były rozpowszechniane.
Działania wobec świadków	Gdy kradzież tożsamości bądź naruszenie dobrego imienia ofiary jest znane szerszemu gronu uczniów szkoły, należy podjąć wobec nich działania wychowawcze, zwracające uwagę na negatywną ocenę narażania na uszczerbek wizerunku ucznia – koleżanki lub kolegi – oraz odpowiedzialność prawną.
Współpraca z policją i sądami rodzinnymi	Gdy naruszenie prywatności czy wyłudzenie lub kradzież tożsamości skutkują wyrządzeniem ofierze szkody majątkowej lub osobistej, rodzice ucznia powinni o tym powiadomić policję.
Współpraca ze służbami placówkami specjalistycznymi	W przypadku konieczności podejmowania dalszych działań pomocowych wobec ofiary, można skierować ucznia, za zgodą i we współpracy z rodzicami/opiekunami prawnymi, do placówki specjalistycznej, np. terapeutycznej.

2.5. Nadmierne korzystanie z internetu – procedura reagowania

Zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z internetu	
Podstawy prawne uruchomienia procedury	*Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe* (Dz.U. 2020, poz. 910, z późn. zm.).
Rodzaj zagrożenia objętego procedurą (opis)	Infoholizm (siecioholizm) – nadmierne, obejmujące niekiedy niemal całą dobę, korzystanie z zasobów internetu i gier komputerowych (najczęściej sieciowych) oraz portali społecznościowych przez dzieci. Jego negatywne efekty polegają na pogarszaniu się stanu zdrowia fizycznego (np. choroby oczu, padaczka ekranowa, choroby kręgosłupa) i psychicznego (irytacja, rozdrażnienie, spadek sprawności psychofizycznej, a nawet depresja), zaniedbywaniu codziennych czynności, oraz osłabianiu relacji rodzinnych i społecznych.

Sposób postępowania w przypadku wystąpienia zagrożenia	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	W przypadku nadmiernego korzystania z komputera lub podejrzenia infoholizmu konieczne jest podejmowanie działań pomocowych – głównie skierowanie ucznia, za zgodą i we współpracy z rodzicami/opiekunami prawnymi, do placówki specjalistycznej, np. terapeutycznej. Kluczowe są tutaj pozostałe objawy wskazane wyżej. Nauczyciele w szkole powinni zainteresować się przypadkami dzieci nieangażujących się w życie klasy, a poświęcającymi wolne chwile na kontakt online lub przychodzącymi do szkoły po nieprzespanej nocy. Rzadziej zgłoszeń można się spodziewać od rówieśników dziecka nadmiernie korzystającego z sieci.
Opis okoliczności, analiza, zabezpieczenie dowodów	Reakcja szkoły powinna polegać w pierwszej kolejności na ustaleniu we współpracy z rodzicami skutków zdrowotnych i psychicznych, jakie nadmierne korzystanie z zasobów internetu wywołało u dziecka (np. gorsze wyniki w nauce, niedosypianie, niedojadanie, rezygnacja z dawnych zainteresowań, załamanie się relacji z rodziną czy rówieśnikami). Celem tych ustaleń jest wybór odpowiedniej ścieżki rozwiązywania problemu: z udziałem specjalistów (lekarzy, terapeutów) lub bez – wyłącznie w szkole.
Działania wobec ofiar zdarzenia	Osoba, której problem dotyczy, powinna zostać otoczona zindywidualizowaną opieką pedagoga/psychologa szkolnego. Pierwszym etapem powinno być zebranie wywiadu od ucznia i jego rodziców w celu określenia sytuacji i wstępnego ustalenia poziomu zagrożenia. Następnie, w zależności od stwierdzonego zagrożenia, proponuje się konsultacje ze specjalistą, który pozwoli zdiagnozować poziom zagrożenia, określić przyczyny popadnięcia ucznia w nałóg (np. takie jak trudna sytuacja domowa, brak sukcesów edukacyjnych w szkole, izolacja w środowisku rówieśniczym) i ukazać specyfikę przypadku. Każde dziecko, u którego podejrzewa się nałóg korzystania z internetu, powinno zostać profesjonalnie zdiagnozowane za zgodą rodziców/opiekunów prawnych przez psychologa szkolnego lub poradnię psychologiczno-pedagogiczną. Dziecku w trakcie wsparcia należy zapewnić komfort psychiczny – o jego sytuacji i specyfice uwarunkowań osobistych powinni zostać powiadomieni wszyscy uczący i oceniający je nauczyciele. Z rodzicami/opiekunami prawnymi dziecka należy omówić wspólne rozwiązania trudnej sytuacji. Tylko synergiczne współdziałanie rodziców i szkoły może zagwarantować powodzenie podejmowanych działań wspierających dziecko.
Działania wobec świadków	Jeśli świadkami problemu są rówieśnicy dziecka, należy im w rozmowie zwrócić uwagę na negatywne aspekty nadmiernego korzystania z zasobów internetu oraz zaapelować o wsparcie dziecka dotkniętego problemem.

Współpraca ze służbami i placówkami specjalistycznymi	W przypadku zdiagnozowania przez psychologa uzależnienia od internetu dziecko powinno zostać skierowane, we współpracy z rodzicami/opiekunami prawnymi, do placówki specjalistycznej oferującej program terapeutyczny.

2.6. Dezinformacja, bezkrytyczna wiara w treści zamieszczone w internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, w tym szkodliwość reklam – procedury reagowania

Bezkrytyczna wiara w treści zamieszczone w internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, szkodliwość reklam	
Podstawy prawne uruchomienia procedury	*Ustawa z 14 grudnia 2016 r. Prawo oświatowe* (Dz.U. 2020, poz. 910, z późn. zm.).
Rodzaj zagrożenia objętego procedurą (opis)	Brak umiejętności odróżniania informacji prawdziwych od nieprawdziwych publikowanych w internecie, bezkrytyczne uznawanie za prawdę tez publikowanych na forach internetowych, kierowanie się informacjami zawartymi w reklamach. Taka postawa dzieci prowadzić może do zagrożeń życia i zdrowia (np. stosowania wyniszczającej diety, samookaleczeń), skutkować rozczarowaniami i porażkami życiowymi (w efekcie korzystania z fałszywych informacji), utrudniać lub uniemożliwiać osiąganie dobrych wyników w edukacji (korzystanie z upraszczających i zawężających wiedzę nieprofesjonalnych opracowań), a także do utrwalania się u ucznia ambiwalentnych postaw moralnych. Działania mające na celu wyposażenie uczniów w kompetencje pozwalające na radzenie sobie z dezinformacją i krytyczne podejście do informacji powinny być elementem edukacji prowadzonej dla całej społeczności szkolnej, nie tylko w ramach realizacji zapisów podstawy programowej.
Sposób postępowania w przypadku wystąpienia zagrożenia	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Uczniowie nieumiejący odróżniać prawdy od fałszu informacji publikowanych w internecie powinni być identyfikowani przez nauczycieli i wychowawców w trakcie lekcji wszystkich przedmiotów. Często niepożądana postawa ujawnia się podczas przygotowania prac domowych i jest stosunkowo łatwa do zidentyfikowania przez oceniającego je nauczyciela. Procedury interwencyjne mają uzasadnienie w przypadku uczniów podejmujących zachowania ryzykowne (np. samookaleczających się lub stosujących ryzykowne diety itp.).

Opis okoliczności, analiza, zabezpieczenie dowodów	Posługiwanie się nieprawdziwymi informacjami zaczerpniętymi z internetu w procesie dydaktycznym – podczas lekcji lub w zadaniach domowych – każdorazowo powinno być zauważone przez nauczyciela, przeanalizowane i skomentowane.
Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Wystarczającą reakcją jest opublikowanie sprostowania nieprawdziwych informacji i – w miarę możliwości – rozpowszechnienie go w internecie, na portalach o zbliżonej tematyce.
Działania wobec ofiar zdarzenia i świadków	Szkoła powinna prowadzić działania profilaktyczne – edukację medialną (informacyjną), np. w trakcie zajęć nieinformatycznych (np. historii, języka polskiego) przez wszystkie lata nauki ucznia w szkole lub podczas lekcji ukierunkowanych na zdobywanie przez dzieci i młodzież kompetencji cyfrowych. Edukacja medialna może być prowadzona również na zajęciach pozalekcyjnych. Działania mające na celu zapobieganie angażowaniu się młodzieży w zachowania autodestrukcyjne powinny być zaplanowane w ramach programu profilaktycznego szkoły oraz skierowane od ogółu uczniów (profilaktyka uniwersalna).

2.7. Cyberprzemoc – procedura reagowania

Cyberprzemoc	
Podstawy prawne uruchomienia procedury	*Kodeks karny:* art.190 § 1–2, art. 190a § 1–3, art. 212 § 1–2, art. 256, art. 267 § 1–4, art. 268a. Statut szkoły, regulamin szkoły. Niektóre akty cyberprzemocy stanowiące naruszenie prawa mogą być ścigane na wniosek pokrzywdzonego (w przypadku dzieci do 18. r.ż. na wniosek rodziców lub opiekunów prawnych). Są to: groźba karalna (art. 190 *Kodeksu karnego* – dalej kk), zmuszanie groźbą do określonego działania (art. 191 kk), uporczywe nękanie – stalking (art. 190a kk), naruszenie wizerunku (art. 23 i 24 *Kodeksu cywilnego*), zniesławienie/znieważenie (art. 216 i 212 kk), włamanie (art. 267 i 268a kk). Czyny karalne ścigane z urzędu powinny być niezwłocznie zgłoszone na policję lub do prokuratury. Dotyczy to sytuacji takich jak rozpowszechnianie zdjęć lub filmów z udziałem osoby nieletniej, mających cechy pornograficzne, czy publikowanie materiałów prezentujących seksualne wykorzystywanie nieletnich (art. 202 kk).

