3. Bezpieczeństwo cyfrowe

3.1 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 inte- raktywne 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 popraw- nego reagowania w przypadku wystąpienia zagrożeń cyberbezpieczeństwa uczniów.

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-komunika-cyjnych", 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 wszyst- kich 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 ichzakres należy wpisać w realizowany w szkole program wychowawczo-profilaktyczny.

3.2 Rekomendacje strategiczne i profilaktyczne

REKOMENDACJA STRATEGICZNA

Opracowanie, realizacja i aktualizacja szkolnych działań mających na celuzapewnienie 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-inwestycyj- nym. 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 proce- dur zgłaszania incydentów oraz podejmowania interwencji w sytuacji wystąpienia zagrożenia (określać, jak zgłaszać, do kogo, gdzie szukać pomocy itp.) 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. Internet – jego zasoby i możliwości komunikacyjne – to wielkie bogactwo, z którego ko- rzysta 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 indywidual-nych przypadków, a także ich szkolne i środowiskowe tło, aby reagować adekwatnie do po- ziomu odpowiedzialności i winy ucznia.

REKOMENDACJA PROFILAKTYCZNA

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 naucza- nia, 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 cyberbez- pieczeństwa 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 cyfro- wych (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

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 odbdbija się na skuteczności ich nauki w szkole.

Dlatego realizację Szkolnego Planu Zapewnienia Bezpieczeństwa Cyfrowego należy potraktować jako inspirację do przeprowadzenia dyskusji i opracowania szkolnego kontraktucyfrowego (w formie umowy), uzgodnionego

i zawartego między wszystkimi współ- twórcami środowiska edukacji: uczniami i ich rodzicami oraz nauczycielami i innymi

Zakazy te wpisywane są często do statutu i/lub regulaminu szkoły lub zostają objęte specjalnymi zastrzeże- niami 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

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, 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. 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 stronyinternetowej.

Strategiczny cel – zapewnienie bezpieczeństwa cyfrowego dzieci i młodzieży, a także przestrzeni szkolnej – można osiągnąć głównie poprzez wychowanie i edukację, pro- wadzone 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)

Przy założeniu zapewnienia przez infrastrukturę sieciową szkoły identyfikacji każdej osoby, każdy uczeń inny użytkownik sieci w szkole powinien mieć indywidualny login i hasło: do sieci i do WiFi.

(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" przykłada-mi ku przestrodze innych – lub listę zasad bezpiecznego i efektywnego, przynoszącego uczniom korzyści edukacyjne, korzystania z internetu.

REKOMENDACJA PROFILAKTYCZNA

Działania profilaktyczne i edukacyjne adresowane do uczniów

Wyniki badań z ostatnich lat wskazują, że niemal wszyscy nastolatkowie (96%) korzystając sieci każdego dnia. Respondenci najczęściej korzystają z internetu w domu (95,4% wska- zań). 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 .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 przewod- ników 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 interne- tu, odnoszące się do systemu wartości akceptowanego przez uczniów działania wy- chowawcze i edukacyjne adresowane do uczniów są fundamentalnym sposobem za-pewnienia 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)
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 cyfrowegow szkole zaprosić powinni samorząd uczniowski, przewodniczących klas, a także radęrodziców (szkoły). Bezpośrednim organizatorem może być np. samorząd uczniowski, którego działania adresowane do społeczności szkolnej byłyby lepiej ukierunkowanei skuteczniejsze. Na wydarzenie składać się mogą prelekcje i zajęcia praktyczne (warsztaty) w szkole, a także spotkania uświadamiające, dyskusje, happeningi, pikniki i inneformy popularyzacji tematyki cyberbezpieczeństwa (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 ufundo-wanymi 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.

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.

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 udziałuw konkursach.

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 internetowymszkoły oraz na profilach szkoły w portalach społecznościowych jako oddzielne zagadnienie. Szczególne znaczenie ma publikowanie w nich numerów telefonów, pod którymimożna zgłosić przypadki naruszenia bezpieczeństwa cyfrowego w sposób anonimowy lubjako 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 cyfrowegoczy odsyłająca do materiałów informacyjnych i edukacyjnych w sieci.

REKOMENDACJA PROFILAKTYCZNA

Przygotowanie grona pedagogicznego do prowadzenia zajęćw 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 bezpieczeństwa 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. Publikacje te obejmują zarówno raporty przedstawiające stan bezpieczeństwa polskiej części internetu, raporty z działalności zespołu Dyżurnet.pl, jak i poradniki dobrych praktyk.

REKOMENDACJA PROFILAKTYCZNA

Uświadamianie rodzicom i opiekunom prawnym uczniów znaczeniadziałań 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 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.

