**PRZEMOC W SIECI CYBERATAKI**

* **WYTYCZNE, PRZEPISY, DEFINICJE**
* **ZADANIA DYREKTORA SZKOŁY**
* **PROCEDURY POSTĘPOWANIA**

**Szkoła Podstawowa w Gładyszowie**

# CZĘŚĆ I. PRZEMOC W SIECI

**Internet i urządzenia elektroniczne stały się nieodzownym elementem życia każdego młodego człowieka. Zdecydowana większość nastolatków nie potrafi sobie wyobrazić bez nich codziennego funkcjonowania. Czując się bardzo pewnie w wirtualnej rzeczywistości, dostrzegają w nowoczesnych technologiach nie tylko korzyści ułatwiające im życie, ale także możliwości łatwego dokuczania, poniżania, obrażania innych. Zjawisko to określane jest jako przemoc w sieci. Staje się ono coraz poważniejszym problemem i zagrożeniem dla bezpieczeństwa dzieci i młodzieży. W związku z tym, że wraz z rozkwitem nowoczesnych technologii rozwija się ono dynamicznie i przybiera na sile, każda szkoła w trosce o bezpieczeństwo swoich uczniów powinna dostrzec problem, podejmować działania profilaktyczne oraz szybko interweniować w sytuacji, gdy ten problem się pojawi.**

## CYBERPRZEMOC

**Cyberprzemoc** to przemoc z użyciem urządzeń elektronicznych, najczęściej komputera i telefonów komórkowych. W przypadku dzieci i młodzieży przemoc elektroniczna, podobnie jak tradycyjna, jest działaniem wymierzonym w słabszych rówieśników, podejmowanym regularnie i z premedytacją za pośrednictwem mediów społecznościowych, poczty elektronicznej, blogów, komunikatorów internetowych i komórkowych, takich jak SMS-y czy MMS-y.

W odróżnieniu od przemocy obserwowanej w bezpośrednich relacjach rówieśniczych charakteryzuje ją:

1. wysoki poziom anonimowości sprawcy,
2. różnorodność form krzywdzenia,
3. wielokrotność działania – powtarzalny charakter,
4. szybkość rozpowszechniania materiałów kierowanych przeciwko ofierze,
5. powszechna dostępność materiałów,
6. duży zasięg materiałów – wiele osób ma do nich dostęp w krótkim czasie,
7. możliwość ataku niezależnie od miejsca i pory dnia lub nocy,
8. trwałość kompromitujących materiałów,
9. nierównowaga sił między sprawcą a ofiarą,
10. trudność zaobserwowania i kontrolowania zjawiska.

## FORMY CYBERPRZEMOCY

Przemocy za pośrednictwem Internetu lub telefonii komórkowej doświadczają młodzi ludzie, gdy ktoś:

■ ujawnia prywatne materiały bez zgody osoby, której one dotyczą;

■ rozsiewa plotki i rozpowszechnia nieprawdziwe, krzywdzące informacje, by skompromitować bądź zawstydzić określoną osobę;

■ publikuje złośliwe i obraźliwe komentarze do zdjęć i wpisów;

■ zamieszcza wulgarne, nieprzyzwoite wpisy na portalach społecznościowych;

■ robi zdjęcia i rejestruje filmy bez zgody lub wbrew woli osoby fotografowanej bądź filmowanej;

■ umieszcza ośmieszające zdjęcia i filmy w sieci lub rozsyła je przy użyciu telefonu, bez zgody osoby, której dotyczą;

■ rozsyła kompromitujące informacje, zapisy rozmów, zdjęcia lub filmy wśród znajomych albo publikuje je na stronach internetowych z zamiarem uzyskania obraźliwych komentarzy innych użytkowników;

■ podszywa się pod kogoś, by w ten sposób nastawić negatywnie otoczenie do tej osoby, świadomie manipulując przekazem;

■ zakłada fikcyjny profil w celu ośmieszenia prześladowanej osoby;

■ regularnie przesyła nieprzyjemne wiadomości, złośliwe i obraźliwe SMS-y lub e-maile do ofiary;

■ włamuje się na pocztę elektroniczną lub prywatne konto w celu rozpowszechnienia kompromitujących materiałów lub kradzieży zamieszczonych tam treści;

■ agresywnie atakuje innych użytkowników miejsc internetowych spotkań i pogawędek, zamieszcza pogardliwe, ośmieszające, wulgarne wypisy wobec innych osób prowadzących dyskusję; ■ wysyła groźby, obelgi i zniewagi za pomocą Internetu lub telefonu komórkowego, ■ wyklucza daną osobę z grupy rówieśniczej lub internetowych społeczności.

Poprzez stosowanie tych form następuje najczęściej:

1. bezprawne użycie czyjegoś wizerunku;
2. naruszenie czci i godności (niesławienia, znieważenia);
3. zastraszanie i szantażowanie;
4. nękanie, prześladowanie;
5. włamanie i podszywanie się pod kogoś.

## WYKORZYSTYWANIE CZYJEGOŚ WIZERUNKU

Dzieci i młodzież często wykorzystują telefony komórkowe do robienia zdjęć lub filmów z udziałem swoich kolegów, ale nie informują ich o zamiarze późniejszego rozpowszechniania. Wykorzystywanie czyjegoś wizerunku staje się formą cyberprzemocy, gdy **niechciane zdjęcie lub film z czyimś udziałem ktoś umieszcza w sieci bez wiedzy i zgody, a także wbrew woli danej osoby**. Ukazanie się zdjęcia lub filmu, na którym dana osoba nie akceptuje swojego wyglądu, często burzy jej wizerunek budowany przez nią z dużą uwagą i zaangażowaniem. Dla nastolatka to, jak wygląda i co inni sądzą o jego wyglądzie, odgrywa znaczącą rolę. To, jak postrzegają go rówieśnicy, ma wpływ na zdobycie uznania i sympatii kolegów oraz pozycję i prestiż w grupie rówieśniczej. Dlatego niechciane zdjęcie lub film wywołuje silne emocje związane z obawą znalezienia się poza ważną dla dziecka grupą – klasą, forum czy portalem społecznościowym.

## PRZYKŁAD

Na jednym z portali społecznościowych uczennica szkoły zamieściła zdjęcia swojej koleżanki z klasy zrobione bez jej wiedzy podczas dyskoteki szkolnej. Dziewczyna stwierdziła, że wygląda na nich okropnie i nie chce, żeby ktokolwiek je oglądał. Jest zawstydzona, obawia się komentarzy i dowcipów kolegów.

## NARUSZENIE CZCI I GODNOŚCI

Każdy człowiek zasługuje na szacunek, ma obowiązek szanować innych i ma prawo do szacunku innych osób. Naruszenia dobrego imienia bardzo często łączy się z jednoczesnym naruszeniem prawa do godności. Osoby stosujące przemoc w sieci naruszają te wartości, kiedy szkalują określoną osobę, przedstawiają ją w negatywnym świetle, podają nieprawdziwe fakty na jej temat, wykorzystują posiadane materiały, zdjęcia lub filmy do skompromitowania, poniżania, ośmieszania, upokarzania lub obrażania drugiej osoby. Działania tego rodzaju doprowadzają do tego, że osoba atakowana czuje się nie tylko poniżona w swoich oczach, ale przede wszystkim w oczach innych. Umieszczenie kompromitujących, ośmieszających treści w cyberprzestrzeni powoduje, że to upokorzenie jest dla wszystkich widoczne. Każda sytuacja ośmieszająca młodego człowieka może spowodować zmianę postrzegania go przez rówieśników, odrzucenie, wyizolowanie z grupy. Taka reakcja grupy jest bardzo dotkliwą karą i źródłem negatywnych przeżyć dla osoby dotkniętej cyberprzemocą. Konsekwencją może być zmiana nastawienia do nauki, szkoły, samego siebie. Poniżanie, ośmieszanie lub upokarzanie w sieci może odbić się na kontaktach społecznych, zdrowiu psychicznym i fizycznym, a nawet zagrażać życiu osób, które doświadczają tej formy przemocy.