Rodzaj zagrożenia objętego procedurą	Cyberprzemoc – przemoc z użyciem technologii informacyjno-komunikacyjnych, głównie internetu oraz telefonów komórkowych. Podstawowe formy zjawiska to nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów, z użyciem sieci oraz podszywanie się w sieci pod kogoś wbrew jego woli. Do działań określanych mianem cyberprzemocy wykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, media społecznościowe, grupy dyskusyjne, SMS i MMS[31].
Telefony alarmowe krajowe i lokalne	Dziecięcy Telefon Zaufania telefon rzecznika praw dziecka: 800 12 12 12 telefon zaufania dla dzieci i młodzieży: 116 111, https://11611.pl/ telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci: 800 100 100, https://800100100.pl/ Zgłaszanie nielegalnych treści: dyzurnet.pl dyzurnet@dyzurnet.pl
Sposób postępowania w przypadku wystąpienia zagrożenia	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Akt cyberprzemocy może zostać ujawniony przez ofiarę, świadka (np. innego ucznia, nauczyciela, rodzica) lub osobę bliską ofierze (np. rodzice, rodzeństwo, przyjaciele). W każdym przypadku należy ze spokojem wysłuchać osoby zgłaszającej i okazać jej wsparcie, trzeba podziękować jej za zaufanie i zgłoszenie tej sprawy. Jeśli zgłaszającym jest ofiara cyberprzemocy, podejmując działania, przede wszystkim należy okazać wsparcie – z zachowaniem jej podmiotowości i poszanowaniem jej uczuć. Trzeba potwierdzić, że ujawnienie przemocy jest dobrą decyzją. Taką rozmowę należy przeprowadzić w miejscu bezpiecznym, zapewniającym ofierze intymność. Nie należy podejmować kroków, które mogłyby prowadzić do powtórnej wiktymizacji czy wzbudzić podejrzenia sprawcy (np. wywoływać ucznia z lekcji do gabinetu dyrektora). Jeśli osobą zgłaszającą nie jest ofiara, najpierw warto poprosić o opis sytuacji, także z zachowaniem podmiotowości i poszanowaniem uczuć osoby zgłaszającej (np. jej strachu przed posądzeniem o donosicielstwo, obawy o własne bezpieczeństwo).

[31] Pyżalski J., (2012), *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Kraków: Impuls; Wojtasik Ł., *Cyberprzemoc – charakterystyka zjawiska*, [w:] Wojtasik Ł. (red.), *Jak reagować na cyberprzemoc? Poradnik dla szkół*, Fundacja Dajemy Dzieciom Siłę, https://www.edukacja.fdds.pl/cb0428e3-c0d-8-47cb-8508-1b865100a1f9/Extras/ksiazka-jak_reagowac_na_cyberprzemoc-FDDS-12042017.pdf [dostęp: 29.08.2020 r.].

Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	W każdej sytuacji w trakcie ustalania okoliczności trzeba określić charakter zdarzenia (rozmiar i rangę szkody, jednorazowość/powtarzalność). Realizując procedurę, należy unikać działań, które mogłyby wtórnie stygmatyzować ofiarę lub sprawcę, np.: wywoływanie uczniów z lekcji, konfrontowanie ofiary i sprawcy, niewspółmierna kara, wytykanie palcami itd. Trzeba dokonać oceny, czy zdarzenie wyczerpuje znamiona cyberprzemocy, czy jest np. niezbyt udanym żartem (wtedy trzeba podjąć działania profilaktyczne mające na celu niedopuszczenie do eskalacji tego typu zachowań.
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zabezpieczyć wszystkie dowody związane z aktem cyberprzemocy (np. zrobić kopię materiałów, zanotować datę i czas otrzymania materiałów, dane nadawcy, adresy stron www, historię połączeń itd.). W trakcie zbierania materiałów trzeba zadbać o bezpieczeństwo osób zaangażowanych w problem.
Identyfikacja sprawcy(-ów)	Identyfikacja sprawcy(-ów) często jest możliwa dzięki zebranym materiałom – wynikom rozmów z osobą zgłaszającą, z ofiarą – oraz analizie zebranych materiałów. Ofiara często domyśla się, kto stosuje wobec niej cyberprzemoc. Jeśli ustalenie sprawcy wydaje się niemożliwe, a w ocenie kadry pedagogicznej jest konieczne, należy skontaktować się z policją. Bezwzględnie należy zgłosić rozpowszechnianie nagich zdjęć osób poniżej 18. r.ż. (art. 202 § 3 kk).
Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog szkolny powinien przeprowadzić z nim rozmowę o jego zachowaniu. Rozmowa taka ma służyć ustaleniu okoliczności zdarzenia, jego wspólnej analizie (w tym np. przyjrzeniu się przyczynom), a także próbie rozwiązania sytuacji konfliktowej (w tym sposobów zadośćuczynienia ofiarom cyberprzemocy). Cyberprzemoc powinna podlegać sankcjom określonym w wewnętrznych przepisach szkoły (m.in. w statucie, kontrakcie, regulaminie). Szkoła może stosować konsekwencje przewidziane dla sytuacji „tradycyjnej" przemocy. Warto jednak rozszerzyć katalog dostępnych środków, np. o czasowy zakaz korzystania ze szkolnej pracowni komputerowej w czasie wolnym i przynoszenia do szkoły akcesoriów elektronicznych (np. PSP, MP3) itp. W sytuacji, gdy sprawca jest nieznany, podstawowe działanie polega na przerwaniu aktu cyberprzemocy (zawiadomieniu administratora serwisu w celu usunięcia materiału po wcześniejszym zabezpieczeniu dowodów), zapewnieniu pomocy psychologiczno-pedagogicznej poszkodowanemu oraz wsparciu rodziców poszkodowanego ucznia w ewentualnym zgłoszeniu sprawy policji.

Działania wobec ofiar zdarzenia	W pierwszej kolejności należy udzielić wsparcia ofierze. Musi się ona czuć bezpieczna i otoczona opieką dorosłych. Na poczucie bezpieczeństwa dziecka wpływa fakt, że wie ono, iż szkoła podejmuje kroki w celu rozwiązania problemu. Podczas rozmowy z uczniem – ofiarą cyberprzemocy – należy zapewnić go, że nie jest winny zaistniałej sytuacji oraz że nikt nie ma prawa zachowywać się w ten sposób wobec niego, a także podkreślić, że dobrze zrobił, ujawniając sytuację. Należy okazać zrozumienie dla jego uczuć, w tym trudności z ujawnieniem okoliczności wydarzenia, strachu, wstydu. Trzeba podkreślić, że szkoła nie toleruje przemocy i że zostaną uruchomione odpowiednie procedury interwencyjne. Należy poinformować ucznia o krokach, jakie może podjąć szkoła, i sposobach, w jaki może zapewnić mu bezpieczeństwo. Należy pomóc ofierze (rodzicom/opiekunom prawnym) w zabezpieczeniu dowodów (to może być dla niej zadanie trudne zarówno ze względów technicznych, jak i emocjonalnych), omówić strategię postępowania wobec sprawcy (np. zerwanie kontaktu ze sprawcą, niepodejmowanie agresywnej konfrontacji itp.), zadbać o podstawowe zasady bezpieczeństwa online (np. nieudostępnianie swoich danych kontaktowych, kształtowanie własnego wizerunku itd.). Pomoc ofierze nie może kończyć się w momencie zamknięcia procedury. Warto monitorować sytuację, czuwać nad jej bezpieczeństwem, np. zwracać uwagę, czy nie są podejmowane wobec niej dalsze działania przemocowe, obserwować, jak sobie radzi w grupie po ujawnieniu incydentu cyberprzemocy. W działania wobec ofiary należy także włączyć rodziców/opiekunów ofiary – trzeba na bieżąco ich informować o sytuacji, pamiętając przy tym o podmiotowym traktowaniu dziecka – mówiąc mu o tym i starając się uzyskać jego akceptację dla udziału rodziców. Jeśli dziecko nie wyraża zgody, należy omówić z nim jego obawy, a jeśli to nie pomaga, powołać się na obowiązujące nas zasady i przekazać informację rodzicom. W trakcie rozmowy z dzieckiem i/lub jego rodzicami/opiekunami, jeśli jest to wskazane, można zaproponować pomoc specjalisty (np. psycholog szkolny, poradnia psychologiczno-pedagogiczna) oraz przekazać informację o możliwości zgłoszenia sprawy policji.
Działania wobec świadków	Należy zadbać o bezpieczeństwo świadków zdarzenia, zwłaszcza jeśli byli oni osobami ujawniającymi cyberprzemoc. W trakcie rozmowy ze świadkami należy okazać zrozumienie i empatię wobec ich uczuć – obawy przed posądzeniem o donosicielstwo, strachu przed staniem się kolejną ofiarą sprawcy itp.