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 dziec i 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).
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.

REKOMENDACJA PROFILAKTYCZNA

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, zain- stalowane systemy informacyjne oraz inne oprogramowanie) należy chronić zgodnie z wytycznymi zawartymi w III rozdziale dokumentu *Bezpieczna szkoła cyfrowa. Zaleceni i rekomendacje dla samorządów – realizatorów projektów w ramach unijnej perspekty-* wybudżetowej *2014–2020.*

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 infra-struktury. Sprzyja mu także korzystanie z zewnętrznych platform edukacyjnych 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 zaszkolną 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 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.

3.3 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 reagowa-nia na występujące zagrożenia lub deficyty kompetencji, eksperci korzystali przede wszyst- kim z wartościowej publikacji *Standard bezpieczeństwa online placówek oświatowych*.

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 szkolnei środowiskowe tło, by reagować adekwatnie do poziomu odpowiedzialności i winy ucznia.

3.4. 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);
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 szczegó- łowy opis znajduje się w opracowaniu: *Standard bezpieczeństwa online placówek oświato- wych* 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 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, komen- tarzy 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 oso- bami 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

3.5 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. Należy pośród nich wyróżnić szczególnie współpracę z: (1) policją i sądami rodzinnymi, (2) służbami społecznymi i placówkami spec- jalistycznymi oraz (3) dostawcami usług internetowych oraz operatorami telekomunikacyjnymi.

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 wyciąg-nięte (np. wynikające ze statutu i/lub regulaminu szkoły lub wprowadzonego kontraktu – umowy). Sprawca powinien zostać wezwany do zaprzestania podejmowania po- dobnych 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 jestwięcej, 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 decyzjęo 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 pojedyn- czy incydent;

Szczegółowy wykaz aktów prawnych związanych z bezpieczeństwem cyfrowym szkoły, działaniami podej- mowanymi w szkole oraz wobec osób nieletnich znajduje się w II wydaniu publikacji *Standard bezpieczeństwa online placówek oświatowych z 2018 r.*, na stronach 111–117.
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, jakwiele wysiłku włożył w ukrycie swojej tożsamości itp.;
- **motywacje sprawcy** – należy sprawdzić, czy działanie sprawcy nie jest działa- niem 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 po- winni 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.

3.6 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 zdrowiai życia dzieci, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawołujące do samookaleczeń i samobójstw, korzystania z narkotyków; niebezpieczeństwo werbunku dziecii młodzieży do organizacji nielegalnych i terrorystycznych).
Telefony/kontakty alarmowekrajowe	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 lubszkodliwe 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 elek- tronicznej (pliki z treściami niedozwolonymi, zapisy rozmów w ko- munikatorach, e-maile, zrzuty ekranu), znalezione w internecie lubw komputerze dziecka. Zabezpieczenie dowodów jest zadaniem ro- dziców lub opiekunów prawnych dziecka, w czynnościach tych może wspomagać ich przedstawiciel szkoły posiadający odpowiednie kompetencje techniczne. W pierwszym przypadku (1) rozwiązanie leżypo 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 zda- rzenia ze szkoły/spoza szkoły	W przypadku udostępniania przez ucznia treści opisanych wcześniej jako szkodliwe nielegalne i niebezpieczne dla zdrowia należy prze-prowadzić 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 zawia-domienie 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 roz- mowy 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 uczestni- kami 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.
Współpracaz 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 pla-cówkami specja-listycznymi	Kontakt z treściami szkodliwymi lub niebezpiecznymi może wywołać potrzebę skorzystania przez ofiarę ze specjalistycznej opieki psychoogicznej. Decyzja o takim kontakcie i skierowaniu na terapię musi zostać podjęta w porozumieniu z rodzicami/opiekunami prawnymidziecka.

Rodzaje cyber zagrożeń

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, za- mknięcie w„bańce informacyjnej";
zagrożenia moralne, takie jak: cyberpornografia, prostytucja w sieci, sexting,
sponsoring i inne;
niebezpieczeństwa społeczno-wychowawcze dotyczące zwłaszcza postaw, za- chowań, relacji i więzi, takie jak: cyberprzemoc i agresja w sieci, hazard interne- towy, zaburzenie kontaktów interpersonalnych czy wykorzystywanie internetuprzez 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: łama- nie praw autorskich, hacking, bezprawne niszczenie informacji, sabotaż kompute- rowy, rozpowszechnianie wirusów komputerowych czy przestępstwa przeciwkowiarygodności dokumentów.

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.