## PRZYKŁAD

Na YouTubie ukazał się filmik przedstawiający dziewczynę korzystającą z toalety. Ktoś musiał zrobić go z ukrycia. Wiele osób w szkole otrzymało do niego link i po rozpoznaniu jednej z uczennic zaczęło kierować pod jej adresem obraźliwe komentarze, zniewagi, słowa powszechnie uznane za obelżywe lub wulgarne. Dziewczyna stała się pośmiewiskiem, odmawia chodzenia do szkoły, wagaruje, opuściła się w nauce. Chciałaby, żeby koledzy dali jej spokój, ale nie wie, co zrobić.

## GROŹBY, ZASTRASZANIE, SZANTAŻ

Straszenie, grożenie komuś przy użyciu narzędzi dostępnych w Internecie jest częstym zjawiskiem, choć nie zawsze nadawcy tych treści mają zamiar dokonywać tego, co zapowiadają. Często chcą jedynie dla zabawy wywołać w odbiorcy poczucie lęku. Zdarzają się również sytuacje, w których zapowiedź krzywdy jest rzeczywistym zamiarem. Młodzi ludzie straszeni lub szantażowani w sieci zawsze odczuwają niepokój i obawę, że groźba zostanie spełniona, jeśli nie zachowają się zgodnie z wolą nadawcy takiego komunikatu.

## PRZYKŁAD

Uczeń starszej klasy dokonał kradzieży telefonu komórkowego pozostawionego przez innego ucznia w szatni. Świadkiem zdarzenia był inny uczeń, który od tego zdarzenia otrzymuje SMS-y z wyzwiskami i groźbami, że jeśli komuś o tym powie, to zostanie pobity. Jego zdaniem uczeń, który dokonał kradzieży, jest do wszystkiego zdolny. Boi się, że jeśli sprawa wyjdzie na jaw, chłopak się na nim zemści.

## NĘKANIE

Nękanie jest formą cyberprzemocy wiążącą się z nachalnością i uporem nadawcy, który przez dużą liczbę i intensywność nadawanych komunikatów chce osiągnąć zamierzony cel, np. wymusić określone zachowanie, przestraszyć lub dokuczyć. Złośliwe niepokojenie jakiejś osoby za pomocą e-maili, wiadomości tekstowych zostawianych na kontach w serwisach społecznościowych, złośliwych i obraźliwych SMS-ów i komentarzy do zdjęć wywołuje u odbiorców poczucie osaczenia oraz uzasadnionego okolicznościami poczucia zagrożenia. Młodzi ludzie boją się kontaktu z osobą nękającą, ale jednocześnie nie potrafią rezygnować ze swoich aktywności w Internecie i miejsc kontaktu z przyjaciółmi i znajomymi. Blokowanie internetowych funkcji czy usuwanie własnych kont zdarza się rzadko, gdyż takie działanie równałoby się ze zniknięciem z mediów społecznościowych.

## PRZYKŁAD

Chłopak jednej z uczennic po odmowie dalszego spotykania się z nim postanowił zatruć jej życie. Wciąż wysyła do niej SMS-y i e-maile, że nie pozwoli, by spotykała się z kimś innym. Dziewczyna obawia się, że może zrobić jej coś złego lub koledze przypadkowo znajdującemu się w jej pobliżu.

## WŁAMANIA, PODSZYWANIE SIĘ POD KOGOŚ

Kradzież tożsamości jest jednym z największych zagrożeń związanych z aktywnością w sieci. Polega ona m.in. na posłużeniu się przez nieupoważnioną osobę cudzymi danymi, przybraniu cudzej tożsamości, podszywaniu się pod inną osobę. Młode osoby poświęcają dużo czasu i zaangażowania w przygotowanie swojego bloga czy konta, dlatego włamania na konta e-mailowe, profile w serwisach społecznościowych, na bloga, dokonywanie zmian w treści lub wyglądzie strony lub profilu, niszczenie ich pracy, podszywanie się pod nich w serwisach komunikacyjnych czy czatach wiąże się z bardzo dużymi emocjami.

## PRZYKŁAD

Uczennica stwierdziła, że ktoś włamał się na jej konto w serwisie społecznościowym i wszystko pozmieniał. Zniknęły wszelkie jej zdjęcia i artystyczne fotomontaże. Zamiast tego pojawiły się inne zdjęcia i wulgarne teksty o nauczycielach ze szkoły. Jest pewna, że gdy ktoś to zobaczy, to na pewno będzie miała kłopoty. Nie może się teraz zalogować i nie wie, co zrobić. Obawia się, że trudno jej będzie wytłumaczyć, że to nie ona jest autorem.

## SPRAWCY I OFIARY CYBERPRZEMOCY

Powszechna dostępność do Internetu i urządzeń mobilnych powoduje, że równie łatwo stać się ofiarą cyberprzemocy, jak i jej sprawcą.

**Sprawcy cyberprzemocy**

Sprawcami przemocy rówieśniczej w sieci są najczęściej koledzy uczniów z klasy lub znajomi ze szkoły. Zwykle w cyberprzemoc angażują się ci sami uczniowie, którzy **są też sprawcami** przemocy tradycyjnej. Używając komunikacji elektronicznej, stają się jednak bardziej aktywni w przekonaniu, że działają w ukryciu i unikną konsekwencji, jakie grożą im w przypadku osobistych kontaktów. Przekonani są o swojej bezkarności oraz nieograniczonej możliwości działania wobec osoby „niewidzialnej” w sieci. Mając poczucie, że nie są obserwowani i oceniani przez innych, „na spokojnie” preparują nieprawdziwe i złośliwe treści po to, by swoją ofiarę zdenerwować, zawstydzić, wyśmiać, upokorzyć, wykluczyć, zdyskredytować, zniszczyć reputację. Wykorzystują media elektroniczne także do prześladowania, zastraszania, nękania, wyśmiewania dręczenia, znieważania i grożenia wyrządzeniem krzywdy fizycznej. Używają wulgarnych, niekulturalnych i nieprzyzwoitych wpisów, wyrażająkontrowersyjne opinie, zamieszczają obraźliwe, bardzo dotkliwe komentarze, ośmieszają lub znieważają inne osoby przez upowszechnianie kompromitujących materiałów, np. publikowanie cudzego zdjęcia zrobionego w szatni lub toalecie. Sprawcy przemocy realizujący agresywne działania w sieci oddzielają świat rzeczywisty od wirtualnego**.** Wydaje się im, że krzywda i cierpienie osoby, którą atakują, są tylko wirtualne, bo nie widzą jej emocjonalnej reakcji i nie biorą pod uwagę, że ich ofiara ma swoje uczucia. Unikając nieprzyjemności, jakie mogłyby ich spotkać w bezpośrednich kontaktach, nie mają zahamowania, by w sieci, w poczuciu złudnej anonimowości dokonywać określonych aktów przemocy. Często nie zdają sobie również sprawy z odpowiedzialności za własne czyny i istnienia możliwości zdemaskowania sprawcy cyberprzemocy, udowodnienia mu winy i wyciągnięcia konsekwencji za niedozwoloną, sprzeczną **z prawem działalność** w Internecie.

Zwykle sprawca przemocy w sieci długo pozostaje bezkarny. U sprawców cyberprzemocy działających bez ograniczeń w dłuższym czasie:

■ utrwalają się zachowania agresywne,

■ obniża się poczucie odpowiedzialności za własne działania,

■ może nasilać się skłonność do zachowań aspołecznych w przyszłości, ■ występuje łatwe wchodzenie w konflikty z prawem.

**Ofiary cyberprzemocy**

Typowymi ofiarami elektronicznej przemocy rówieśniczej, doświadczającymi kpin i wulgarnych wpisów na portalach społecznościowych, nieprawdziwych i szkalujących informacji, a czasem nawet gróźb są młodzi ludzie z jakichś powodów nielubiani przez swych kolegów. Większość z nich doświadczała **wcześniej** zaczepek i agresji fizycznej, ale przemoc w sieci jest dla nich szczególnie dotkliwa i szkodzi o wiele mocniej niż przemoc bezpośrednia. Ofiara cyberprzemocy żyje w ciągłym napięciu psychicznym, nie ma możliwości ucieczki, nie wie, kto zobaczy upubliczniane na jej temat dane lub kiedy oprawca znowu będzie ją dręczył. Jest przekonana, że z jej sytuacją już nic się nie da zrobić, czuje **się osaczona, zdana tylko na siebie i bezsilna**.