Współpraca z policją i sądami rodzinnymi	Samo wystąpienie zjawiska cyberprzemocy nie jest jednoznaczne z koniecznością zaangażowania policji i sądu rodzinnego – procedura powinna umożliwiać rozwiązanie sytuacji problemowej na poziomie pracy wychowawczej szkoły. Szkoła powinna powiadomić odpowiednie służby (np. sąd rodzinny), gdy wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje wobec sprawcy wynikające ze statutu i/lub regulaminu) i interwencje pedagogiczne, a ich zastosowanie nie przynosi pożądanych rezultatów (np. nie ma zmian postawy ucznia). Kontaktu z policją wymagają wszelkie sytuacje, w których zostało naruszone prawo (np. groźby karalne, świadome publikowanie nielegalnych treści, rozpowszechnianie nagich zdjęć z udziałem małoletnich). Za zgłoszenie powinien odpowiadać dyrektor szkoły.
Współpraca z dostawcami internetu i operatorami telekomunikacyjnymi	Kontakt z dostawcą usługi może być wskazany w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów. Do podjęcia takiego działania stymuluje administratora serwisu art. 14 *Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (t.j. Dz.U. 2020, poz. 344).

2.8. Seksting – procedura reagowania

Seksting, prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich	
Podstawy prawne uruchomienia procedury	*Kodeks karny* – art. 191a, art. 202 § 1–4c.
Rodzaj zagrożenia objętego procedurą	Seksting to przesyłanie wiadomości drogą elektroniczną w formie wiadomości MMS lub z wykorzystaniem różnych aplikacji i komunikatorów albo publikowanie np. na portalach (społecznościowych) prywatnych treści, głównie zdjęć lub filmów, o kontekście seksualnym, erotycznym.

Sposób postępowania w przypadku wystąpienia zagrożenia	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	W przypadku sekstingu zgłoszeń dokonują głównie rodzice lub opiekunowie prawni dziecka – ofiary. Czasami informacja dociera do szkoły bezpośrednio od ucznia lub z grona bliskich znajomych dziecka. W rzadkich wypadkach nauczyciele i inni pracownicy szkoły sami identyfikują takie zdarzenia w sieci. Delikatny charakter sprawy, a także odpowiedzialność karna sprawcy, wymagają zachowania daleko posuniętej dyskrecji i profesjonalnej reakcji. Niekiedy zgłoszenia dokonują ofiary lub osoby je znające.
Opis okoliczności, analiza, zabezpieczenie dowodów	Wyróżniamy 3 podstawowe rodzaje sekstingu, które skutkują koniecznością realizacji zmodyfikowanych procedur reagowania: **Rodzaj 1.** Wymiana materiałów o charakterze seksualnym następuje tylko w ramach związku między dwojgiem rówieśników. Materiały nie uległy rozprzestrzenieniu dalej. **Rodzaj 2.** Materiały o charakterze seksualnym zostały rozesłane większej liczbie osób, jednak nie dochodzi do cyberprzemocy na tym tle. Młodzież traktuje materiał jako formę wyrażenia siebie. **Rodzaj 3.** Materiały zostały rozesłane większej liczbie osób (bez względu na intencje) i na tym tle dochodzi do cyberprzemocy.
Identyfikacja sprawcy (-ów)	Identyfikacja sprawcy będzie możliwa przede wszystkim dzięki zabezpieczeniu dowodów – przesyłanych zdjęć czy zrzutów ekranów portali, w których opublikowano zdjęcie(-a). W niektórych przypadkach seksting może nosić znamiona przestępstwa związanego z produkcją oraz rozpowszechnianiem materiałów pornograficznych z udziałem osoby małoletniej (poniżej 18. r.ż.) – art. 202 § 3 i 4 kk, dlatego skrupulatność i wiarygodność dokumentacji ma duże znaczenie. Należy przy tym przestrzegać zasad dyskrecji, szczególnie w środowisku rówieśniczym ofiary.
Działania wobec sprawców zdarzenia ze szkoły/spoza szkoły	Zidentyfikowani małoletni sprawcy sekstingu winni zostać wezwani do dyrekcji szkoły, gdzie zostaną im przedstawione dowody ich aktywności. Niezależnie od zakresu negatywnych zachowań i działań, wszyscy sprawcy powinni otrzymać wsparcie pedagogiczne i psychologiczne. Konieczne są także rozmowy ze sprawcami w obecności ich rodziców zaproszonych do szkoły. **Rodzaj 1.** Dalsze działania poza zapewnieniem wsparcia i opieki psychologiczno-pedagogicznej nie są konieczne, jednak istotne jest pouczenie sprawców zdarzenia, że dalsze rozpowszechnianie materiałów może być nielegalne i będzie miało poważniejsze konsekwencje, w tym prawne.

Działania wobec sprawców zdarzenia ze szkoły/spoza szkoły	**Rodzaj 2.** Niektóre tego typu materiały mogą zostać uznane za pornograficzne, w takim wypadku na dyrektorze szkoły/placówki ciąży obowiązek zgłoszenia incydentu policji. Rozpowszechnianie materiałów pornograficznych z udziałem nieletnich jest przestępstwem ściganym z urzędu (art. 202 *Kodeksu karnego*), dlatego też dyrektor szkoły/placówki jest zobowiązany do zgłoszenia incydentu policji i/lub do sądu rodzinnego. Wszelkie działania wobec sprawców incydentu powinny być podejmowane w porozumieniu z ich rodzicami lub opiekunami prawnymi. **Rodzaj 3.** W sytuacji zaistnienia znamion cyberprzemocy należy dodatkowo zastosować procedurę: cyberprzemoc.
Działania wobec ofiar zdarzenia	W razie upublicznienia przypadku sekstingu w środowisku rówieśniczym pierwszą reakcją szkoły i rodziców, oprócz dokumentacji dowodów, winno być otoczenie opieką psychologiczno-pedagogiczną ofiary oraz zaproponowanie odpowiednich działań wychowawczych. Rozmowa na temat identyfikacji potencjalnego sprawcy powinna być realizowana z uwzględnieniem komfortu psychicznego dziecka – ofiary sekstingu, z jego poszanowaniem.
Działania wobec świadków	Jeśli przypadek sekstingu zostanie upowszechniony w środowisku rówieśniczym, np. poprzez media społecznościowe czy MMS, wśród uczniów tej samej szkoły lub klasy lub publikację na portalu społecznościowym, należy podjąć działania wychowawcze, uświadamiające negatywne aspekty moralne sekstingu oraz narażanie się na dotkliwe kary osób, które go stosują.
Współpraca z policją i sądami rodzinnymi	W przypadku publikacji lub upowszechniania zdjęć o charakterze pornografii dziecięcej (co jest wykroczeniem ściganym z urzędu) kierownictwo szkoły jest zobowiązane do powiadomienia o tym zdarzeniu policji lub sądu rodzinnego.
Współpraca ze służbami społecznymi, placówkami specjalistycznymi	Kontakt ofiar z placówkami specjalistycznymi może okazać się konieczny w indywidualnych przypadkach. O skierowaniu do nich decyzję powinien podjąć psycholog/pedagog szkolny wspólnie z rodzicami/opiekunami prawnymi ofiary.

2.9. Bezprawne użycie cudzego wizerunku w sieci – procedura reagowania

Bezprawne użycie wizerunku w sieci	
Podstawy prawne uruchomienia procedury	*Kodeks cywilny* i *Ustawa z dnia 4 lutego 1994 r.* o *prawie autorskim i prawach pokrewnych*, t.j. Dz.U. 2019, poz. 1231; 2020, poz. 288.
Rodzaj zagrożenia objętego procedurą	Bezprawne, tj. bez wymaganej prawem zgody, użycie wizerunku osoby fizycznej w internecie.
Sposób postępowania w przypadku wystąpienia zagrożenia	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Wizerunek jest jednym z dóbr osobistych wymienionych w art. 23 *Kodeksu cywilnego* obok zdrowia, wolności, czci, swobody sumienia, nazwiska lub pseudonimu, tajemnicy korespondencji, nietykalności mieszkania, twórczości naukowej, artystycznej, wynalazczej i racjonalizatorskiej. Wizerunek ma cechy prawa niezbywalnego, czyli takiego, które nie może zostać komuś sprzedane czy pożyczone. Podobnie jak inne dobra osobiste, pozostaje pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Ochronę wizerunku gwarantuje także prawo autorskie. Art. 81 ust. 1 zd. 1 *Ustawy o prawie autorskim i prawach pokrewnych* stanowi, że: *Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej*. Naruszeniem tego prawa jest bezprawne rozpowszechnianie wizerunku rozumiane jako publiczne udostępnianie, czy też stworzenie możliwości zapoznania się z wizerunkiem np. użytkownikom internetu. Uczniowie bardzo często udostępniają zarówno swoje zdjęcia, jak i zdjęcia kolegów, w mediach społecznościowych bez uzyskania ich zgody w myśl zasady, że skoro kolega nie pyta, czy może udostępnić moje zdjęcie, to ja również nie będę o to pytał. Problem może pojawić się w sytuacji upublicznienia zdjęcia/filmu ukazującego kolegę lub koleżankę w sposób prześmiewczy i poniżający. Należy pamiętać, że opublikowanie czyjegoś zdjęcia bez zgody tej osoby może skutkować odpowiedzialnością cywilną i karną osoby, która takiej publikacji się dopuściła. Dlatego należy pamiętać o wcześniejszym uzyskaniu zgody osoby, której wizerunek ma zostać opublikowany.

Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Przepisy nie wymagają żadnej szczególnej formy. Oświadczenie woli osoby, której wizerunek ma zostać wykorzystany, może być wyrażone przez każde zachowanie, które ujawni tę wolę w sposób dostateczny. Zgoda na publikowanie wizerunku powinna zostać wyrażona wprost. Jednocześnie osoba, która takiej zgody udziela, musi mieć pełną świadomość formy, w jakiej zostanie przedstawiony jej wizerunek, miejsca i czasu publikacji tego wizerunku, ewentualnego zestawienia jej wizerunku z innymi wizerunkami czy towarzyszącego publikacji wizerunku komentarza. Z art. 24 § 1 i 2 *Kodeksu cywilnego* wynika, że osoba, której dobro osobiste zostało zagrożone cudzym działaniem, może żądać zaniechania, czyli zaprzestania tego działania, o ile jest ono bezprawne. Dodatkowo może także żądać, aby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w *Kodeksie cywilnym* ofiara może też żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny. Jak wiemy z prasy i telewizji, konieczność sprostowania i zapłata określonej kwoty są bardzo częste w kontekście procesów o naruszenie dóbr osobistych. Ponadto należy pamiętać, że jeśli wskutek naruszenia dóbr osobistych została wyrządzona szkoda majątkowa, to można na zasadach określonych w *Kodeksie cywilnym* żądać jej naprawienia. Przepisy te w niczym nie uchybiają uprawnieniom wynikającym z *Ustawy o prawie autorskim i prawach pokrewnych*. Zgodnie z art. 78 ust. 1 ustawy osoba, której prawa zostały zagrożone cudzym działaniem, może żądać zaniechania tego działania. W razie dokonanego naruszenia może także żądać, aby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności aby złożyła publiczne oświadczenie o odpowiedniej treści i formie. Natomiast jeżeli naruszenie było zawinione, sąd może przyznać osobie, której prawa zostały naruszone, odpowiednią sumę pieniężną tytułem zadośćuczynienia za doznaną krzywdę lub, na wyraźne żądanie twórcy, zobowiązać sprawcę, aby wpłacił odpowiednią sumę pieniężną na wskazany cel społeczny.
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zebrać informacje przede wszystkim o: • osobie dokonującej zgłoszenia, czy jest do tego uprawniona, tj. czy to jej wizerunek lub wizerunek osoby, która jest pod jej władzą rodzicielską, został naruszony bezprawnym działaniem; • okolicznościach zdarzenia; • możliwych dowodach, np. zrzut ekranu dokumentujący bezprawne użycie wizerunku.

Identyfikacja sprawcy (-ów)	Dochodzenie naruszeń dóbr osobistych, w tym wizerunku, jest, co do zasady działaniem podejmowanym z inicjatywy samego uprawnionego przed sądami. Natomiast w przypadku naruszeń stanowiących przestępstwo dodatkowo mogą być zaangażowane organy ścigania.
Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Decyzja o dalszych krokach prawnych w sprawach o naruszenie dóbr osobistych, w tym wizerunku, należy do osoby, której wizerunek został bezprawnie użyty w internecie. Szkoła, oprócz realizacji zapisów podstawy programowej związanych z prawem autorskim, może na lekcjach wychowawczych proponować aktywności, których celem będzie wprowadzenie uczniów w tematykę związaną z bezpiecznym i przemyślanym udostępnianiem wizerunku w internecie, w tym przede wszystkim w mediach społecznościowych. Działania prewencyjne mogą zapobiec podobnym zdarzeniom w przyszłości.
Działania wobec ofiar zdarzenia	Ofiarę zdarzenia, w szczególności jeśli wizerunek został bezprawnie użyty w sposób prześmiewczy i poniżający, należy objąć opieką psychologa lub pedagoga szkolnego.
Działania wobec świadków	W przypadku gdy więcej osób wiedziało o bezprawnym użyciu wizerunku w sposób prześmiewczy lub poniżający, należy przeprowadzić z nimi rozmowy wychowawcze mające na celu uzmysłowienie im problemu i ukształtowanie w nich postawy sprzeciwu wobec podobnych działań.
Współpraca z policją i sądami rodzinnymi	Decyzja o dalszych krokach prawnych w sprawach o naruszenie dóbr osobistych, w tym wizerunku, należy do uprawnionego. Szkoła może zaangażować się w spór, jeśli dotyczy to sytuacji, w której bezprawnego użycia wizerunku dopuścił się uczeń wobec drugiego ucznia, np. w charakterze mediatora pomiędzy stronami w celu uniknięcia procesu sądowego.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	Informacje, szkolenia dla pracowników szkoły oraz pogadanki dla uczniów z zakresu świadomego i zgodnego z prawem użycia wizerunku innej osoby w internecie.

2.10. Niebezpieczne kontakty w internecie – procedura reagowania

Nawiązywanie niebezpiecznych kontaktów w internecie – uwodzenie, zagrożenie pedofilią	
Podstawy prawne uruchomienia procedury	*Kodeks karny*: art. 200, art. 200a § 1 i 2, art. 286 § 1.
Rodzaj zagrożenia objętego procedurą (opis)	Zagrożenie obejmuje kontakt osoby dorosłej z małoletnią w celu zainicjowania znajomości prowadzących do wyłudzenia poufnych informacji, nawiązania kontaktów seksualnych, skłonienia dziecka do zachowań niebezpiecznych dla jego zdrowia i życia lub wyłudzenia własności (np. danych, pieniędzy, cennych przedmiotów rodzinnych).
Telefony alarmowe krajowe	Telefon zaufania dla dzieci i młodzieży: 116 111, https://116111.pl/ Telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci: 800 100 100, https://800100100.pl/ Zgłaszanie nielegalnych treści: dyzurnet.pl dyzurnet@dyzurnet.pl, 801 615 005
Sposób postępowania w przypadku wystąpienia zagrożenia	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Osobami najczęściej zgłaszającymi omawiany problem są rodzice/opiekunowie prawni dziecka lub osoby „ścigające pedofili". W pierwszym przypadku informacja trafia najpierw do szkół, w drugim – na policję. Zdarza się, że informacja uzyskiwana jest ze środowiska rówieśników ofiary. Kluczowe znaczenie w działaniach szkoły ma czas reakcji – szybkość przeciwdziałania zagrożeniu ze względu na niezwykle szkodliwe konsekwencje realizacji kontaktu online, przeradzającego się w zachowania w świecie rzeczywistym: uwiedzenie i wykorzystanie seksualne, kidnaping, a także wyłudzenie pieniędzy czy przedmiotów dużej wartości. W przypadku niebezpiecznych kontaktów inicjowanych w internecie może dochodzić do zagrożenia życia i zdrowia dziecka, szantażu i przymusu realizacji czynności seksualnych.
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zidentyfikować i zabezpieczyć w szkole, w formie elektronicznej, dowody działania dorosłego sprawcy uwodzenia (zapisy rozmów w komunikatorach czy na portalach społecznościowych, zrzuty ekranowe, zdjęcia, wiadomości e-mail). Jednocześnie bezzwłocznie należy zawiadomić policję o wystąpieniu zdarzenia.

Identyfikacja sprawcy(-ów)	Ze względu na bezpieczeństwo nie należy podejmować samodzielnych działań w celu dotarcia do sprawcy, lecz udzielać wszelkiego możliwego wsparcia organom ścigania, m.in. zabezpieczyć i przekazać zebrane dowody. Identyfikacja sprawcy wykracza poza kompetencje i możliwości szkoły w większości przypadków uwodzenia przez internet.
Działania wobec sprawców ze szkoły/ spoza szkoły	Nie należy podejmować aktywności zmierzających bezpośrednio do kontaktu ze sprawcą. Zadaniem szkoły jest zebranie dowodów i opieka nad ofiarą i ewentualnymi świadkami.
Działania wobec ofiar zdarzenia	W każdym przypadku próby nawiązania niebezpiecznego kontaktu – np. w celu werbunku do sekty lub grupy promującej niebezpieczne zachowania, a także rekrutacji do grupy terrorystycznej – należy przede wszystkim zapewnić ofierze opiekę psychologiczną i poczucie bezpieczeństwa. Podobnego wsparcia należy udzielić w przypadku zaobserwowania zachowań uczniów zagrażających ich zdrowiu i życiu (samookaleczenia, zażywanie substancji psychoaktywnych), bowiem zachowania te mogą być inicjowane i wzmacniane poprzez kontakty w internecie. O możliwym związku takich zachowań dzieci z inspiracją płynącą z internetu należy powiadomić rodziców. Pierwszą czynnością w ramach reakcji na zagrożenie jest otoczenie ofiary pomocą psychologiczno-pedagogiczną we współpracy szkoły z rodzicami/opiekunami prawnymi. W trakcie rozmowy z dzieckiem prowadzonej z uwzględnieniem jego komfortu psychicznego przez wychowawcę/pedagoga/psychologa/pracownika szkoły, do którego dziecko ma szczególne zaufanie, należy uzyskać wszelkie możliwe informacje o sprawcy i przekazać je policji. Trzeba upewnić się, że kontakt ofiary ze sprawcą został przerwany, a dziecko odzyskało poczucie bezpieczeństwa. Towarzyszyć temu powinna analiza sytuacji domowej (rodzinnej) dziecka, w której tkwić może źródło poszukiwania kontaktów w internecie. Dziecku należy udzielić profesjonalnej opieki terapeutycznej i/lub lekarskiej. Wszelkie działania szkoły wobec dziecka powinny być uzgadniane z rodzicami/opiekunami prawnymi i inicjowane za ich zgodą.
Działania wobec świadków	Jeżeli zgłaszającym zagrożenie był rówieśnik ofiary, należy docenić jego prospołeczną postawę.
Współpraca z policją i sądami rodzinnymi	W przypadkach naruszenia prawa – szczególnie w przypadku uwodzenia dziecka do lat 15 – obowiązkiem szkoły jest powiadomienie policji lub sądu rodzinnego.

