



BEZPIECZNY INTERNET – ŚWIADOMOŚĆ DZIECI I MŁODZIEŻY

ADRIANA CIUPKA

PLAN WARSZTATÓW

- Najnowsze wyniki badań – świadomość uczniów
- Słownik zachowań agresywnych w cyberprzestrzeni
- Procedury postępowania, obowiązki szkoły
- Standard bezpieczeństwa online
- Dobre praktyki

Cyberprzemoc

Najnowsze wyniki badań – świadomość uczniów

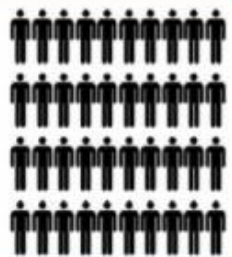
- Ryzykowane zachowania w sieci – badania z ostatnich 10 lat (prof. dr. hab. Jacka Pyżalskiego)
- Nik o cyberprzemocy –wyniki badań w szkołach, wrzesień 2017

Co było kontrolowane przez NIK?

- Czy szkoły identyfikują problem cyberprzemocy?
- Czy prawidłowo prowadzona jest działalność profilaktyczna i edukacyjna?
- Czy działalność właściwych instytucji i służb w celu zapobiegania i przeciwdziałania cyberprzemocy wśród dzieci i młodzieży jest skutecznie realizowana?

JAK WYGLĄDA ZJAWISKO CYBERPRZEMOCY WŚRÓD ANKIETOWANYCH?

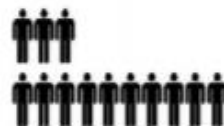
40% uczniów
zetrknęło się
ze zjawiskiem
cyberprzemocy



49% uczniów
nie zwróciłoby się
o pomoc



13% dzieci
zwróciłoby się
o pomoc
do nauczyciela



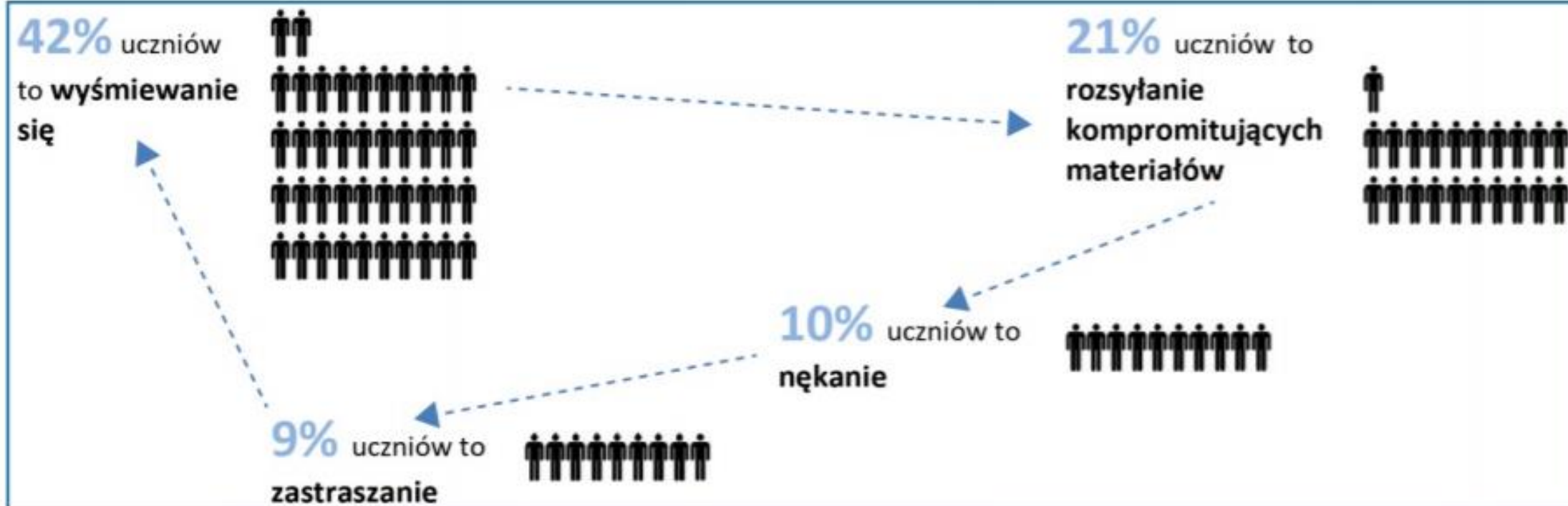
19% dzieci
zwróciłoby się
o pomoc
do rodziców