## UWAGA

Przemoc w sieci zawsze krzywdzi emocjonalnie drugiegoczłowieka. Ofiary przemocy krzywdzeni przez swych rówieśników za pomocą Internetu i telefonii komórkowej czują się zranieni, zastraszeni, przerażeni, upokorzeni. Wstydzą się tego, co im się przytrafiło, i nie potrafią sobie poradzić z nową, trudną sytuacją. W krótkim czasie po rozpoczęciu prześladowań może pojawić się poczucie stygmatyzacji i wykluczenia społecznego.

U ofiar cyberprzemocy skutki doświadczania prześladowania objawiają się najczęściej:

1. przeżywaniem silnych, negatywnych emocji takich jak: strach, lęk, złość, gniew, frustracja;
2. oznakami zdenerwowania podczas korzystania z komputera lub telefonu;
3. poczuciem bezradności;
4. spadkiem samooceny i pewności siebie;
5. problemami ze snem i koncentrowaniem uwagi;
6. izolacją od rówieśników;
7. niechęcią chodzenie do szkoły, zaniedbywaniem obowiązków, opuszczaniem zajęć, co przekłada się w efekcie na gorsze wyniki w nauce;
8. utratą zainteresowania dla dotychczasowych hobby; 9) nastrojami depresyjnymi; 10) myślami samobójczymi.

Szybkość, z jaką rozpowszechniane są krzywdzące informacje bądź kompromitujące zdjęcia, sprawia, że ofiara cyberprzemocy ma wrażenie ciągłego, niekończącego się ataku. Niektóre z nich nie wytrzymując ciągłego napięcia, okaleczają się, albo podejmują próby samobójcze, które nierzadko kończą się tragicznie.

## UWAGA

Eksperci stwierdzają, że ryzyko samobójczych myśli i prób popełnienia samobójstwa wzrasta dwukrotnie wśród ofiar cyberprzemocy w porównaniu z nastolatkami, które takiej przemocy nie doświadczyły. Z obawy przed reakcją rodziców, np. zdenerwowaniem i zabraniem sprzętu, lub przed kompromitacją i wyśmianiem, nie informują nikogo o skierowanym na nich ataku. Brak reakcji daje sprawcom przyzwolenie na kontynuowanie działań. Ofiary przemocy po opuszczeniu szkoły nadal zmagają się z problemami psychosomatycznymi, depresją, lękiem, obniżonym poczuciem wartości. Skutki bycia ofiarą cyberprzemocy utrzymują się długo po zakończeniu prześladowania, nawet w życiu dorosłym.

## ZAPOBIEGANIE I PRZECIWDZIAŁANIE CYBERPRZEMOCY WŚRÓD DZIECI I MŁODZIEŻY

Zapewnienie dzieciom i młodzieży bezpieczeństwa w cyberprzestrzeni oraz ochrona ich przed zagrożeniami, które wynikają z ich aktywności w Internecie i posługiwania się urządzeniami służącymi do zdalnej komunikacji, jest obowiązkiem dorosłych. Szczególną rolę pełnią osoby z ich najbliższego otoczenia – rodzice i nauczyciele. Do nich należy rozpoznanie internetowej przemocy, przeciwdziałanie jej skutkom oraz podejmowanie szybkiej interwencji w sytuacji, gdy zachodzi podejrzenie, że dziecko jest ofiarą lub sprawą przemocy w sieci. Realizowanie tego zadania jest trudne, gdyż dzieci i młodzież dopuszczają się aktów cyberprzemocy w miejscach poza zasięgiem wzroku rodziców i nauczycieli. Dlatego ich wysiłki powinny koncentrować się przede wszystkim na działaniach zapobiegawczych, uprzedzających pojawienie się cyberprzemocy. Bardzo ważną rolę w przeciwdziałaniu cyberprzemocy **pełni szkoła**. Przepisy nakładają na nią **obowiązek prowadzenia edukacji medialnej i profilaktyki zachowań ryzykownych** oraz przygotowania uczniów do pełnego, świadomego i mądrego funkcjonowania w świecie multimediów i Internetu. Do podstawowych zadań szkoły w tym zakresie należy:

1. upowszechnianie wśród dzieci i młodzieży wiedzy o bezpieczeństwie oraz kształtowanie właściwych postaw wobec zagrożeń, w tym związanych z korzystaniem z technologii informacyjno-komunikacyjnych, i sytuacji nadzwyczajnych (art. 1 pkt 21 UPO);
2. kształtowanie u uczniów umiejętności sprawnego posługiwania się technologiami informacyjno-komunikacyjnymi (art. 1 pkt 22 UPO);
3. stwarzanie uczniom warunków do nabywania wiedzy i umiejętności potrzebnych do rozwiązywania problemów z wykorzystaniem metod i technik wywodzących się z informatyki, w tym logicznego i algorytmicznego myślenia, programowania, posługiwania się aplikacjami komputerowymi, wyszukiwania i wykorzystywania informacji z różnych źródeł, posługiwania się komputerem i podstawowymi urządzeniami cyfrowymi (rozporządzenie MEN w sprawie podstawy programowej);
4. przygotowywanie uczniów do dokonywania świadomych i odpowiedzialnych wyborów w trakcie korzystania z zasobów dostępnych w Internecie, krytycznej analizy informacji, bezpiecznego poruszania się w przestrzeni cyfrowej, w tym nawiązywania i utrzymywania relacji z innymi użytkownikami sieci opartych na wzajemnym szacunku, uwrażliwianie na potencjalne zagrożenia i niewchodzenie w niepewne kontakty online;
5. podejmowanie działań zabezpieczających uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju (art. 27 UPO),
6. zapewnienie bezpieczeństwa uczniom, chronienie ich przed agresją i udzielanie im pomocy, gdy jej doświadczą.

## UWAGA

Aby ograniczyć możliwość wykorzystywania telefonów komórkowych i innych urządzeń elektronicznych do działań przemocowych, szkoła powinna **jasno określić w swoim statucie warunki korzystania z nich na terenie szkoły** (art. 98 ust. 1 pkt 17 i art. 99 pkt 4 UPO). W przypadku łamania przez uczniów obowiązujących w szkole zasad i używania telefonów w innych sytuacjach niż przewiduje statut, nie jest wykluczone wprowadzenie całkowitego zakazu ich używania w szkole.

Przygotowanie uczniów do korzystania z Internetu i urządzeń służących telekomunikacji nie może ograniczyć się do spraw dotyczących posługiwania się sprzętem i jego oprogramowaniem. Szkoła powinna pokazywać uczniom, w czym pomagają nowoczesne urządzenia i jakie dają im możliwości, ale także wdrażać do takiego z nich korzystania, które przyniesie im wyłącznie korzyść i pozwoli uniknąć zagrożeń. Konieczne jest uświadamianie uczniom, że takie zagrożenia istnieją i **są** sposoby pozwalające ich unikać. Zajęcia prowadzone z uczniami powinny uwzględniać tematykę odnoszącą się do bezpieczeństwa w cyberprzestrzeni.

Zgodnie z podstawą programową kształcenia ogólnego już od I etapu edukacyjnego uczniowie powinni:

zdobywać wiedzę i umiejętności posługiwania się technologią komunikacyjną;

■ nabywać kompetencje w zakresie posługiwania się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi;

■ znać i stosować zasady bezpieczeństwa podczas korzystania z urządzeń cyfrowych;

■ posługiwać się udostępnioną im technologią zgodnie z przyjętymi zasadami i prawem;

■ rozróżniać pożądane i niepożądane zachowania innych osób korzystających z technologii;

■ oceniać zagrożenia związane z technologią i uwzględniać je dla bezpieczeństwa swojego i innych.

W szkole dla dzieci i młodzieży zadania związane z bezpiecznym poruszaniem się w uczniów cyberprzestrzeni powinny uwzględniać opracowany na podstawie wyników corocznej diagnozy program wychowawczo-profilaktyczny szkoły. Dyrektor szkoły albo upoważniony przez niego pracownik powinien przeprowadzać taką diagnozę każdego roku w zakresie występujących w środowisku szkolnym czynników ryzyka, w tym rozpoznać występujące w szkole zagrożenia i problemy związane z posługiwaniem się Internetem i innymi urządzeniami elektronicznymi oraz zaplanować odpowiednie działania wychowawcze i profilaktyczne (art. 26 UPO).