Współpraca ze służbami społecznymi i placówkami specjalistycznymi	W przypadkach uwiedzenia nieletnich przez osoby dorosłe rekomenduje się – w porozumieniu z rodzicami/opiekunami prawnymi – skierowanie ofiary na terapię do placówki specjalistycznej opieki psychologicznej.

2.11. Łamanie prawa autorskiego – procedura reagowania

Łamanie prawa autorskiego	
Podstawy prawne uruchomienia procedury	*Ustawa o prawie autorskim i prawach pokrewnych*, *Kodeks karny, Kodeks cywilny.*
Rodzaj zagrożenia objętego procedurą	Ryzyko poniesienia odpowiedzialności cywilnej lub karnej z tytułu naruszenia prawa autorskiego albo negatywnych skutków pochopnego spełnienia nieuzasadnionych roszczeń (tzw. *copyright trolling*).
Sposób postępowania w przypadku wystąpienia zagrożenia	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	W zależności od okoliczności oraz skali problemu zdarzenie może zostać zgłoszone w sposób nieformalny (ustnie, telefonicznie, pocztą elektroniczną, na zamkniętym lub publicznym forum internetowym, na piśmie w postaci wezwania podpisanego przez domniemanego uprawnionego lub jego pełnomocnika) lub formalny (w postaci doręczenia odpisu pozwu lub innego pisma urzędowego, np. wezwania z policji lub prokuratury). Przyjęcie zgłoszenia dokonanego w sposób nieformalny powinno zaowocować powstaniem bardziej formalnego śladu, w postaci np. notatki służbowej, zakomunikowania przełożonemu itd., w zależności od wagi sprawy. Na wstępnym etapie należy przede wszystkim unikać wdawania się w argumentację, pochopnego przyznawania roszczeń lub spełniania żądań, piętnowania domniemanych sprawców itd. bez ustalenia wszystkich okoliczności sprawy, w razie potrzeby w konsultacji z prawnikiem. Prawo autorskie jest regulacją skomplikowaną, a sądy decydują w sprawach o naruszenie praw autorskich często w bardzo odmienny sposób, dlatego w większości przypadków uzyskanie fachowej pomocy prawnej jest wysoce wskazane.

Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Najczęstszym przypadkiem, w którym szkoła może zetknąć się z problemem naruszenia praw autorskich, jest użycie materiałów prawnie chronionych na stronach internetowych szkoły, poza zakresem dozwolonego użytku, przez jej pracowników bądź uczniów. W przypadku naruszeń dokonanych przez uczniów, szkoła nie może występować w roli sędziego – dochodzenie roszczeń należy pozostawić osobom uprawnionym. Szkoła powinna na każdym etapie skupić się na swojej roli edukacyjno-wychowawczej poprzez realizację podstawy programowej w tym zakresie oraz organizację pogadanek na temat praw autorskich, zwracając przy tym uwagę, że powinny one rzeczowo i konkretnie informować, jakie czyny są dozwolone, a jakie zabronione prawem.
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zebrać informacje przede wszystkim o: • osobie dokonującej zgłoszenia, czy jest do tego uprawniona (czy faktycznie przysługują jej prawa autorskie do danego utworu, czy posiada ważne pełnomocnictwo itd.); • wykorzystanym utworze (czy faktycznie jest chroniony przez prawo autorskie, w jakim zakresie został wykorzystany i czy zakres ten mieści się w zakresie posiadanych licencji lub dozwolonego użytku). Należy zweryfikować wszystkie informacje podawane przez zgłaszającego lub inne osoby. Jeżeli np. powołuje się on na toczące się w sprawie postępowanie karne, należy podjąć kontakt z odpowiednimi służbami w celu ustalenia, czy takie postępowanie faktycznie się toczy, czego dokładnie dotyczy i jaka jest w nim rola poszczególnych osób. Taki kontakt najlepiej przeprowadzać za pośrednictwem adwokata lub radcy prawnego. Należy sprawdzić, czy okoliczności podane w zgłoszeniu faktycznie miały miejsce i czy przedstawiane tam dowody nie zostały zmanipulowane.
Identyfikacja sprawcy(-ów)	Dochodzenie naruszeń praw autorskich realizowane jest, co do zasady, z inicjatywy samego uprawnionego przed sądami, a w przypadku naruszeń stanowiących przestępstwo dodatkowo zaangażowane mogą być policja i prokuratura. Szkoła nie powinna wyręczać tych organów w ich obowiązkach ani też wkraczać w ich kompetencje. Powinna natomiast skupić się na swojej roli wychowawczej i edukacyjnej, wykorzystując okoliczność zgłoszenia rzekomego naruszenia do przekazania zaangażowanym osobom (a być może i wszystkim uczniom, nauczycielom i opiekunom) wiedzy na temat tego, jak faktycznie prawo reguluje konkretne kwestie.

Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Zasadniczo o dochodzeniu roszczeń wobec sprawcy decyduje sam uprawniony (tzn. autor lub inna osoba, której przysługują prawa autorskie). Szkoła powinna natomiast podjąć działania o charakterze edukacyjno-wychowawczym, polegające na obszernym wyjaśnieniu, na czym polegało naruszenie, oraz przekazaniu wiedzy, jak do naruszeń nie dopuścić w przyszłości.
Działania wobec ofiar zdarzenia	Jeżeli osobą, której prawa autorskie naruszono, jest uczeń, należy rozważyć możliwość wystąpienia w roli mediatora, aby stosownie do okoliczności ułatwić stronom ugodowe lub kompromisowe zakończenie powstałego sporu. Np. w przypadku, gdy ofiarą jest osoba ze szkoły, autorytet szkoły może pomóc w skłonieniu sprawcy do zaprzestania naruszeń. Z kolei w przypadku, gdy ofiarą jest osoba spoza szkoły, szkoła może pomóc sprawcy w doprowadzeniu do zaniechania naruszeń i naprawienia ich skutków bez niepotrzebnej eskalacji sporu.
Działania wobec świadków	Stosownie do okoliczności, należy samodzielnie zebrać zeznania lub zadbać, aby zostały one zebrane przez uprawnione organy.
Współpraca z policją i sądami rodzinnymi	Ponieważ dochodzenie roszczeń z tytułu naruszeń zależy od decyzji uprawnionego, to uprawniony musi samodzielnie zdecydować, czy zawiadamiać policję lub składać powództwo. Stosownie do wskazanej wyżej roli mediatora szkoła powinna przede wszystkim zaangażować się w ułatwienie zakończenia sporu bez nadmiernej jego eskalacji.
Współpraca ze służbami społecznymi i placówkami specjalistycznym	Warto rozważyć zorganizowanie szkoleń z zakresu prawa autorskiego, w tym w internecie, dla wszystkich zainteresowanych osób w szkole[32].
Współpraca z dostawcami internetu i operatorami telekomunikacyjnymi	Zależnie od okoliczności może być wskazana asysta sprawcy bądź ofiary podczas kontaktu z tego typu podmiotami, np. w celu zablokowania dostępu do utworu umieszczonego w internecie z naruszeniem prawa. Ponadto, stosownie do przepisów prawa, tego typu usługodawcy mogą zostać zobowiązani do przekazania szczegółów dotyczących naruszenia dokonanego z użyciem ich usług (do czego jednak może być potrzebne postanowienie sądowe).

[32] Można skorzystać m.in. z materiałów edukacyjnych (scenariusze zajęć, podręczniki) dostępnych na stronach http://prawokultury.pl/, http://edukacjamedialna.edu.pl oraz http://www.legalnakultura.pl/pl. Fundacja Nowoczesna Polska prowadzi nieodpłatną pomoc w sprawach prawnoautorskich – w każdy poniedziałek w godz. 15.00–17.00 pod numerem tel. +48 739 231 233 oraz przez internet https://prawokultury.pl/pierwsza-pomoc/pytanie/ [dostęp: 28.08.2020 r.].

Rozdział III
Bezpieczeństwo techniczne sieci i sprzętu IT

1. Rodzaje zagrożeń

W dzisiejszych czasach zapewnienie bezpieczeństwa technicznego sieci i sprzętu IT w szkołach powinno być priorytetem. Szkoła/placówka oświatowa narażona jest na cały szereg niebezpieczeństw: od złośliwego oprogramowania (ang. *malware*), przez próby wyłudzenia poufnych danych, kończąc na blokadzie usług sieciowych czy wręcz włamaniu do szkolnej sieci komputerowej.

Podstawowa klasyfikacja zagrożeń technicznych dla sieci i sprzętu IT obejmuje szkodliwe oprogramowanie, w ramach którego wyróżnia się:

1. **Wirusy** – programy, których zadaniem jest przede wszystkim jak najszybsze rozprzestrzenianie się w celu opanowania jak największej liczby systemów komputerowych, a następnie zniszczenie, kradzież lub zmiana informacji użytkowników.
2. **„Konie trojańskie"** – programy, których kod realizuje zazwyczaj inne funkcje niż użytkownik zakłada, np. w programie do edycji tekstu zawarte są funkcje szpiegujące działania użytkownika na urządzeniu końcowym (np. wykradanie haseł). Najgroźniejszym przykładem konia trojańskiego jest tzw. *backdoor* (luka w zabezpieczeniach systemu).
3. **Backdoor** – wirus, który daje kontrolującej go osobie możliwość zdalnego dostępu do komputera ofiary. Backdoory instalują się, uruchamiają i działają niezauważalnie, bez wiedzy i zgody użytkownika.
4. **Robaki komputerowe** – programy, które w sposób niekontrolowany mnożą się w zasobach sieci komputerowej, a ich działanie sprowadza się do powielania swojego kodu. W momencie zapełnienia wolnego miejsca na dysku komputera mogą spowodować jego zatrzymanie.