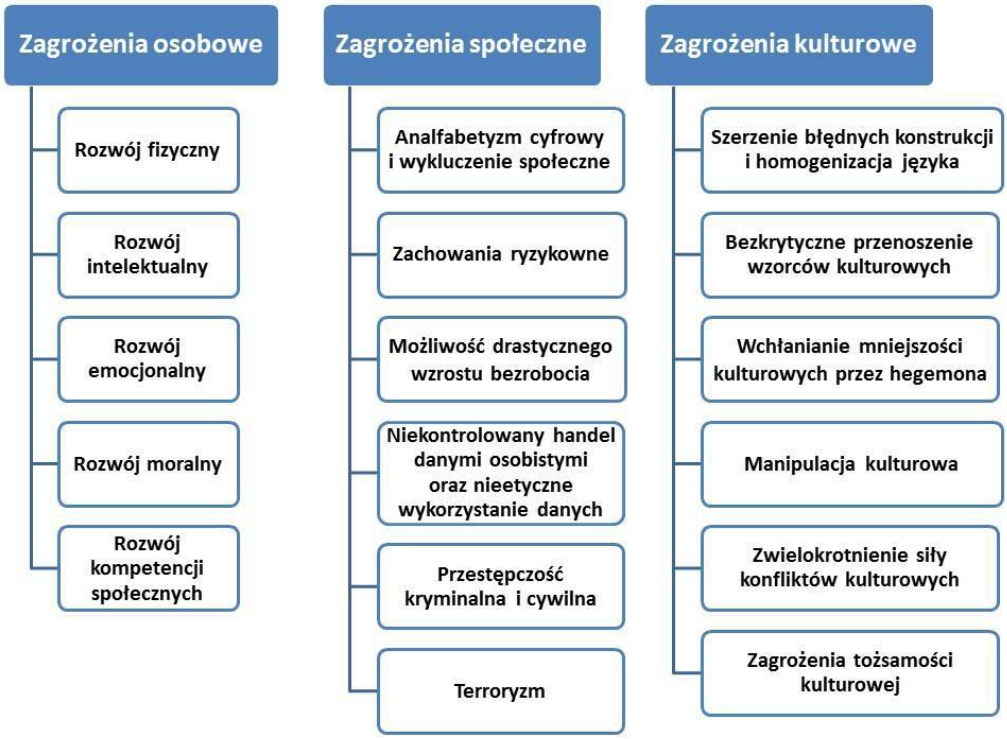
Inny podział cyberzagrożeń wyróżnia siedem podstawowych kategorii:

1. Kontakty z nieodpowiednimi treściami:
    - cyberpornografia;
    - cyberprostytucja (w tym także sexting prowadzący do osiągania korzyścimaterialnych);
    - 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 kliknięciaw link podsunięty przez przestępcę);
    - zagrożenia dla systemów mobilnych.

Natomiast do zagrożeń osobowych, społecznych i kulturowych wynikających z rozwojucyberprzestrzeni należą zjawiska wskazane na poniższym schemacie:

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.

Klasyfikacja za: Tanaś M. , Galanciak S., (2019), *Dziecko w sieci zagrożeń – ryzykowne zachowania internetowedzieci 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 bezpie-czeństwa należy ściśle wiązać z edukacją zarówno dzieci, jak i dorosłych – edukacją, umożliwiającą poznanie rozmaitych zagrożeń, ich źródeł, przejawów, skutków, sposobów radze- nia sobie w sytuacjach trudnych, a przede wszystkim sprzyjającej rozwijaniu kompetencji cyfrowych.

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 świe-tle 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 zgłoszeniai ustalenie okoliczności zdarzenia	Gdy sprawcą jest uczeń – kolega ofiary ze szkoły czy klasy – uczniowie lub rodzice powinni skontaktować się z dyrektorem szkoły, wy- chowawcą 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 skontakto- wać 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 dowo- dów potwierdzających, że sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej.

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 da- nych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dziennik Urzędowy Unii Europejskiej.

Opis okolicz- ności, 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 zostałwizerunek 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 in- ternetowych, tak aby uniemożliwić kontynuację procederu narusza- nia 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 wymagająincydenty 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 sprawcyów	W przypadku gdy dowody jasno wskazują na konkretnego sprawcę oraz potwierdzają, że sprawca zmierzał do wyrządzenia ofierze szko- dy 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 powin- no 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/sądurodzinnego. 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 incyden- tu, opinie wychowawcy i pedagoga. Dobrym rozwiązaniem jest uzyskanie interpretacji prawnej radcy prawnego.