Działania wychowawcze kierowane do uczniów powinny sprzyjać rozwijaniu postaw społecznych, wskazywać wartości wynikające z budowania dobrych relacji, uczyć akceptacji i szacunku dla godności innych osób, alternatywnych zachowań i ważnych umiejętności życiowych, takich jak empatia i przyjmowania perspektywy innej osoby. Dzięki działaniom profilaktycznym uczniowie powinni nauczyć się, jak w sposób umiejętny i rozsądny korzystać z Internetu, być świadomymi odpowiedzialności za to, co robią w sieci, a także wiedzieć o istniejących ograniczeniach i zagrożeniach oraz konsekwencjach ryzykownych zachowań.

Aby skutecznie przeciwdziałać przemocy w sieci, **szkoła powinna ściśle współpracować z rodzicami**. Działania o charakterze profilaktycznym skierowane do rodziców powinny **służyć:**

1. uświadamianiu istnienia problemu cyberprzemocy i pokazania, że Internetu i komputera można **używać do wyrządzania szkody** innym;
2. przedstawieniu zagrożeń płynących z korzystania z Internetu i telefonii komórkowej;
3. rozwijaniu kompetencji do odpowiedniego nadzorowania i czuwania nad bezpiecznym korzystaniem z Internetu i telefonów komórkowych przez dzieci i młodzież;
4. zwróceniu uwagi i uwrażliwieniu na pierwsze objawy, które mogą wskazywać, że dziecko doznaje krzywdy,
5. pokazaniu sposobów służących ochronie dziecka przed agresją w sieci (kontakt z dzieckiem, zbudowanie zaufania, zapewnienie odpowiedniego wsparcia, zapewnienie pomocy specjalistów, dyskretna kontrola korzystania z Internetu zarówno co do czasu spędzanego przed komputerem, jak i treści, do jakich dziecko ma dostęp); 6) pokazaniu sposobów udzielania pomocy dziecku, gdy doświadczy cyberprzemocy; 7) wskazaniu sposobu postępowania, gdy okaże się, że dziecko jest sprawcą przemocy; 8) włączeniu rodziców uczniów w działania szkoły na rzecz zapobiegania cyberprzemocy. Młody człowiek, który będzie czuł życzliwe i kompetentne wsparcie ze strony rodziców, będzie łatwiej sygnalizował, kiedy coś go zaniepokoi w trakcie korzystania z komputera. Może uda się dzięki temu uniknąć zagrożenia.

W ramach współpracy z rodzicami szkoła powinna poinformować ich o konsekwencjach wynikających ze stosowania przemocy w sieci oraz prawach dzieci, które tej przemocy doznają. Powinni także otrzymać informację o organizacjach, które dostarczają wiedzy i udzielają wsparcia prawnego i psychologicznego osobom doświadczającym cyberprzemocy oraz wskazują, jakie środki w konkretnej sytuacji można przedsięwziąć. Rodzicom można również wskazać, że w skrajnych wypadkach niewywiązywania się ich z należytej opieki i nadzoru nad dzieckiem może mieć zastosowanie art. 105 Kodeksu wykroczeń, który stanowi, że kto przez rażące naruszenie obowiązków wynikających z władzy rodzicielskiej dopuszcza do popełnienia przez nieletniego czynu zabronionego przez ustawę jako przestępstwo lub wykroczenie i wskazującego na demoralizację nieletniego, podlega karze grzywny albo karze nagany.

## UWAGA

W związku z tym, że przemoc w sieci jest faktem, w każdej szkole zapobieganie i przeciwdziałanie cyberprzemocy powinno być jednym z istotnych zadań wychowawczych i profilaktycznych. Podejmowane przez nią działania w zakresie przeciwdziałania cyberprzemocy powinny prowadzić do **ograniczenia lub całkowitego wyeliminowania zachowań** realizowanych przy użyciu technologii komunikacyjnych w szkole i poza nią oraz zapobiegać powstawaniu tego rodzaju problemów.

Sprzyjać temu powinny:

■ dobra atmosfera w szkole i właściwe, pozytywne relacje nauczyciel-uczeń;

■ funkcjonujący w szkole czytelny system norm współżycia społecznego i jasny system konsekwencji w przypadku złamania zasad;

■ dostarczanie uczniom wiedzy i umiejętności posługiwania się technologią komunikacyjną;

■ uświadamianie całej społeczności szkolnej zagrożeń płynących z użytkowania Internetu i telefonii komórkowej, a jednocześnie uczenie zasad odpowiedzialnego i bezpiecznego korzystania z tych technologii.

Praktyka wskazuje jednak, że pomimo przekazywania uczniom odpowiednich treści zawartych w podstawie programowej, stawiania im wymagań, kierowania do uczniów działań wychowawczych oraz stosowania środków dyscyplinujących wobec sprawców angażujących się w agresywne zachowania, odpowiedzialne i etyczne postępowanie w środowisku komputerowo-sieciowym nie zawsze jest normą stosowaną przez wszystkich uczniów. Dlatego każda szkoła powinna:

1. opracować procedury reagowania w szkole na zjawisko cyberprzemocy,
2. podejmować interwencje w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy.

## UJAWNIENIE CYBERPRZEMOCY W SZKOLE – SPOSÓB POSTĘPOWANIA

Ujawnienie w szkole przypadku cyberprzemocy powinno uruchomić **opracowaną procedurę reagowania na to zjawisko**. Szkolna procedura postępowania powinna określać, jak i kiedy należy reagować wobec ofiar, sprawców i świadków przemocy oraz w jaki sposób współpracować z rodzicami uczniów doznających przemocy w sieci i będących jej sprawcami.

Wobec sprawcy cyberprzemocy proponowany jest **poniższy sposób postępowania**.

Po ujawnieniu przypadku cyberprzemocy należy:

1. ustalić okoliczności zdarzenia (rodzaj materiału, sposób jego rozpowszechniania, sprawcę i świadków zdarzenia);
2. powiadomić dyrektora lub pedagoga szkolnego o zdarzeniu;
3. zabezpieczyć dowody;
4. dokonać analizy zdarzenia przy współudziale wychowawcy, pedagoga i dyrektora.

Dalszy tok postępowania uzależniony jest od tego, **czy sprawca został zidentyfikowany, czy nie**.

|  |  |
| --- | --- |
| **W PRZYPADKU** **GDY** **TOŻSAMOŚCI** **SPRAWCY NIE** **UDAŁO SIĘ** **USTALIĆ, NALEŻY:** | **W PRZYPADKU GDY SPRAWCĄ JEST UCZEŃ SZKOŁY, NALEŻY:** |
| ■ zawiadomić administratora serwisu o konieczności usunięcia szkodliwego materiału – przerwanie aktu cyberprzemocy (art. 14 ustawy z 18 lipca 2002 r. o świadczeniu usług drogą elekltroniczną);■ powiadomić policję, w przypadku gdy zostało złamane prawo, a tożsamości sprawcy nie udało się ustalić■ Podjęcie czynności przez policję | ■ przeprowadzić rozmowę wy-jaśniającą ze sprawcą: ustalić okoliczności zajzścia, jego przyyczyny, sposób rozwiązania sytuaacji konfliktowej, omówić skutki i konsekwencje postępowania; ■ zobowiązać sprawcę do zaprzestania działania i usunięcia z sieci szkodliwych materiałów;■ określić sposób zadośćuczynienia wobec ofiary cyberprzemocy;■ wyciągnąć konsekwencje wobec sprawcy przemocy; ■ zapewnić sprawcy pomoc psychologiczno-pedagogiczną – pomóc uczniowi w zrozumieniu konsekwencji | ■ powiadomić rodziców sprawcy o przebiegu zdarzenia, zapoznać z materiałem doewodowym, de-cyzją w sprawie dalszego postęapowania i podjętych środkach wobec ich dziecka;■ pozyskać rodziaców do współó-pracy i ustalić jej zasady;■ przygotować projekt kontraktu dla dziecka; ■ podpisać kontrakt określający zobowiązania ucznia, rodziców i przedstawiciela szkoły, konsekwencje nieprzestrzegania przyjętych wymagań oraz terminy realizacji zadań zawartych w umowie | ■ powiadomić po-licję i/lub sąd rodzinny w sytuacji naruszenia prawa■ Podjęcie czynności przez policję/sąd |
| **W PRZYPADKU** **GDY** **TOŻSAMOŚCI** **SPRAWCY NIE** **UDAŁO SIĘ** **USTALIĆ, NALEŻY:** | **W PRZYPADKU GDY SPRAWCĄ JEST UCZEŃ SZKOŁY, NALEŻY:** |
|  | swojego zachowania, w zmianie postawy i postępowania, w tym sposobu korzystania z nowych technologii; ■ monitorować zachowanie ucznia,■ podjąć współpracę z sądem rodzinnym i/lub policją, jeśli uczeń popełnił czyn karalny lub przejawia zachowania świadczące o demoralizacji |  |  |

Wobec sprawcy cyberprzemocy powinny być zastosowane sankcje przewidziane w statucie szkoły. Reakcją na informację o stosowaniu przemocy może być kara stosowana w przypadku wystąpienia przemocy tradycyjnej lub kara z katalogu kar przewidzianych dla przemocy z użyciem narzędzi elektronicznych, np. ograniczenie korzystania z pracowni komputerowej po zajęciach, całkowity zakaz wnoszenia do szkoły urządzeń elektronicznych.