5. **Makrowirusy** – dodają swój kod do makr skojarzonych z dokumentami, arkuszami kalkulacyjnymi i innymi plikami danych. Uruchamiają się tak jak zwykłe makra w środowisku innego programu, najczęściej któregoś z pakietu Microsoft Office.

Jak już wspomniano, szkodliwe oprogramowanie często służy do zdalnego przejęcia systemów komputerowych za sprawą wykorzystania ich słabości i podatności. Poniżej przedstawiono inne zagrożenia mające na celu zakłócenie działania lub przejęcie systemów i/lub sieci komputerowych:

1. **DoS/DDoS** – atak polegający na zakłóceniu działania systemu komputerowego poprzez wysyłanie do niego nadmiernej ilości danych.
2. **Skanowanie sieci** w celu wykrycia podatnych na zagrożenia systemów. Odbywa się poprzez skanowanie portów sieciowych i sprawdzanie odpowiedzi przychodzącej. Odpowiedź wskazuje, czy port jest wykorzystywany oraz czy skanowany system jest podatny na atak.
3. **Próby logowania się** do serwerów udostępniających usługi w internecie (np. stron www, poczty e-mail) za pomocą podsłuchanych lub odgadniętych haseł.
4. **Exploit** – program, część kodu, a nawet pewne dane wykorzystujące błąd lub podatność w aplikacji lub systemie operacyjnym. W rezultacie takiego ataku osoba atakująca zdobywa pełne uprawnienia do atakowanego systemu komputerowego lub sieci.
5. **„Taktyka wodopoju"** – polega na tym, że atakujący stara się zaatakować określoną grupę użytkowników końcowych poprzez infekowanie złośliwym oprogramowaniem stron internetowych, które odwiedzają członkowie tej grupy. Celem jest zainfekowanie komputera docelowego użytkownika i uzyskanie dostępu do jego sieci.

Często atak ułatwiają działania nieostrożnego użytkownika, który nieświadomie wykonuje zamierzone przez atakującego czynności w celu ułatwienia mu zdobycia dostępu do systemów i/lub sieci komputerowych. Zastosowanie poniższych zasad minimalizuje ryzyko wystąpienia omówionych powyżej zagrożeń.

Zasady bezpieczeństwa witryny internetowej

1. Adres, pod którym utrzymywana jest strona szkoły/placówki (tzw. domena internetowa), powinien być zarejestrowany na szkołę/placówkę. Korzystanie z domeny zarejestrowanej na pracownika czy firmę świadczącą usługi IT może łatwo doprowadzić do utraty kontroli nad nią, a w przyszłości do braku dostępu nie tylko do strony www, ale także poczty czy ważnych danych.
2. Strona internetowa powinna być utrzymywana na dedykowanym serwerze (fizycznym, wirtualnym czy w chmurze). Na tym samym serwerze nie powinny działać inne usługi – poczta, wymiana plików itp. Korzystanie z serwera, na którym znajduje się wiele stron należących do różnych instytucji, także jest niewskazane – wyjątkiem może być infrastruktura dedykowana szkołom/placówkom oświatowym.

3. Oprogramowanie odpowiedzialne za działanie strony musi być na bieżąco aktualizowane. Dotyczy to systemu operacyjnego, programu serwera, a także silnika strony i systemu zarządzania treścią.
4. Wszystkie osoby odpowiadające za utrzymanie serwera i publikowanie na nim treści muszą stosować zasady dotyczące haseł dostępowych (patrz niżej).

Zasady bezpieczeństwa sieci i urządzeń

1. Aktualizuj oprogramowanie wykorzystywane na wszystkich stacjach roboczych – systemy operacyjne, oprogramowanie biurowe i inne. Dotyczy to także urządzeń mobilnych (tabletów, smartfonów i in.).
2. Stosuj oprogramowanie antywirusowe na stacjach roboczych oraz na serwerze pocztowym.
3. Zadbaj o segmentację sieci – publicznie dostępne sieci dla uczniów i gości (np. WiFi) powinny być logicznie oddzielone od stacji roboczych, laboratoriów, zasobów nauczycieli czy administracji (kadry, dyrekcji).
4. Nie podłączaj do komputera urządzeń niewiadomego pochodzenia (w szczególności urządzeń USB, takich jak pendrive). Znalezienie urządzenia tego typu należy traktować jako incydent zagrożenia bezpieczeństwa.
5. Zapewnij oddzielne konta każdemu użytkownikowi, dbając o odpowiedni poziom uprawnień.
6. Wymuszaj blokowanie urządzenia (np. blokadę ekranu).

Ciągłość działania – wskazówki

1. Regularnie wykonuj kopie zapasowe istotnych danych. Co najmniej jedna kopia powinna być przechowywana w miejscu pozbawionym dostępu z pozostałych systemów.
   Co pewien czas testuj przywracanie danych z kopii zapasowej.
2. Zastanów się, jak będzie działać placówka, jeśli dostęp do internetu okaże się w całości lub w części niemożliwy w wyniku awarii lub ataku. Przygotuj odpowiednie procedury. Jeśli to konieczne, zadbaj o zabezpieczenie łącza usługą anty-DDoS.

Eliminowanie zagrożeń socjotechnicznych – wskazówki

1. Nie działaj w pośpiechu i pod presją – zwłaszcza jeśli ktoś w wiadomości elektronicznej prosi cię o szybką reakcję, np. kliknięcie linka lub pobranie pliku.
2. Dbaj o edukację wszystkich użytkowników sieci – uczniów, rodziców, nauczycieli i pracowników administracyjnych szkoły. Publikuj informacje o zagrożeniach, zachęcaj do odwiedzania serwisów informacyjnych (np. https://www.facebook.com/CERT.Polska, www.z3s.pl [dostęp: 29.08.2020 r.]).
3. Weryfikuj wszystkie instrukcje otrzymywane przez telefon lub e-mail, w szczególności związane z podaniem danych dostępowych czy finansowych (na przykład zmiana rachunku do przelewu). Można do tego wykorzystać numer telefonu czy e-mail opublikowany na stronie instytucji lub potwierdzony we wcześniejszych kontaktach, ale nie numer podany w weryfikowanej wiadomości!

4. Zawsze sprawdzaj wiarygodność strony, na której publikowane są informacje, instrukcje czy formularze logowania – czy w jej adresie nie ma literówek, czy są w sieci opinie na jej temat?
5. Pamiętaj, że „zielona kłódka" nie jest gwarancją bezpieczeństwa strony. Świadczy ona jedynie o tym, że przesyłane dane są szyfrowane, a nie o tym, że trafiają w bezpieczne miejsce.

Zasady dotyczące haseł

1. Nie należy używać tego samego hasła do wielu serwisów.
2. Nie wolno udostępniać haseł. Jedno hasło powinno być stosowane przez jednego użytkownika.
3. Bezpieczne hasło powinno być długie (zaleca się co najmniej 12 znaków).
4. Nie należy stosować w charakterze hasła wyrazów słownikowych, nazw własnych, ciągów liczb, sekwencji liter sąsiadujących na klawiaturze („qwerty") lub powtórzeń („aaaa"). Można wykorzystywać łączenie kilku wyrazów w jedną frazę.
5. Do zapamiętywania haseł można korzystać z menadżerów haseł (np. KeePass, LastPass).
6. Tam, gdzie to możliwe, należy stosować drugi czynnik chroniący dostęp, niezależny od hasła (kod SMS, klucz sprzętowy FIDO, aplikacja Google Authenticator lub Authy).

Zgłaszanie incydentów

1. Wyznacz osoby odpowiedzialne za przyjmowanie zgłoszeń i ich obsługę.
2. Zgłoś do CSIRT NASK osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa – https://incydent.cert.pl/osoba-kontaktowa.
3. Wyczul użytkowników, aby reagowali na podejrzane zachowania, wiadomości, zdarzenia. Powiedz im, jak zgłaszać incydenty.
4. Incydenty, które mają wpływ na usługę publiczną albo wymagają zewnętrznej koordynacji zgłaszaj do CSIRT NASK (https://incydent.cert.pl [dostęp: 28.08.2020 r.]). W pozostałych przypadkach zgłoszenie jest dobrowolne, ale warto to zrobić – możesz w ten sposób pomóc w ostrzeżeniu innych.