Działania wobec ofiar zdarzenia	Nieletnią ofiarę incydentu należy otoczyć – w porozumieniu z rodzi- cami/opiekunami prawnymi – opieką psychologiczno-pedagogicz- ną (jeśli jest taka potrzeba) i powiadomić o działaniach podjętych w celu usunięcia skutków działania sprawcy (np. usunięcie z interne- tu intymnych zdjęć ofiary, zablokowanie dostępu do konta w portalu społecznościowym). Jeśli kradzież tożsamości bądź naruszenie do- brego 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 – orazodpowiedzialność 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 współ- pracy z rodzicami/opiekunami prawnymi, do placówki specjalistycz- nej, np. terapeutycznej.

3.7 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 dzie- ci. Jego negatywne efekty polegają na pogarszaniu się stanu zdrowia fizycznego (np. choroby oczu, padaczka ekranowa, choroby kręgo-słupa) i psychicznego (irytacja, rozdrażnienie, spadek sprawności psy-chofizycznej, a nawet depresja), zaniedbywaniu codziennych czynności, oraz osłabianiu relacji rodzinnych i społecznych.

Sposób postępowania w przypadku wystąpienia zagrożenia	
Przyjęcie zgłoszeniai 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 przypadka- mi 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 rówieśni- ków 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, ja- kie 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 rówie- śnikami). Celem tych ustaleń jest wybór odpowiedniej ścieżki rozwią-zywania problemu: z udziałem specjalistów (lekarzy, terapeutów) lub bezwyłącznie w szkole.

Działania wobec ofiarzdarzenia	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 zagroże- nia. Następnie, w zależności od stwierdzonego zagrożenia, proponu-je 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 inter- netu, powinno zostać profesjonalnie zdiagnozowane za zgodą rodzi- ców/opiekunów prawnych przez psychologa szkolnego lub porad- nię 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 podejmowanychdziałań wspierających dziecko.
Działania wobec świadków	Jeśli świadkami problemu są rówieśnicy dziecka, należy im w rozmowie zwrócić uwagę na negatywne aspekty nadmiernego korzystaniaz zasobów internetu oraz zaapelować o wsparcie dziecka dotkniętego problemem.

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

3.8 .Dezinformacja, bezkrytyczna wiara w treści zamieszczone w internecie, nieumiejęt- ność odróżnienia treści prawdziwych od nieprawdziwych, w tym szkodliwość reklam – proceduryreagowania

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 sięinformacjami zawartymi w reklamach. Taka postawa dzieci prowadzić może do zagrożeń życia i zdrowia (np. stosowania wyniszczającej die- ty, samookaleczeń), skutkować rozczarowaniami i porażkami życio- wymi (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 kompe- tencje pozwalające na radzenie sobie z dezinformacją i krytyczne po- dejście 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 zgłoszeniai 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 przy- padku uczniów podejmujących zachowania ryzykowne (np. samooka-leczających 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 zdarzeniaze 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 ofiarzdarzenia 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 pod- czas lekcji ukierunkowanych na zdobywanie przez dzieci i młodzież kompetencji cyfrowych. Edukacja medialna może być prowadzona również na zajęciach pozalekcyjnych. Działania mające na celu zapo- bieganie angażowaniu się młodzieży w zachowania autodestrukcyj- ne powinny być zaplanowane w ramach programu profilaktycznego szkoły oraz skierowane od ogółu uczniów (profilaktyka uniwersalna).

3.9 Cyberprzemoc procedura reagowania

	CYBERPRZEMOC
Podstawy prawne uruchomienia procedury	Kodeks Karny, Statut szkoły, Regulamin szkoły
Rodzaj zagrożenia objętego procedurą	Cyberprzemoc – przemoc z użyciem technologii informacyjnych i komunikacyjnych, głównie Internetu oraz telefonów komórkowych. Podstawowe formy zjawiska to nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów z użyciem sieci oraz podszywanie się w sieci pod kogoś wbrew jego woli. Do działań określanych mianem cyberprzemocy wykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, media społecznościowe, grupy dyskusyjne, SMS i MMS[1]
Telefony alarmowe krajowe i lokalne	Dziecięcy Telefon Zaufania 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, 810 615 005.
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Przypadek cyberprzemocy może zostać ujawniony przez ofiarę, świadka (np. innego ucznia, nauczyciela, rodzica) lub osobę bliską ofierze (np. rodzice, rodzeństwo, przyjaciele). W każdym przypadku należy ze spokojem wysłuchać osoby zgłaszającej i okazać jej wsparcie. Podziękować za zaufanie i zgłoszenie tej sprawy. ▪ Jeśli zgłaszającym jest ofiara cyberprzemocy, podejmując działania przede wszystkim należy okazać wsparcie, z zachowaniem jej podmiotowości i poszanowaniem jej uczuć. Potwierdzić, że ujawnienie przemocy jest dobrą decyzją. Taką rozmowę należy przeprowadzić w miejscu bezpiecznym, zapewniającym ofierze intymność. Nie należy podejmować kroków, które mogłyby prowadzić do powtórnej wiktymizacji czy wzbudzić podejrzenia sprawcy (np. wywoływać ucznia z lekcji do dyrekcji). ▪ Jeśli osobą zgłaszającą nie jest ofiara, na początku prosimy o opis sytuacji, także z zachowaniem podmiotowości i poszanowaniem uczuć osoby zgłaszającej (np. strach przed byciem kapusiem, obawa o własne bezpieczeństwo). W każdej sytuacji w trakcie ustalania okoliczności trzeba ustalić charakter zdarzenia (rozmiar i rangę szkody, jednorazowość/powtarzalność). Realizując procedurę należy unikać działań, które mogłyby wtórnie stygmatyzować ofiarę lub sprawcę, np.: wywoływanie uczniów z lekcji, konfrontowanie ofiary i sprawcy, niewspółmierna kara, wytykanie palcami, etc. Trzeba dokonać oceny, czy zdarzenie wyczerpuje znamiona cyberprzemocy, czy jest np. niezbyt udanym