**Rodzaj kary**, jaka zostanie wymierzona uczniowi, powinien zależeć od:

■ rozmiaru upokorzenia, jakiego doznaje ofiara (zasięg i dostępność materiału dla wielu osób, trwałość kompromitujących materiałów);

■ czasu trwania prześladowania – czy było to długotrwałe działanie, czy pojedynczy incydent;

■ **świadomości popełnianego czynu (zaplanowanie działania z chęcią wyrządzenia krzywdy)**;

■ motywacji sprawcy (świadomej intencji skrzywdzenia drugiej osoby); ■ rodzaju rozpowszechnianego materiału.

**Zastosowanie sankcji wobec sprawcy powinno:**

■ spowodować zatrzymanie stosowania przemocy i zapewnić poczucie bezpieczeństwa poszkodowanemu uczniowi;

■ wzbudzić refleksję na temat zachowania, spowodować zrozumienie krzywdy, jaką wyrządził, i powstrzymać przed podobnym zachowaniem w przyszłości;

■ pokazać innym uczniom, że cyberprzemoc nie jest tolerowana w szkole i zawsze wywołuje skuteczną reakcję.

**UWAGA**

Sprawca musi usłyszeć wyraźny komunikat, że krzywdzenie kogoś w sieci

nie jest nieszkodliwym żartem.

**Wobec ofiary cyberprzemocy sposób postępowania jest podobny.** Po ujawnienie przypadku cyberprzemocy należy:

1. przeprowadzić rozmowę z ofiarą cyberprzemocy – udzielić jej pomocy i wsparcia emocjonalnego;
2. ujawnić okoliczności zdarzenia (rodzaj materiału, sposób rozpowszechniania, ustalenie sprawców, świadków zdarzenia);
3. zabezpieczyć dowody;
4. powiadomić dyrektora, pedagoga szkolnego;
5. przeprowadzić analizę zdarzenia i zaplanować dalsze postępowanie;
6. poinformować rodziców poszkodowanego ucznia o zdarzeniu, o działaniach szkoły, udzielić pomocy i porady, jakie działania mogą podjąć rodzice, np. powiadomić policję,

7) zapewnić pomoc psychologiczno-pedagogiczną poszkodowanemu uczniowi; 8) monitorować zachowanie ucznia.

Uczniowi, który doświadcza cyberprzemocy, należy poradzić, jak ma się zachować, aby zapewnić sobie poczucie bezpieczeństwa i nie doprowadzić do eskalacji prześladowania.

Żeby poczuł się bezpieczniejszy i mniej podatny na ataki, powinien:

■ przerwać jakikolwiek kontakt ze sprawcą, nie odpowiadać na przesyłane przez niego wiadomości;

■ nie kasować dowodów cyberprzemocy i przedstawić je osobie dorosłej;

■ zmienić swoje dane kontaktowe w komunikatorach, adres e-mail, numer telefonu komórkowego itp.;

■ zablokować sprawcę – jego adres e-mailowy, telefon, usunąć go z listy kontaktów na profilu społecznościowym, ustawić komunikator, tak aby nikt spoza listy kontaktów nie mógł się z nim porozumieć.

## UWAGA

Każde ujawnienie cyberprzemocy w szkole nie może polegać wyłącznie na działaniach interwencyjnych oraz potępianiu i rozliczaniu jej sprawców. **Równolegle z tymi działaniami powinny być realizowane zadania wychowawcze i profilaktyczne** polegające na wzmacnianiu czynników chroniących oraz zwiększeniu poczucia bezpieczeństwa w szkole.

## DOKUMENTOWANIE ZDARZENIA CYBERPRZEMOCY

Wszystkie przypadki przemocy z wykorzystaniem mediów elektronicznych powinny zostać właściwie **zbadane, zarejestrowane i udokumentowane**. Dokumentację z zajścia powinien sporządzić pedagog szkolny. Z rozmów ze sprawcą, poszkodowanym, ich rodzicami oraz świadkami zdarzenia powinny być sporządzone notatki służbowe, zawierające datę i miejsce rozmowy, dane osób biorących w niej udział i opis ustalonego przebiegu wydarzeń. Do dokumentacji pedagogicznej należy włączyć zabezpieczone dowody cyberprzemocy. Będą nimi:

■ wiadomości e-mail;

■ zdjęcia i grafiki;

■ wiadomości nagrane na pocztę głosową telefonu komórkowego;

■ komentarze do wpisów lub zdjęć w serwisach społecznościowych, na blogach, w fotogaleriach;

■ treści rozmów prowadzonych przy użyciu czatów lub komunikatorów;

■ wpisy na stronach internetowych;

■ SMS-y i MMS-y;

■ linki do stron, na których pojawiły się dotyczące sprawy treści;

■ historia połączeń w telefonie komórkowym.

Należy zanotować datę i czas otrzymanego materiału, treść wiadomości, dane nadawcy (jeśli to możliwe) lub adres strony WWW, na której pojawiły się szkodliwe treści, czy profil w serwisie społecznościowym.

## WSPÓŁPRACA SZKOŁY Z POLICJĄ I SĄDEM RODZINNYM

Większość przypadków cyberprzemocy nie wymaga powiadamiania sądu rodzinnego lub policji. Szkoła będzie jednak zobowiązana do powiadomienia organów ścigania, jeśli **ujawnione przypadki cyberprzemocy przebiegają z naruszeniem prawa –** **cyberprzemoc ma znamiona przestępstwa lub wykroczenia**. Jeśli szkoła wie o przestępstwach ściganych z urzędu, powinna niezwłocznie zawiadomić prokuratora lub policję. Każdy, dowiedziawszy się o popełnieniu przestępstwa ściganego z urzędu, ma społeczny obowiązek zawiadomić o tym te organy.

Niepodporządkowanie się temu nakazowi nie pociąga za sobą żadnych konsekwencji prawnych, ale brak reakcji wywołuje poważne konsekwencje społeczne, gdyż oznacza przyzwalanie na popełnianie tych przestępstw.

## UWAGA

Obowiązek zgłoszenia poważnych przypadków cyberprzemocy ciąży na dyrektorze szkoły (art. 304 § 1 i 2 kpk). Do czasu przybycia właściwego organu powinien on przedsięwziąć niezbędne czynności, aby nie dopuścić do zatarcia śladów i dowodów przestępstwa.

W postępowaniu w sprawach o czyny karalne w stosunku do osób, które dopuściły się takiego czynu po ukończeniu lat 13, ale nie ukończyły lat 17, stosuje się przepisy ustawy o postępowaniu w sprawach nieletnich. Zgodnie z nimi każdy, kto dowie się o popełnieniu czynu karalnego przez nieletniego, ma społeczny obowiązek zawiadomić o tym sąd rodzinny lub policję (art. 4 § 2 ustawy z 26 października 1982 r.).

Szkoła będzie zobowiązana **zg**ł**osić sprawę do sądu rodzinnego, gdy**:

1. rodzice sprawcy cyberprzemocy odmawiają współpracy ze szkołą;
2. uczeń nie zaprzestał dotychczasowego, niewłaściwego postępowania;
3. szkoła wykorzystała wszystkie dostępne środki wychowawcze, a ich zastosowanie nie przynosi pożądanych rezultatów.