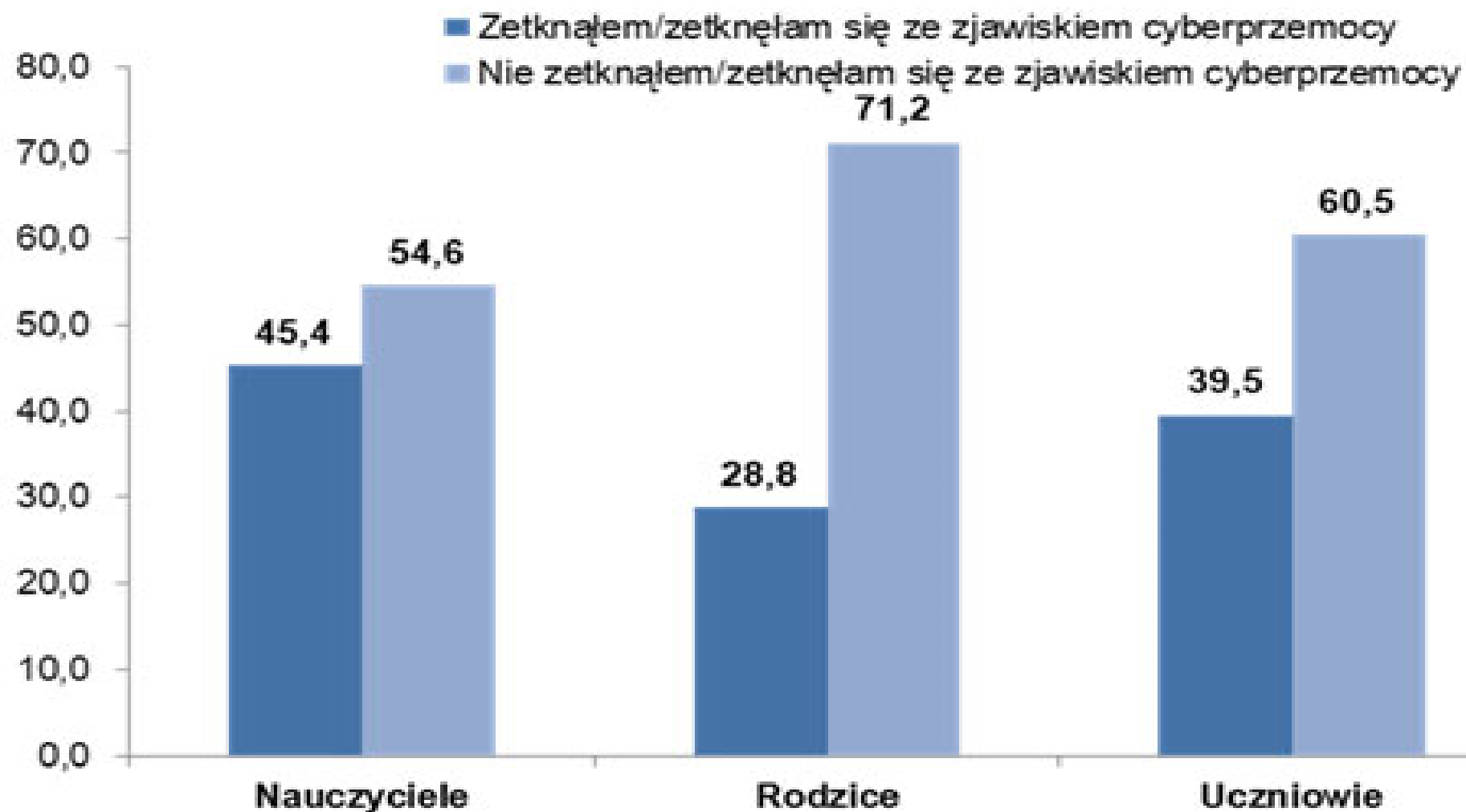
43% nauczycieli uważa,
że w szkole, w której uczą występuje
zjawisko cyberprzemocy wśród dzieci
i młodzieży