	żartem (wtedy trzeba podjąć działania profilaktyczne mające na celu nie dopuszczenie do eskalacji tego typu zachowań w stronę cyberprzemocy).
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zabezpieczyć wszystkie dowody związane z aktem cyberprzemocy (np. zrobić kopię materiałów, zanotować datę i czas otrzymania materiałów, dane nadawcy, adresy stron www, historię połączeń, etc.). W trakcie zbierania materiałów należy 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, analizie zebranych materiałów. Ofiara często domyśla się, kto stosuje wobec niego cyberprzemoc. Jeśli ustalenie sprawcy nie jest możliwe, a w ocenie kadry pedagogicznej jest to konieczne, należy skontaktować się z Policją. Bezwzględnie należy zgłosić rozpowszechnianie nagich zdjęć osób poniżej 18 roku życia (art. 202 par. 3 KK)
Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog szkolny powinien przeprowadzić z nim rozmowę o jego zachowaniu. Rozmowa taka ma służyć ustaleniu okoliczności zdarzenia, jego wspólnej analizie (w tym np. przyjrzeniu się przyczynom), a także próbie rozwiązania sytuacji konfliktowej (w tym sposobów zadośćuczynienia ofiarom cyberprzemocy). Cyberprzemoc powinna podlegać sankcjom określonym w wewnętrznych przepisach szkoły (m. in. w statucie, kontrakcie, regulaminie). Szkoła może tu stosować konsekwencje przewidziane dla sytuacji „tradycyjnej" przemocy. Warto jednak rozszerzyć repertuar dostępnych środków, np. o czasowy zakaz korzystania ze szkolnej pracowni komputerowej w czasie wolnym i przynoszenia do szkoły akcesoriów elektronicznych (PSP, mp3) itp.
Aktywności wobec ofiar zdarzenia	W pierwszej kolejności należy udzielić wsparcia ofierze. Musi się ona czuć bezpieczna i zaopiekowana przez dorosłych. Na poczucie bezpieczeństwa dziecka wpływa fakt, że wie ono, iż szkoła podejmuje kroki w celu rozwiązania problemu. Podczas rozmowy z uczniem – ofiarą cyberprzemocy – należy zapewnić go, że nie jest winny zaistniałej sytuacji oraz że nikt nie ma prawa zachowywać się w ten sposób wobec niego, a także podkreślić, że dobrze zrobił ujawniając sytuację. Należy okazać zrozumienie dla jego uczuć, w tym trudności z ujawnieniem okoliczności wydarzenia, strachu, wstydu. Trzeba podkreślić, że szkoła nie toleruje przemocy i że zostaną podjęte odpowiednie procedury interwencyjne. Należy poinformować ucznia o krokach, jakie może podjąć szkoła i sposobach, w jaki może zapewnić mu bezpieczeństwo. Należy pomóc ofierze (rodzicom ofiary) w zabezpieczeniu dowodów (to może być dla niej zadanie trudne zarówno ze względów technicznych, jak i emocjonalnych), zerwaniu kontaktu ze sprawcą, zadbaniu o podstawowe zasady bezpieczeństwa on-line (np. nieudostępnianie swoich danych kontaktowych, kształtowanie swojego wizerunku etc). Pomoc ofierze nie może kończyć się w momencie zakończenia procedury. Warto monitorować sytuację, „czuwać" nad jej bezpieczeństwem, np. zwracać uwagę czy nie są podejmowane wobec niej dalsze działania przemocowe, obserwować, jak sobie radzi w grupie po ujawnionym incydencie cyberprzemocy. W działania wobec ofiary należy także włączyć rodziców/opiekunów ofiary – trzeba na bieżąco ich informować o sytuacji, pamiętając przy tym o podmiotowym traktowaniu dziecka – mówiąc mu o tym i starając się uzyskać jego akceptację dla udziału rodziców. Jeśli dziecko nie wyraża zgody, należy