W takim przypadku dyrektor szkoły powinien pisemnie powiadomić sąd opiekuńczy o zaistniałej sytuacji i zwrócić się z wnioskiem o podjęcie odpowiednich środków wynikających z ustawy o postępowaniu w sprawach nieletnich. Wobec nieletnich sąd rodzinny może m.in.:

 1) udzielić upomnienia;

1. zobowiązać do określonego postępowania, a zwłaszcza do naprawienia wyrządzonej szkody, do wykonania określonych prac lub świadczeń na rzecz pokrzywdzonego lub społeczności lokalnej, do przeproszenia pokrzywdzonego;
2. ustanowić nadzór odpowiedzialny rodziców;
3. zastosować nadzór kuratora,
4. orzec umieszczenie w młodzieżowym ośrodku wychowawczym,
5. zastosować inne środki zastrzeżone w tej ustawie do właściwości sądu rodzinnego, jak również zastosować środki przewidziane w Kodeksie rodzinnym i opiekuńczym. Sąd rodzinny może zobowiązać rodziców do ścisłej współpracy ze szkołą i do naprawienia w całości lub w części szkody wyrządzonej przez nieletniego. W wypadku gdy rodzice będą uchylać się od wykonania obowiązków nałożonych na nich, sąd ten może wymierzyć im karę pieniężną w wysokości od 50 do 1.500 złotych (art. 8 § 1 ustawy o postępowaniu w sprawach nieletnich).

Na zasadach określonych w Kodeksie karnym odpowiada ten, kto popełnia czyn zabroniony po ukończeniu 17 lat (art. 10 § 1 kk).

## OCHRONA PRAWNA PRZED CYBERPRZEMOCĄ

Młodzi ludzie często nie mają świadomości, że ich działania są nie tylko przemocą, ale również podlegają karze i mogą powodować konsekwencje prawne.

Małoletnie ofiary przemocy w Internecie można chronić przed cyberprzemocą, wykorzystując istniejące regulacje prawne. Dostępne są dwie drogi: **karna i cywilna**. Pod ochroną prawa cywilnego pozostają dobra osobiste dziecka, takie jak m.in. nazwisko lub pseudonim, wizerunek oraz cześć.

Pod ochroną prawa karnego znajdują się działania opisane w Kodeksie karnym jako przestępstwa, a wśród nich:

■ przestępstwo zniesławienia lub zniewagi zgłaszane z oskarżenia prywatnego;

■ przestępstwo włamania ścigane z urzędu;

■ przestępstwo groźby karalnej i groźby bezprawnej ścigane z urzędu.

## UWAGA

W zależności od konkretnego przypadku przemoc psychiczna może być kwalifikowana zarówno jako przestępstwo wypełniające znamiona czynu zabronionego z art. 212 k (zniesławienie) czy z art. 216 kk (znieważenie), jak i z art. 207 kk (znęcanie się), art. 190 kk (groźby karalne), art. 191 § 1 kk (groźba bezprawna w celu zmuszenia), czy wreszcie przestępstwa uporczywego nękania z art. 190a kk (stalking).

Dyrektor będzie mógł skutecznie dopełniać obowiązku zgłoszenia czynu karalnego, jeśli będzie wiedział, jakie czyny są przestępstwami i co należy zrobić, gdy jest się świadkiem zdarzenia, które może być przestępstwem.

Przewidziane prawem konsekwencje stosowania cyberprzemocy przedstawia tabela.

|  |  |  |  |
| --- | --- | --- | --- |
| **LP.** | **ZAKRES OCHRONY** | **DZIAŁANIA NARUSZAJĄCE PRAWO** | **PRZEWIDZIANE** **PRAWEM** **KONSEKWENCJE**  |
| 1. | Ochrona dóbr osobistych Kodeks cywilny – art. 23 i 24 Ochrona czci i godności (zniesławienie, znieważenie) Kodeks karny – art. 212 i art. 216.  | ■ bezprawne użycie, upu blicznianie wizerunku, imienia i nazwiska lub pseudonimu bez zgody, wiedzy lub wbrew woli ich właściciela;■ wszelkie zachowania uwłaczające czyjejś godcności, stanowiące przesjaw lekceważenia oraz pogardy;■ znieważenie drugiej osoby w Internecie lub przy użyciu innych techcnologii komunikacyjnych;■ pomówienie o postępowanie lub właściwości, które mogą poniżyć daeną osobę;■ użycie wizerunku osoby w celu jej ośmieszania, upokorzenia;■ wypowiadanie pod adresem pokrzywdzonego znieważających go wulygaryzmów lub epitetów. | Rodzice dziecka, którego dobra osobiste zostały zagrożone działaniem innej osoby, mogą w postępowaniu cywilnym żądać: ■ zaniechania działania;■ dopełnienia czynności potrzebnych do usunięcia skutków działania, w szczególności złożenia oświadczenia odpowiedniej treści i formie;■ zadośćuczynienia pienniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny. ■ Pokrzywdzony lub osoba działająca w jego imieniu może jednocześnie dochodzić swoich praw w oparciu o przepisy prawa karnego.■ Za pomówienie poniżające daną osobę za pomocą środków masowego komunikowa-nia grozi kara grzywny, ograniczenia wolności albo pozbawienia wolności do roku.  |

|  |  |  |  |
| --- | --- | --- | --- |
| **LP.** | **ZAKRES OCHRONY** | **DZIAŁANIA NARUSZAJĄCE PRAWO** | **PRZEWIDZIANE** **PRAWEM** **KONSEKWENCJE**  |
|  |  |  | ■ Za znieważenie innej osoby za pomocą środków masowego komunikowania grozi kara grzywny, ograniczenia wolności albo pozbawienia wolności do roku. **Ściganie tych przestępstw odbywa się z oskarżenia prywatnego.** |
| 2. | Ochrona przed uporczywym nękaniem, podszywanie się Kodeks karny art. 190a Kodeks wykroczeń art. 107 | ■ złośliwe niepokojenie jakiejś osoby w celu dokuczenia jej poprzez wykorzystanie Internetu;■ wielokrotne powtarzanie jakiegoś działania w Internecie skierowanego na jakąś osobę wbrew jej woli. | ■ Za uporczywe nękanie, które wzbudza u danej osoby uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność grozi kara pozbawienia wolności do lat 3.■ Tej samej karze podlega osoba, która, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej.■ Jeżeli następstwem czynu jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od roku do lat 10.Ściganie przestępstwa następuje na wniosek pokrzywdzonego. |

|  |  |  |  |
| --- | --- | --- | --- |
| **LP.** | **ZAKRES OCHRONY** | **DZIAŁANIA NARUSZAJĄCE PRAWO** | **PRZEWIDZIANE** **PRAWEM** **KONSEKWENCJE**  |
|  |  |  | Osoba, która w celu dokuczenia innej osobie złośliwie wprowadza ją w błąd lub w inny spoysób złośliwie niepokoi, podlega karze ograniczenia wolności, grzywny do 1.500 zł albo karze nagany. |
| 3. | Ochrona przed groźbą popełnienia przestępstwa lub zmuszania do określonego działania Kodeks karny art. 190 § 1 i 2 oraz § 191 § 1 | ■ grożenie popełnieniem przestępstwa (np. pozbawieniem życia);■ kierowanie gróźb w celu zmuszenia do określonego działania w taki sposób, że groźba wzbudza obawę, że zostanie spełniona. | ■ Za grożenie innej osobie popełnieniem przestępstwa, jeżeli groźba wzbudza w zagrożonym uzasadnioną obawę, że będzie spełniona, grozi kara grzywy, ograniczenia wolności albo pozbawienia wolności do lat 2. Ściganie następuje na wniosek pokrzywdzonego.■ Za stosowanie przemocy lub groźby bezprawnej w celu zmuszenia danej osoby do określonego działania, zaniechania lub znoszenia, podlega karze pozbawienia wolności do lat 3. |
| 4. | Ochrona przed podszywaniem się, bezprawnym uzyskaniem informacji niszczeniem, uszkadzaniem, usuwaniem lub zmienianiem zapisu informacji | ■ włamania do miejsca strzeżonego hasłem lub innym zabezpieczeniem; ■ wprowadzanie zmian hasła, treści czy w wyglądu strony lub profilu, dodawanie lub usuwanie zdjęć, niszczenie, uszkadzanie. | ■ Za podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub innych danych w celu wyrządzenia szkody majątkowej lub osobistej grozi kara pozbawienia wolności do lat 3. |