2. Procedury reagowania w przypadku wystąpienia incydentu zagrożenia cyberbezpieczeństwa w szkole/placówce oświatowej

Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów online	
Podstawy prawne uruchomienia procedury	*Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe,* Dz.U. 2020, poz. 910, z późn. zm. Statut szkoły, regulamin szkoły. *Kodeks karny*, Rozdział XXXIII *Przestępstwa przeciwko ochronie informacji*: art. 267 § 1–4, art. 268 § 1–3, art. 268a § 1–2, art. 269 § 1–2, art. 269a, art. 269b § 1–2 *Kodeks cywilny*: art. 415.
Rodzaj zagrożenia objętego procedurą	Kategoria technicznych zagrożeń bezpieczeństwa cyfrowego obejmuje obecnie szerokie spektrum problemów: (1) ataki przeprowadzane za pomocą szkodliwego oprogramowania, (2) ataki skierowane na zasoby teleinformatyczne szkoły przy wykorzystaniu wielu skomplikowanych technik i narzędzi informatycznych (m.in.: skanowanie sieci w celu wykrycia podatnych na zagrożenia systemów, próby logowania się do serwerów www i poczty e-mail, za pomocą podsłuchanych lub odgadniętych haseł, wykorzystywanie podatności (luk) w oprogramowaniu systemów komputerowych) i socjotechnicznych (*phishing*). Na styku z zagadnieniami technicznymi lokalizują się zagrożenia wynikające z nieprawidłowych i szkodliwych zachowań użytkowników, np. uleganie atakom socjotechnicznym, używanie w różnych serwisach tych samych, łatwych do odgadnięcia haseł, zaniechanie wykonywania aktualizacji systemu operacyjnego urządzeń, przeglądarek internetowych i innego używanego przez użytkowników oprogramowania.
Sposób postępowania w przypadku wystąpienia zagrożenia	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	W przypadku wystąpienia incydentów zagrożenia bezpieczeństwa cyfrowego pracownik szkoły zobowiązany jest do zgłoszenia go osobie odpowiedzialnej za infrastrukturę teleinformatyczną szkoły oraz dyrekcji. Kluczowe znaczenie ma zebranie i zabezpieczenie przez specjalistę dowodów w formie elektronicznej.
Opis okoliczności, analiza, zabezpieczenie dowodów	Szczegółowy opis procedur reagowania na wystąpienie w szkole różnorodnych zagrożeń bezpieczeństwa cyfrowego powinien zostać zawarty w dokumencie **„polityka bezpieczeństwa cyfrowego”** danej szkoły. W części przypadków szkoła jest w stanie poradzić sobie we własnym zakresie, w niektórych konieczne jest skorzystanie z zewnętrznego wsparcia wyspecjalizowanych firm.

Identyfikacja sprawcy(-ów)	Identyfikację sprawców ataku należy pozostawić specjalistom – informatykom. W sytuacji gdy incydent spowodował w szkole straty materialne lub wiązał się z utratą danych, należy powiadomić policję, aby podjęła działania na rzecz zidentyfikowania sprawcy.
Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Jeśli sprawcami incydentu są uczniowie danej szkoły, należy wobec nich podjąć działania wychowawcze i o zaistniałej sytuacji powiadomić ich rodziców. Jeżeli skutki ataku mają dotkliwy charakter, doprowadziły do zniszczenia mienia lub utraty istotnych danych (np. gromadzonych w dzienniku elektronicznym szkoły), należy taki przypadek zgłosić policji.
Działania wobec świadków	O incydencie należy powiadomić społeczność szkolną (uczniów, nauczycieli, rodziców) i zaprezentować podjęte działania, zarówno przywracające działanie aplikacji i sieci komputerowej w szkole, jak i wychowawczo-edukacyjne wobec dzieci.
Współpraca z policją i sądami rodzinnymi	W przypadku wystąpienia strat materialnych oraz utraty danych (szczególnie danych wrażliwych) należy zgłosić incydent policji.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	W przypadku zaawansowanych awarii (np. wywołanych przez „konie trojańskie") lub strat (np. utrata danych z dziennika elektronicznego) konieczne jest skorzystanie z zewnętrznego wsparcia eksperckiego, kontakt z serwisem twórcy oprogramowania lub zamówienie usługi w wyspecjalizowanej firmie.

3. Cyberbezpieczeństwo w Ogólnopolskiej Sieci Edukacyjnej

Zapewnienie bezpieczeństwa cyfrowego środowiska szkolnego jest jednym z priorytetów Ogólnopolskiej Sieci Edukacyjnej – OSE.

OSE to program publicznej sieci telekomunikacyjnej dającej szkołom dostęp do szybkiego, bezpłatnego i bezpiecznego internetu. Program został zaprojektowany przez Ministerstwo Cyfryzacji we współpracy z Ministerstwem Edukacji Narodowej na mocy *Ustawy o Ogólnopolskiej Sieci Edukacyjnej*[33]. Operatorem OSE jest Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, nadzorowany przez ministra cyfryzacji. Szczegółowe informacje o OSE dostępne są na stronie https://ose.gov.pl/. Z informacjami na temat tego, w jaki sposób przystąpić do OSE, można zapoznać się na stronie https://ose.gov.pl/dolacz-do-nas [dostęp: 19.08.2020 r.].

[33] *Ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej* (Dz.U. 2017, poz. 2184; 2019, poz. 1815; 2020, poz. 695).

Bezpieczeństwo cyfrowe środowiska szkolnego: uczniów, nauczycieli i innych pracowników **jest stanem nabytym – a nie danym z góry, zastanym**. Jego zapewnienie wymaga realizacji wielu powiązanych ze sobą merytorycznie działań organizacyjnych, wychowawczych, edukacyjnych i technicznych. Zarówno gwarancję w zakresie technicznego bezpieczeństwa sieci szkolnej, jak i niezbędne narzędzia cyfrowe oraz treści edukacyjne zapewnia OSE.

NASK jako operator OSE dostarcza usługi bezpieczeństwa, które mają na celu zapewnienie ochrony szerokopasmowego dostępu do internetu przed szkodliwym oprogramowaniem, monitorowanie zagrożeń i bezpieczeństwa sieciowego oraz przeciwdziałanie dostępowi do treści, które mogą stanowić zagrożenie dla prawidłowego rozwoju uczniów.

Bezpieczny Internet OSE

„Bezpieczny Internet" jest podstawową usługą dostępną w OSE. Usługa jest włączana domyślnie wraz z uruchomieniem dostępu do internetu, realizuje funkcje ochronne w zakresie blokowania niepożądanej komunikacji w sieciach telekomunikacyjnych, używana jest do odseparowania komunikacji pomiędzy różnymi sieciami telekomunikacyjnymi oraz blokowania komunikacji z serwerami o podejrzanej reputacji.

W zakresie usługi wykonywane są:

1. Kontrola ruchu na poziomie połączeń z internetem, zapewniająca separację niechcianego ruchu sieciowego w celu uniemożliwienia dostępu nieuprawnionym użytkownikom internetu do sieci OSE.
2. Separacja poszczególnych podmiotów (szkół) w sieci OSE w celu ograniczenia skutków ewentualnego złamania zabezpieczeń wewnątrz sieci któregoś z podmiotów.
3. Blokowanie części zapytań o nazwy domenowe serwerów dostępnych w internecie w oparciu o reputację poszczególnych domen – dzięki temu zapewniana jest ochrona na podstawowym poziomie przed szkodliwym oprogramowaniem oraz dostępem do treści, które mogą stanowić zagrożenie dla prawidłowego rozwoju uczniów.

Zaawansowane usługi bezpieczeństwa OSE

1. **Ochrona przed szkodliwym oprogramowaniem**

   Usługa jest włączana na wniosek dyrektora szkoły. Ma na celu zapewnienie ochrony przed szkodliwym oprogramowaniem oraz monitorowanie zagrożeń i bezpieczeństwa sieciowego, czyli takich, które mogą spowodować uszkodzenie, zablokowanie lub pogorszenie działania urządzeń, dzięki którym szkoły korzystają z internetu.

   W skład usługi wchodzą następujące funkcjonalności:

   - system zapobiegania włamaniom (ang. *intrusion prevention system – IPS*), który daje możliwość monitorowania, wykrywania i blokowania ataków w ruchu dopuszczonym przez firewalle;

- ochrona przed złośliwym oprogramowaniem (ang. *anti-malware*) – sieciowy system monitorowania, wykrywania i usuwania znanych wirusów komputerowych w określonej komunikacji sieciowej (przeglądanie stron internetowych, pobieranie plików z sieci).

Do poprawnego działania usługi konieczna jest inspekcja ruchu szyfrowanego SSL, przesyłanego w ramach komunikacji wymienianej z siecią internetową w celu wyszukiwania zagrożeń i zapobiegania im.

2. Ochrona użytkownika OSE

Również włączana jest na wniosek dyrektora szkoły. Usługa zapewnia odpowiedni dobór treści internetowych poprzez blokowanie stron www sklasyfikowanych jako nielegalne lub szkodliwe.

Systemy ochrony, na podstawie zaawansowanych algorytmów, automatycznie monitorują, wykrywają i blokują zagrożenia związane z potencjalnym dostępem do treści nielegalnych i szkodliwych dla użytkowników sieci OSE ze szkół, które zdecydowały się skorzystać z usługi bezpieczeństwa.

System bezpieczeństwa chroni przede wszystkim przed dostępem do treści nielegalnych, czyli treści, których dystrybucja jest zabroniona i podlega karze, zgodnie z przepisami *Kodeksu karnego* i ustaw właściwych. Poza nielegalnymi treściami określanymi przez przepisy system bezpieczeństwa automatycznie chroni przed treściami szkodliwymi, czyli takimi, które zawierają materiały jednoznacznie nieadresowane do młodych odbiorców oraz treściami drastycznymi, wywołującymi u odbiorców silne negatywne emocje.

Do poprawnego działania usługi konieczna jest inspekcja ruchu szyfrowanego SSL, przesyłanego w ramach komunikacji wymienianej z siecią internet, w celu wyszukiwania zagrożeń i zapobiegania im.