	omówić z nim jego obawy, a jeśli to nie pomaga powołać się na obowiązujące nas zasady i przekazać informację rodzicom. W trakcie rozmowy z dzieckiem i/lub jego rodzicami/opiekunami, jeśli jest to wskazane, można zaproponować pomoc specjalisty (np. psycholog szkolny, poradnia psychologiczno-pedagogiczna) oraz przekazać informację o możliwości zgłoszenia sprawy Policji.
Aktywności wobec świadków	Należy zadbać o bezpieczeństwo świadków zdarzenia, zwłaszcza, jeśli byli oni osobami ujawniającymi cyberprzemoc. W trakcie rozmowy ze świadkami należy okazać zrozumienie i empatię dla ich uczuć – obawy przed przypięciem łatki „donosiciela", strachu przed staniem się kolejną ofiarą sprawcy itp.
Współpraca z Policją i sądami rodzinnymi	Samo wystąpienie zjawiska cyberprzemocy nie jest jednoznaczne z koniecznością zaangażowania Policji i sądu rodzinnego – procedura powinna umożliwiać rozwiązanie sytuacji problemowej na poziomie pracy wychowawczej szkoły. Szkoła powinna powiadomić odpowiednie służby (np. sąd rodzinny), gdy wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje z statutu i/lub regulaminu wobec ucznia) i interwencje pedagogiczne, a ich zastosowanie nie przynosi pożądanych rezultatów (np. nie ma zmian postawy ucznia). Kontaktu z Policją wymagają wszelkie sytuacje, w których zostało naruszone prawo (np. groźby karalne, świadome publikowanie nielegalnych treści, rozpowszechnianie nagich zdjęć z udziałem małoletnich). Za zgłoszenie powinien odpowiadać dyrektor szkoły.
Współpraca z dostawcami Internetu i operatorami telekomunikacyjnymi	Kontakt z dostawcą usługi może być wskazany w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów. Do podjęcia takiego działania stymuluje administratora serwisu art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2019 r. poz. 123).

3.10 Seksting – procedura reagowania

Seksting, prowokacyjne zachowania i aktywność seksualnajako 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 zgłoszeniai 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 znajomychdziecka. 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 sprawców	Identyfikacja sprawcy będzie możliwa przede wszystkim dzięki zabezpieczeniu dowodów – przesyłanych zdjęć czy zrzutów ekranów portali, w których opublikowano zdjęcie(-a). W niektórych przy- padkach seksting może nosić znamiona przestępstwa związanego z produkcją oraz rozpowszechnianiem materiałów pornograficznychz 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 psy- chologiczne. Konieczne są także rozmowy ze sprawcami w obecno-ści 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 materia- łów 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 ofiarzdarzenia	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 psychicznegodziecka – 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 dotklwe 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.
Współpracaze 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.

3.11 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 autorskimi prawach pokrewnych*, t.j. Dz.U. 2019, poz. 1231; 2020, poz. 288.
Rodzaj zagrożenia objętego procedurą	Bezprawne, tj. bez wymaganej prawem zgody, użycie wizerunkuosoby fizycznej w internecie.
Sposób postępowania w przypadku wystąpienia zagrożenia	
Przyjęcie zgłoszeniai 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, nietykalno- ści mieszkania, twórczości naukowej, artystycznej, wynalazczej i ra- cjonalizatorskiej. Wizerunek ma cechy prawa niezbywalnego, czylitakiego, które nie może zostać komuś sprzedane czy pożyczone. Podobnie jak inne dobra osobiste, pozostaje pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepi-sach. Ochronę wizerunku gwarantuje także prawo autorskie. Art. 81 ust. 1 zd. 1 *Ustawy o prawie autorskim i prawach pokrewnych* sta- nowi, że: *Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej*. Naruszeniem tego prawa jest bezprawne rozpowszechnianie wizerunku rozumiane jako publiczne udostęp-nianie, 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 ichzgody w myśl zasady, że skoro kolega nie pyta, czy może udostępnić moje zdjęcie, to ja również nie będę o to pytał. Problem może poja- wić się w sytuacji upublicznienia zdjęcia/filmu ukazującego kolegę lub koleżankę w sposób prześmiewczy i poniżający. Należy pamię- tać, 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 zgłoszeniai ustalenie okoliczności zdarzenia	Przepisy nie wymagają żadnej szczególnej formy. Oświadczenie woli osoby, której wizerunek ma zostać wykorzystany, może być wyrażo- ne przez każde zachowanie, które ujawni tę wolę w sposób dosta-teczny. Zgoda na publikowanie wizerunku powinna zostać wyrażona wprost. Jednocześnie osoba, która takiej zgody udziela, musi mieć pełną świadomość formy, w jakiej zostanie przedstawiony jej wize-runek, 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 zanie-chania, czyli zaprzestania tego działania, o ile jest ono bezprawne. Dodatkowo może także żądać, aby osoba, która dopuściła się naru- szenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności złożyła oświadczenie odpowiedniej treści i w odpo-wiedniej formie. Na zasadach przewidzianych w *Kodeksie cywilnym* ofiara może też żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny. Jak wie- my 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 działa- niem, może żądać zaniechania tego działania. W razie dokonanego naruszenia może także żądać, aby osoba, która dopuściła się naru- szenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności aby złożyła publiczne oświadczenie o odpowied- niej 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 odpo- wiednią 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 wła- dzą rodzicielską, został naruszony bezprawnym działaniem; • okolicznościach zdarzenia; • możliwych dowodach, np. zrzut ekranu dokumentujący bezprawe użycie wizerunku.