|  |  |  |  |
| --- | --- | --- | --- |
| **LP.** | **ZAKRES OCHRONY** | **DZIAŁANIA NARUSZAJĄCE PRAWO** | **PRZEWIDZIANE** **PRAWEM** **KONSEKWENCJE**  |
|  | Kodeks karny art. 267 § 1–4, art. 268 § 1–4, art. 268a § 1–3, art. 190a § 2 |  | ■ Za uzyskanie dostępu do informacji w sposób nieuprawniony grozi kara ograniczenia wolności albo pozbawienia wolności do lat 2. Tej samej karze podlega, kto tak uzyskaną informację ujawnia innej osobie. ■ Ściganie tych przestępstw następuje na wniosek pokrzywdzonego.■ Za niszczenie, uszkadzanie, usuwanie lub zmienianie zapisu istotnej informacji albo w inny sposób udaremnianie lub znacznie utrudnianie osobie uprawnionej zapoznanie się z nią grozi kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli czyn dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3. Ściganie przestępstwa następuje na wniosek pokrzywdzonego. |

Ponieważ skrajną konsekwencją działań może być targnięcie się ofiary na własne życie, należy wspomnieć o tym, że Kodeks karny przewiduje sankcje w postaci kary pozbawienia wolności do lat 5 dla sprawcy, który nieumyślnie spowoduje śmierć człowieka (art 155 kk). Tak trzeba byłoby kwalifikować te przypadki, gdyby młoda osoba popełniła samobójstwo na skutek traumatycznych przeżyć wywołanych skutkami udostępnienia w Internecie danych, które ktoś w sposób nieprzewidziany wykorzystał. Inaczej wyglądają konsekwencje, gdy targnięcie się na swe życie jest skutkiem cyberprzemocy. Jeśli dojdzie do takiego dramatycznego finału, sprawca podlega znacznie surowszej karze – od roku do lat 10 pozbawienia wolności (art. 190a § 3 kk). W tym przypadku na ogół nie będzie mowy o nieumyślnym spowodowaniu śmierci.

Prawo karne określa, jakie zachowania są uznawane za niepożądane i wskazuje, że osoby podejmujące takie działania będą przez wymiar sprawiedliwości ścigane i karane. Określenie w Kodeksie karnym czynów i sankcji ma mieć także charakter powstrzymujący (odstraszający) potencjalnych sprawców. Trzeba mieć jednak świadomość, że nawet najlepsze przepisy prawa karnego nie są w stanie same z siebie sprawić, że czyny takie nie będą popełniane. Nawet najlepsze przepisy prawa nie rozwiążą problemu bezpieczeństwa i nie są w stanie uchronić dzieci i młodzieży przed zagrożeniami płynącymi z cyberprzestrzeni. Ich ochroną przed cyberprzemocą powinny zająć się dorośli:

1. rodzice, którzy z mocy ustawy zobowiązani są do sprawowania pieczy nad dzieckiem (art. 92, art. 95 i art. 96 ustawy Kodeks rodzinny i opiekuńczy),
2. dyrektor szkoły zobowiązany do sprawowania opieki nad uczniami i zapewnienia im bezpiecznych warunków pobytu w szkole (art. 68 ust. 1 pkt 3 i 6 UPO, art. 7 KN oraz § 2 rozporządzenia MENiS z 31 grudnia 2002 r.),
3. nauczyciele, których obowiązkiem jest kierowanie się w swoich działaniach dydaktycznych, wychowawczych i opiekuńczych dobrem uczniów i troską o ich zdrowie oraz rzetelne realizowanie zadań związanych z powierzonym im stanowiskiem, w tym związanych z zapewnieniem bezpieczeństwa uczniom w czasie zajęć organizowanych przez szkołę (art. 5 UPO oraz art. 6 KN).

Aby dorośli mogli chronić dzieci i młodzież, sami muszą być świadomi zagrożeń, znać sposoby ich ograniczania, współdziałać ze sobą, współpracować z instytucjami działającymi na rzecz rodziny, dzieci i młodzieży oraz korzystać z pomocy tych instytucji, które czynnie i kompetentnie wspierają rodziców, nauczycieli, a także dzieci i młodzież w sprawach związanych z cyberprzemocą.

## UWAGA

Na stronie cyfrowobezpieczni.pl można znaleźć ważne numery telefonów i adresy e-mail, pod którymi dzieci, młodzież i rodzice otrzymają pomoc: ■ Dziecięcy Telefon Zaufania Rzecznika Praw Dziecka – tel. 800 12 12 12

■ Telefon Zaufania dla Dzieci i Młodzieży – tel. 116 111, strona internetowa: www.116111.pl

■ Telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa w sieci – tel.

800 100 100, strona internetowa: www.800100100.pl

■ nielegalne treści w Internecie można zgłaszać na adres e-mail: dyzurnet@dyzurnet.pl ■ strona internetowej [www.helpline.org.pl](http://www.helpline.org.pl/), adres e-mail: helpline@helpline.org.pl. Adres poczty elektronicznej jest chroniony przed robotami spamującymi.

W przeglądarce musi być włączona obsługa JavaScript, żeby go zobaczyć. ■ incydenty naruszające bezpieczeństwo w sieci: https://incydent.cert.pl

**Podstawa prawna:**

* Ustawa z 14 grudnia 2016 r. – Prawo oświatowe (tekst jedn.: Dz.U. z 2021 r. poz. 1082). • Ustawa z 26 stycznia 1982 r. – Karta Nauczyciela (tekst jedn.: Dz.U. z 2021 r. poz. 1762).
* Ustawa z 6 czerwca 1997 r. – Kodeks karny (tekst jedn.: Dz.U. z 2021 r. poz. 2345).
* Ustawa z 6 czerwca 1997 r. – Kodeks postępowania karnego (tekst jedn.: Dz.U. z 2021 r. poz. 534 ze zm.).
* Ustawa z 23 kwietnia 1964 r. – Kodeks cywilny(tekst jedn**.:** Dz.U. z 2020 r. poz. 1740 ze zm.).
* Ustawa z 26 października 1982 r. o postępowaniu w sprawach nieletnich (tekst jedn.: Dz.U. z 2018 r., poz. 969).
* Ustawa z 20 maja 1971 r. – Kodeks wykroczeń (tekst jedn.: Dz.U. z 2021 r. poz. 2008).
* Ustawa z 25 lutego 1964 r. – Kodeks rodzinny i opiekuńczy (tekst jedn.: Dz.U. z 2020 r. poz. 1359).
* Rozporządzenie Ministra Edukacji Narodowej z 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz.U. z 2017 r. poz. 356 ze zm.).
* Rozporządzenie Ministra Edukacji Narodowej i Sportu z 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (tekst jedn.: Dz.U. z 2020 r. poz. 1604).

# CZĘŚĆ II. CYBERATAKI W SZKOLE

**Agresja Rosji na Ukrainę wiąże się z coraz większą liczbą cyberataków na polskie strony internetowe. Dlatego premier zdecydował o ogłoszeniu trzeciego stopnia alarmowego dotyczącego zagrożeń w cyberprzestrzeni (CHARLIE-CRP). Potencjalne cyberataki mogą dotknąć także szkolnych stron internetowych i baz danych.**

## CYBERATAK

Cyberatak to działanie mające na celu **zmianę, zniszczenie lub kradzież danych**, ewentualnie **wykorzystanie lub uszkodzenie sieci**. Jest ono ukierunkowane na komputer lub jakikolwiek element komputerowego systemu informatycznego. Atak taki może przebiegać na różne sposoby. Najbardziej znane z nich, które mogą zaistnieć w szkole lub organie prowadzącym, są przedstawione w tabeli.