Korzyści dla szkół z tytułu usług bezpieczeństwa:

- spełnienie wymagań art. 27 *Ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe*, która nakłada na szkoły i placówki zapewniające dostęp do internetu obowiązek podejmowania działań zabezpieczających uczniów przed dostępem do treści, mogących stanowić zagrożenie dla ich prawidłowego rozwoju; w szczególności szkoły obowiązane są zainstalować i aktualizować oprogramowanie zabezpieczające;
- możliwość bezpłatnego korzystania z systemów bezpieczeństwa na najwyższym światowym poziomie, dotychczas dostępnych tylko dla instytucji dysponujących bardzo dużymi budżetami IT;
- możliwość znaczącego ograniczenia przez szkoły wydatków na oprogramowanie zabezpieczające dostęp szkoły do internetu;

- zlokalizowanie systemów w centrach przetwarzania danych NASK i zarządzanie nimi przez personel operatora OSE, dzięki czemu szkoły nie muszą zatrudniać wykwalifikowanej kadry IT;
- brak problemów z samodzielną instalacją i aktualizacją oprogramowania zabezpieczającego.

4. Instytucje wspierające cyberbezpieczeństwo

Ogólnopolska Sieć Edukacyjna OSE

Program publicznej sieci telekomunikacyjnej zapewniającej szkołom dostęp do szybkiego, bezpłatnego i bezpiecznego internetu. Został zaprojektowany przez Ministerstwo Cyfryzacji we współpracy z Ministerstwem Edukacji Narodowej na mocy *Ustawy o Ogólnopolskiej Sieci Edukacyjnej*. Program OSE ma na celu umożliwienia szkole szerokopasmowego dostępu do bezpiecznego internetu, podnoszenia poziomu kompetencji cyfrowych uczniów oraz wspomaganie procesu kształcenia w szkołach z wykorzystaniem zasobów dostępnych w internecie – https://ose.gov.pl/ [dostęp: 20.08.2020 r.].

Dyzurnet.pl

Zespół ekspertów Naukowej i Akademickiej Sieci Komputerowej, działający jako punkt kontaktowy do zgłaszania nielegalnych treści w internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci.

Zgodnie z *Ustawą o krajowym systemie cyberbezpieczeństwa*, NASK-PIB został wskazany jako jeden z zespołów reagowania na incydenty komputerowe, tzw. CSIRT – https://dyzurnet.pl/ [dostęp: 28.08.2020 r.].

Zespół CERT Polska

Zespół działa w strukturach NASK-PIB od 1996 roku. Kluczowym obszarem jego działalności jest obsługa incydentów zagrożenia bezpieczeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w zakresie działalności operacyjnej, jak i badawczo-wdrożeniowej. CERT Polska prowadzi analizy złośliwego oprogramowania i systemów wymiany informacji o zagrożeniach, a także rozwija i udostępnia publicznie własne narzędzia do wykrywania, monitorowania, analizy i korelacji zagrożeń. Prowadzi także działania informacyjno-edukacyjne w zakresie bezpieczeństwa teleinformatycznego, takie jak: organizacja cyklicznej konferencji SECURE czy publikowanie informacji o bezpieczeństwie na blogu cert.pl. Należy m.in. do międzynarodowego forum zrzeszającego zespoły reagujące – FIRST, a także grupy roboczej europejskich zespołów reagujących – TERENA TF-CSIRT: https://cert.pl/ [dostęp: 28.08.2020 r.].

Akademia NASK

Dział Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego realizujący działalność szkoleniową, edukacyjną i popularyzatorską Instytutu

w zakresie bezpieczeństwa internetu, a w szczególności jego najmłodszych użytkowników – dostępny na stronie: https://akademia.nask.pl/ [dostęp: 28.08.2020 r.].

Saferinternet.pl

Program, którego celem jest zwiększanie społecznej świadomości na temat zagrożeń, jakie niosą ze sobą najnowsze techniki komunikacji. Wśród podejmowanych działań priorytetem jest edukacja, zarówno dzieci, jak i rodziców, a także podnoszenie kompetencji profesjonalistów w zakresie bezpiecznego korzystania z internetu. Projekt realizowany przez Fundację Dajemy Dzieciom Siłę i Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy we współpracy z Fundacją Orange. Dostępny na stronie: https://www.saferinternet.pl/ [dostęp: 28.08.2020 r.].

„Dzień Bezpiecznego Internetu"

Projekt ma na celu inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych, zaznajomienie rodziców, nauczycieli i wychowawców z problematyką bezpieczeństwa online oraz promocję pozytywnego wykorzystywania internetu. Kluczowe działania projektu to organizacja konferencji z okazji Dnia Bezpiecznego Internetu oraz koordynacja lokalnych inicjatyw szkolnych na rzecz propagowania bezpieczeństwa w internecie. Organizatorem wydarzenia w Polsce od 2005 roku jest Polskie Centrum Programu „Safer Internet" (PCPSI), które tworzą Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy oraz Fundacja Dajemy Dzieciom Siłę – informacje na temat wydarzenia na stronie: https://www.saferinternet.pl/dbi/o-dbi.html [dostęp: 28.08.2020 r.].

Kampania „Nie zagub dziecka w sieci"

Realizowana przez Ministerstwo Cyfryzacji we współpracy z Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym, adresowana do rodziców i opiekunów. Kampania jest poświęcona bezpieczeństwu w internecie i ochronie dzieci przed cyberzagrożeniami. Informacje o kampanii: https://www.gov.pl/web/niezagubdzieckawsieci

5. Linki do stron oraz telefony do instytucji

1. Ośrodek Rozwoju Edukacji: +48 22 345 37 00, www.ore.edu.pl
2. Naukowa i Akademicka Sieć Komputerowa Państwowy Instytut Badawczy: +48 22 380 82 04, +48 22 380 82 01, www.nask.pl
3. Ogólnopolska Sieć Edukacyjna: +48 22 182 55 55, www.ose.gov.pl
4. Akademia NASK: +48 22 380 82 00, +48 22 380 82 01, www.akademia.nask.pl
5. Zespół Dyżurnet.pl: https://dyzurnet.pl/
6. CERT Polska: https://cert.pl/

Rekomendacje podsumowujące

1. **Przedstawione wytyczne** i rekomendacje dotyczące zapewnienia bezpieczeństwa w szkole i placówce są propozycją działań, jakie dyrektorzy szkół i placówek powinni podjąć w swoich środowiskach szkolnych wspólnie z nauczycielami i rodzicami dzieci. Przepisy *Ustawy Prawo oświatowe*, które zostały przedstawione w powyższej publikacji, należy traktować jako **obowiązek**.
2. Zapewnienie bezpieczeństwa cyfrowego uczniów – dzieci i młodzieży – jest obecnie równie istotne, jak zapewnienie bezpieczeństwa fizycznego i psychicznego. Często zagrożenie bezpieczeństwa ucznia ma mieszany charakter – np. rozpoczyna się od nękania podczas przerw w lekcjach, rozwijając się następnie w internecie. **Wagę tych problemów powinni sobie uświadamiać zarówno nauczyciele i dyrektorzy szkół, organy prowadzące oraz rodzice**. Tylko stała – nie incydentalna – współpraca wszystkich tych podmiotów może zminimalizować zagrożenia poruszania się dzieci w cyfrowym świecie.
3. **Bezpieczeństwo cyfrowe powinno być jednym z elementów programu wychowawczo-profilaktycznego szkoły, za którego realizację odpowiada całe grono pedagogiczne**. Należy pamiętać, że nawet jeśli w szkole wytypowano osobę odpowiedzialną za bezpieczeństwo cyfrowe, nie zwalania to z odpowiedzialności za jego zapewnienie pozostałych pracowników szkoły/placówki.
4. **Kluczowe dla zapewnienia bezpieczeństwa w szkole są działania profilaktyczne**, obejmujące całą społeczność szkolną – uczniów, ich rodziców/opiekunów oraz nauczycieli. Działania te powinny być podejmowane cyklicznie, przez cały rok szkolny.
5. **W działaniach podejmowanych przez szkołę na rzecz bezpieczeństwa uczniów ważną rolę powinni odgrywać oni sami**, dlatego do codziennej pracy warto zaangażować poszczególne jednostki i samorządy uczniowskie, np. poprzez powierzenie samorządowi organizacji wydarzeń i wyłonienia m.in. „uczniowskich liderów bezpieczeństwa cyfrowego szkoły".

6. Uczeń ma kontakt z cyfrowym światem niemal przez cały czas swojej aktywności poza szkołą: w domu, środowisku rówieśniczym, w podróży czy w miejscach publicznych. **Zapewnienie bezpieczeństwa cyfrowego jest zatem wyzwaniem zarówno dla jego rodziców, jak i dla szkoły. Szkoła powinna bardzo aktywnie inspirować rodziców do podejmowania działań kontrolnych i wychowawczych, a także zapewnić im minimalny choćby poziom wsparcia szkoleniowego na tym polu**/edukację w zakresie bezpieczeństwa online.
7. W działaniach na rzecz bezpieczeństwa szkoły **warto korzystać z dobrych praktyk wypracowanych przez inne placówki** – np. zwrócić się do szkół z regionu o prezentację ich działań lub skorzystać z materiałów opracowywanych przez organizacje pozarządowe, instytucje publiczne oraz podmioty biznesowe.
8. Bezpieczna szkoła to miejsce pracy kompetentnych nauczycieli, dlatego **kadra pedagogiczna powinna stale aktualizować i pogłębiać wiedzę na temat bezpieczeństwa w środowisku szkolnym, szczególnie w zakresie kompetencji cyfrowych**. Służyć temu ma ukończenie przez wszystkich nauczycieli szkoleń z zakresu cyberbezpieczeństwa.