Identyfikacja sprawców	Dochodzenie naruszeń dóbr osobistych, w tym wizerunku, jest, co do zasady działaniem podejmowanym z inicjatywy samego uprawnio-nego przed sądami. Natomiast w przypadku naruszeń stanowiących przestępstwo dodatkowo mogą być zaangażowane organy ścigania.

Działania wobec sprawców zdarzeniaze szkoły/ spoza szkoły	Decyzja o dalszych krokach prawnych w sprawach o naruszenie dóbrosobistych, 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 pro-ponować aktywności, których celem będzie wprowadzenie uczniów w tematykę związaną z bezpiecznym i przemyślanym udostępnia- niem wizerunku w internecie, w tym przede wszystkim w mediach społecznościowych. Działania prewencyjne mogą zapobiec podobnym zdarzeniom w przyszłości.
Działania wobec ofiarzdarzenia	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 wi- zerunku 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.
Współpracaz policją i sądami rodzinnymi	Decyzja o dalszych krokach prawnych w sprawach o naruszenie dóbrosobistych, w tym wizerunku, należy do uprawnionego. Szkoła możezaangażować 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 uniknięciaprocesu sądowego.
Współpraca ze służbami społecznymi i placówkami specja- listycznymi	Informacje, szkolenia dla pracowników szkoły oraz pogadanki dla uczniów z zakresu świadomego i zgodnego z prawem użycia wize- runku innej osoby w internecie.

3.12 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 zanicjowania 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).
Telefonyalarmowe 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 zgłoszeniai ustalenie okoliczności zdarzenia	Osobami najczęściej zgłaszającymi omawiany problem są rodzice/ opiekunowie prawni dziecka lub osoby „ścigające pedofili". W pierw-szym 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 za- chowania w świecie rzeczywistym: uwiedzenie i wykorzystanie sek- sualne, kidnaping, a także wyłudzenie pieniędzy czy przedmiotów dużej wartości. W przypadku niebezpiecznych kontaktów inicjowa- nych 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 elektronicz- nej, dowody działania dorosłego sprawcy uwodzenia (zapisy roz- mów w komunikatorach czy na portalach społecznościowych, zrzutyekranowe, zdjęcia, wiadomości e-mail). Jednocześnie bezzwłocznie należy zawiadomić policję o wystąpieniu zdarzenia.

Identyfikacja sprawcy(ów0	Ze względu na bezpieczeństwo nie należy podejmować samodzielnych działań w celu dotarcia do sprawcy, lecz udzielać wszelkiegomożliwego wsparcia organom ścigania, m.in. zabezpieczyć i prze-kazać zebrane dowody. Identyfikacja sprawcy wykracza poza kom- petencje i możliwości szkoły w większości przypadków uwodzeniaprzez 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 ofiarzdarzenia	W każdym przypadku próby nawiązania niebezpiecznego kontaktu – np. w celu werbunku do sekty lub grupy promującej niebezpiecz- ne zachowania, a także rekrutacji do grupy terrorystycznej – należy przede wszystkim zapewnić ofierze opiekę psychologiczną i poczu-cie 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 możliweinformacje o sprawcy i przekazać je policji. Trzeba upewnić się, że kontakt ofiary ze sprawcą został przerwany, a dziecko odzyskało po- czucie bezpieczeństwa. Towarzyszyć temu powinna analiza sytuacji domowej (rodzinnej) dziecka, w której tkwić może źródło poszuki-wania kontaktów w internecie. Dziecku należy udzielić profesjonal- nej 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 docenićjego prospołeczną postawę.
Współpraca z policją i sądami rodzinnymi	W przypadkach naruszenia prawa – szczególnie w przypadku uwo- dzenia dziecka do lat 15 – obowiązkiem szkoły jest powiadomienie policji lub sądu rodzinnego.