**6 rodzajów cyberataków w szkole**

|  |  |
| --- | --- |
| **Malware** | Jest to rodzaj złośliwego oprogramowania, które infekuje komputer. Jednocześnie zmienia sposób jego działania w sposób zaplanowany przez atakującego. Najczęściej niszczy dane lub szpieguje użytkownika. Złośliwe oprogramowanie może rozprzestrzeniać się z jednego urządzenia na drugie. Albo też pozostawać na swoim miejscu, wpływając tylko na urządzenie gospodarza. |
| **DoS i DDoS** | Cyberatak typu denial-of-service (DoS) prowadzi do przeciążenia zasobów systemu. Przeciążenie następuje do tego stopnia, że system nie jest w stanie odpowiadać na uzasadnione żądania usług. Z kolei cyberatak DDoS (distributed denial-of-service) również ma na celu wyczerpanie zasobów systemu. Cyberatak DDoS jest inicjowany przez ogromną liczbę zainfekowanych złośliwym oprogramowaniem maszyn kontrolowanych przez atakującego. |
| **MiTM** | Cyberataki typu man-in-the-middle umożliwiają atakującemu podsłuchiwanie danych przesyłanych tam i z powrotem między dwiema osobami, sieciami lub komputerami. Nazwa cyberataku wzięła się stąd, że atakujący znajduje się „w środku” lub pomiędzy dwiema stronami próbującymi się komunikować. W efekcie atakujący szpieguje interakcję pomiędzy nimi. |
| **Phishing** | Atakujący wysyła wiadomości (e-mail, czat), które wydają się pochodzić z zaufanych, legalnych źródeł, próbując w ten sposób wyłudzić poufne informacje od swojego celu. Innymi słowy, atakujący wysyła link, który przeniesie użytkownika na stronę internetową. Następnie zaistnieje pobranie złośliwego oprogramowania albo przekazania atakującemu informacji o ofierze. |
| **Ransomware** | System ofiary jest przetrzymywany niejako w roli zakładnika dopóty, dopóki nie zostanie zapłacony okup atakującemu. Sam cyberatak pozbawia czasowo administratora dostępu do jego danych. W przypadku niezapłacenia okupu może dojść do trwałej utraty danych. Zmanipulowana ofiara pobiera oprogramowanie szyfrujące z witryny internetowej lub z załącznika do wiadomości e-mail. Wykorzystawszy luki na poszczególnych systemach, potrafi się ono zainstalować na wielu maszynach w danej sieci. Następnie, gdy atakujący zainicjuje szyfrowanie, wystąpi ono na wszystkich zainfekowanych systemach jednocześnie. |
| **Oszustwo nigeryjskie** | Nadawca prosi o pomoc, zazwyczaj w formie wiadomości e-mail, w ułatwieniu przekazania pewnej sumy pieniędzy. W zamian nadawca oferuje prowizję ‒ dużą kwotę, czasami nawet do kilku milionów dolarów. Następnie oszuści proszą o przesłanie pieniędzy w celu pokrycia części kosztów związanych z przelewem. Jeśli pieniądze zostaną wysłane do oszustów, to oni znikają. Ewentualnie oszuści próbują zdobyć więcej pieniędzy, twierdząc, że ciągle występują problemy z przelewem. |

## SZKOLENIE PRACOWNIKÓW SZKOŁY

W przypadku takich cyberataków jak DoS czy DDoS pracownik szkoły pozostaje właściwie bezradny. Może natomiast swoim zachowaniem zapobiec pozostałym rodzajom cyberataków w szkole dzięki zdobytej wiedzy. Dlatego dyrektor szkoły powinien zadbać o to, by pracownicy zdobyli informacje pozwalające im właściwie zareagować w przypadku prób cyberataku. Szkolenia powinny być organizowane dla nowo zatrudnionych pracowników oraz okresowo powtarzane.

Warto zorganizować szkolenie ze specjalistą ds. cyberbezpieczeństwa, który wskaże, na co zwrócić uwagę np. w korzystaniu ze służbowej poczty elektronicznej. Alternatywnym rozwiązaniem jest opracowanie skryptów, ulotek uświadamiających i przypominających zasady postępowania na wypadek próby wyłudzenia danych. Dyrektor i pozostała kadra kierownicza powinni też kontrolować i przypominać pracownikom o tych zasadach.

Przede wszystkim pracowników należy edukować w zakresie:

1. oprogramowania, którego należy unikać,
2. rodzajów linków, które należy sprawdzić przed kliknięciem,
3. wiadomości e-mail i załączników, których nie należy otwierać.

Jest to bardzo istotne w aspekcie cyberataków typu malware oraz ransomware.

Z kolei w kontekście cyberataków phishingowych należy uczulić pracowników, aby dokładnie analizowali rodzaje otwieranych wiadomości e-mail i klikanych linków. Pracownicy szkoły powinni zwracać uwagę na nagłówki wiadomości i nie klikać na nic, co wygląda podejrzanie.

Duże znaczenie mają parametry „Reply-to” i „Return-path”. Powinny one wskazywać na tę samą domenę, która została wskazana w e-mailu jako domena nadawcy wiadomości. Dotyczy to także wspomnianych wyżej oszustw nigeryjskich.

## ROZWIĄZANIA TECHNICZNE

Szkoła powinna rozważyć **wprowadzenie lub zaktualizowanie środków bezpieczeństwa**. Nie obowiązuje tu żadna zamknięta lista rozwiązań. Aby dokonać właściwego wyboru, warto przeprowadzić analizę ryzyka. Pozwoli ona na wytypowanie i zastosowanie odpowiednich zabezpieczeń, adekwatnych do zagrożeń dla danej organizacji. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, administrator powinien uwzględnić ryzyko wiążące się z przetwarzaniem danych osobowych:

1. przesyłanych,
2. przechowywanych,
3. w inny sposób przetwarzanych w organizacji.

**PRZYKŁAD**

W przypadku cyberataków typu MITM sprawdza się:

■

silne szyfrowanie w punktach dostępowych,

■

korzystanie z wirtualnej sieci prywatnej (VPN).

Warto więc zarekomendować wdrożenie takich rozwiązań w szkolnej sieci.

Jedno z narzędzi jest jednak wysoce rekomendowane w kontekście cyberataków. Chodzi tu o **szyfrowanie i hasłowanie załączników z danymi osobowymi** np. w wiadomościach e-mail. Pozwala to na minimalizację ryzyka utraty danych podczas próby ich nieuprawnionego uzyskania.

Priorytetem powinno być **odpowiednie zabezpieczenie urządzeń służbowych** przed cyberatakiem w szkole. W szczególności należy regularnie uaktualniać oprogramowanie i systemy operacyjne. Jeżeli zaś pracownicy szkoły korzystają z urządzeń służbowych, wówczas zasadne jest stosowanie na nich programów antywirusowych lub rozwiązań klasy MDM.

Należy też rozważyć dokonanie klasyfikacji witryn internetowych. Na tej podstawie należy **zablokować te witryny**, które według administratora stwarzają zagrożenie podczas korzystania z nich przez pracowników w innych celach niż służbowe. Pracownicy podczas surfowania w Internecie stosunkowo łatwo mogą doznać kradzieży służbowych danych osobowych.

## PROCEDURA NA WYPADEK CYBERATAKU W SZKOLE

Dyrektor powinien polecić opracowanie dokumentacji (**procedury**) na wypadek wystąpienia zagrożeń związanych z nieuprawnionym pozyskiwaniem danych. W dokumentacji takiej należy przede wszystkim zawrzeć sposób postępowania pracowników w przypadku wystąpienia cyberataku.

**PRZYKŁAD**

Takimi witrynami są strony z grami online. Gry tego typu dają możliwość kon

-

taktu z innymi graczami o nieznanej tożsamości. To zaś rodzi ryzyko np. udo

-

stępnienia hasła.

**PRZYKŁAD**

Procedura powinna regulować sposób komunikowania np. podejrzanych e-maili.

Pracownik powinien niezwłocznie zgłaszać takie e-maile do bezpośredniego

przełożonego i szkolnego inspektora ochrony danych.

Warto też rozważyć blokadę pobierania bez kontroli plików, zwłaszcza darmowych. Często pobranie darmowego programu wiąże się z podaniem danych osobowych. Te zaś mogłyby być wykorzystane w sposób nieuprawniony.

**Podstawa prawna:**

• Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.Urz. UE.L nr 119, str. 1) – art. 24, art. 32.

Szkoła Podstawowa w Gładyszowie