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

3.13 .Łamanie prawa autorskiego – procedura reagowania

Łamanie prawa autorskiego	
Podstawy prawne uruchomienia procedury	*Ustawa o prawie autorskim i prawach pokrewnyc*h, *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 zgłoszeniai ustalenie okoliczności zdarzenia	W zależności od okoliczności oraz skali problemu zdarzenie może zostać zgłoszone w sposób nieformalny (ustnie, telefonicznie, pocztąelektroniczną, na zamkniętym lub publicznym forum internetowym, na piśmie w postaci wezwania podpisanego przez domniemane-go uprawnionego lub jego pełnomocnika) lub formalny (w postaci doręczenia odpisu pozwu lub innego pisma urzędowego, np. we- zwania z policji lub prokuratury). Przyjęcie zgłoszenia dokonanego w sposób nieformalny powinno zaowocować powstaniem bardziej formalnego śladu, w postaci np. notatki służbowej, zakomunikowa- nia 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 konsultacjiz prawnikiem. Prawo autorskie jest regulacją skomplikowaną, a sądy decydują w sprawach o naruszenie praw autorskich często w bardzoodmienny sposób, dlatego w większości przypadków uzyskanie fa-chowej pomocy prawnej jest wysoce wskazane.

Przyjęcie zgłoszeniai ustalenie okoliczności zdarzenia	Najczęstszym przypadkiem, w którym szkoła może zetknąć się z problemem naruszenia praw autorskich, jest użycie materiałów praw- nie chronionych na stronach internetowych szkoły, poza zakresem dozwolonego użytku, przez jej pracowników bądź uczniów. W przypadku naruszeń dokonanych przez uczniów, szkoła nie może wystę- pować w roli sędziego – dochodzenie roszczeń należy pozostawić osobom uprawnionym. Szkoła powinna na każdym etapie skupić się na swojej roli edukacyjno-wychowawczej poprzez realizację pod- stawy 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 pra- wo 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 zgła- szającego lub inne osoby. Jeżeli np. powołuje się on na toczące się w sprawie postępowanie karne, należy podjąć kontakt z odpowied- nimi służbami w celu ustalenia, czy takie postępowanie faktycznie się toczy, czego dokładnie dotyczy i jaka jest w nim rola poszczegól- nych 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 eduka- cyjnej, wykorzystując okoliczność zgłoszenia rzekomego naruszenia do przekazania zaangażowanym osobom (a być może i wszystkim uczniom, nauczycielom i opiekunom) wiedzy na temat tego, jak fak- tycznie 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 au- torskie). Szkoła powinna natomiast podjąć działania o charakterze edukacyjno-wychowawczym, polegające na obszernym wyjaśnieniu, na czym polegało naruszenie, oraz przekazaniu wiedzy, jak donaruszeń nie dopuścić w przyszłości.
Działania wobec ofiarzdarzenia	Jeżeli osobą, której prawa autorskie naruszono, jest uczeń, należy rozważyć możliwość wystąpienia w roli mediatora, aby stosownie do okoliczności ułatwić stronom ugodowe lub kompromisowe za- kończenie powstałego sporu. Np. w przypadku, gdy ofiarą jest oso- ba ze szkoły, autorytet szkoły może pomóc w skłonieniu sprawcy do zaprzestania naruszeń. Z kolei w przypadku, gdy ofiarą jest oso- ba 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 lubzadbać, aby zostały one zebrane przez uprawnione organy.
Współpracaz 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 wska- zanej wyżej roli mediatora szkoła powinna przede wszystkim zaan- gażować się w ułatwienie zakończenia sporu bez nadmiernej jegoeskalacji.
Współpracaze służbami społecznymi i placówkami specjalistycznym	Warto rozważyć zorganizowanie szkoleń z zakresu prawa autorskiego, w tym w internecie, dla wszystkich zainteresowanych osóbw szkole·
Współpraca z dostawcami internetu i operatorami telekomunika- cyjnymi	Zależnie od okoliczności może być wskazana asysta sprawcy bądź ofiary podczas kontaktu z tego typu podmiotami, np. w celu zablo-kowania dostępu do utworu umieszczonego w internecie z naru- szeniem prawa. Ponadto, stosownie do przepisów prawa, tego typu usługodawcy mogą zostać zobowiązani do przekazania szczegółówdotyczących naruszenia dokonanego z użyciem ich usług (do czegojednak może być potrzebne postanowienie sądowe).