Najczęściej stosowana forma cyberprzemocy wg



Skala zjawiska cyberprzemocy wśród dzieci i młodzieży w opinii ankietowanych



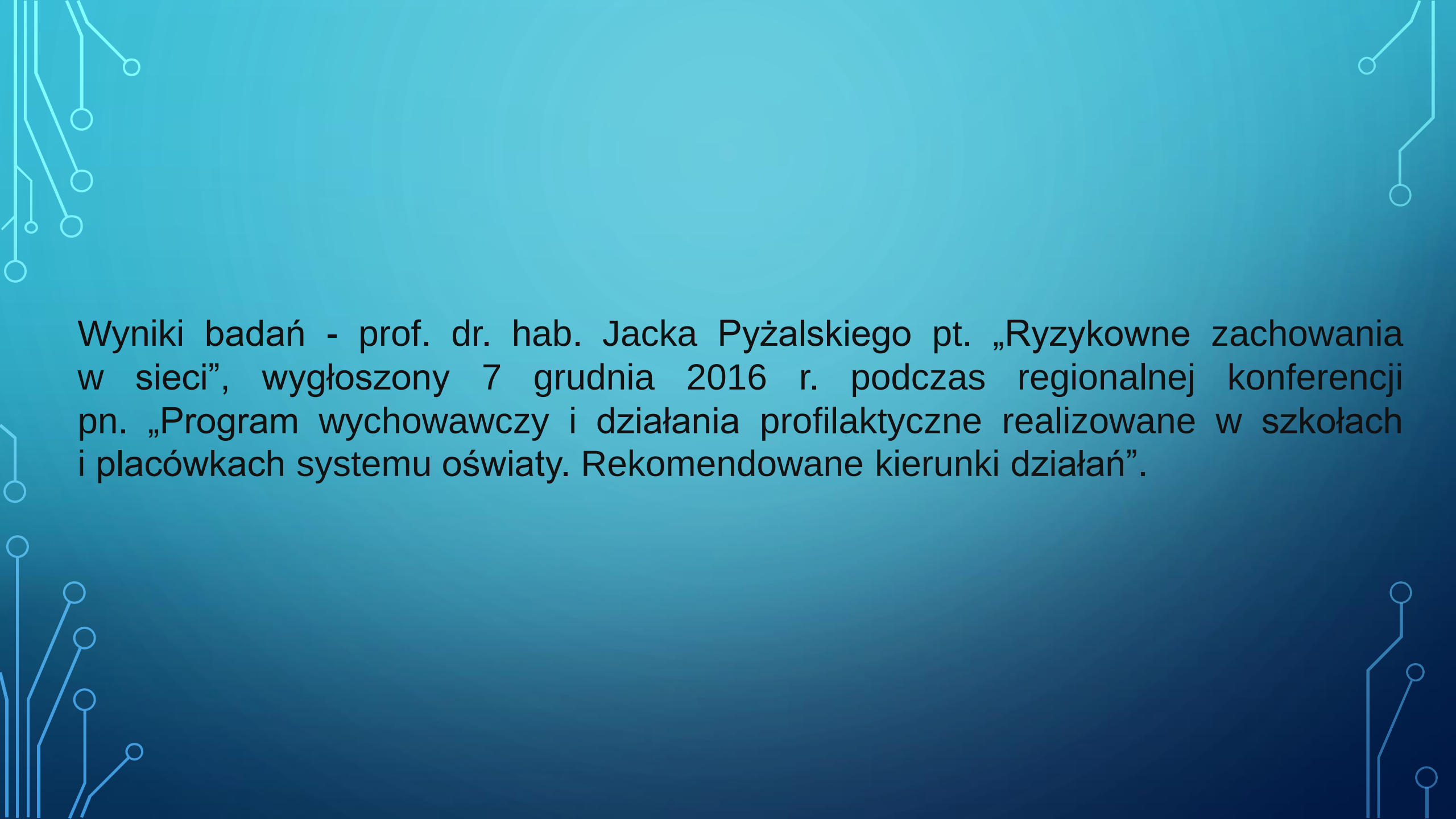
Źródło: Opracowanie własne NIK

Stwierdzony stan – stwierdzone akty cyberprzemocy

- w dziesięciu objętych kontrolą szkołach w latach szkolnych 2013/2014-2016/2017 ujawniono łącznie 60 aktów cyberprzemocy wśród dzieci i młodzieży (średnio dwa akty cyberprzemocy ujawnione przez szkołę w roku szkolnym)
- kontrola wykazała, że ofiarom zgłoszonej cyberprzemocy udzielono właściwego wsparcia, a w stosunku do sprawców cyberprzemocy zastosowano właściwe, zgodne z procedurami konsekwencje

Stwierdzony – stan szkoły

- We wszystkich objętych kontrolą szkołach realizowana była działalność profilaktyczna dotycząca cyberprzemocy w ramach przyjętych programów profilaktyki i programów wychowawczych,
- Działania profilaktyczne zostały ukierunkowane na przekazanie ogólnych informacji dotyczących tego zagadnienia uczniom i były prowadzone głównie w ramach godzin wychowawczych
- Planowane działania profilaktyczne nie obejmowały rodziców uczniów oraz zatrudnionych nauczycieli oraz realizacji zadań przy współudziale funkcjonariuszy Policji
- w 70% skontrolowanych szkół obowiązywały w całym okresie objętym kontrolą procedury dotyczące przeciwdziałaniu cyberprzemocy

The background is a solid blue gradient. In the corners, there are decorative white line art elements resembling electronic circuit boards or neural network connections. These elements consist of thin lines that branch out and terminate in small circles, creating a symmetrical, abstract pattern in each corner.

Wyniki badań - prof. dr. hab. Jacka Pyżalskiego pt. „Ryzykowne zachowania w sieci”, wygłoszony 7 grudnia 2016 r. podczas regionalnej konferencji pn. „Program wychowawczy i działania profilaktyczne realizowane w szkołach i placówkach systemu oświaty. Rekomendowane kierunki działań”.

Najnowsze wyniki badań – świadomość uczniów



Nękanie w Internecie powinno być zabronione?

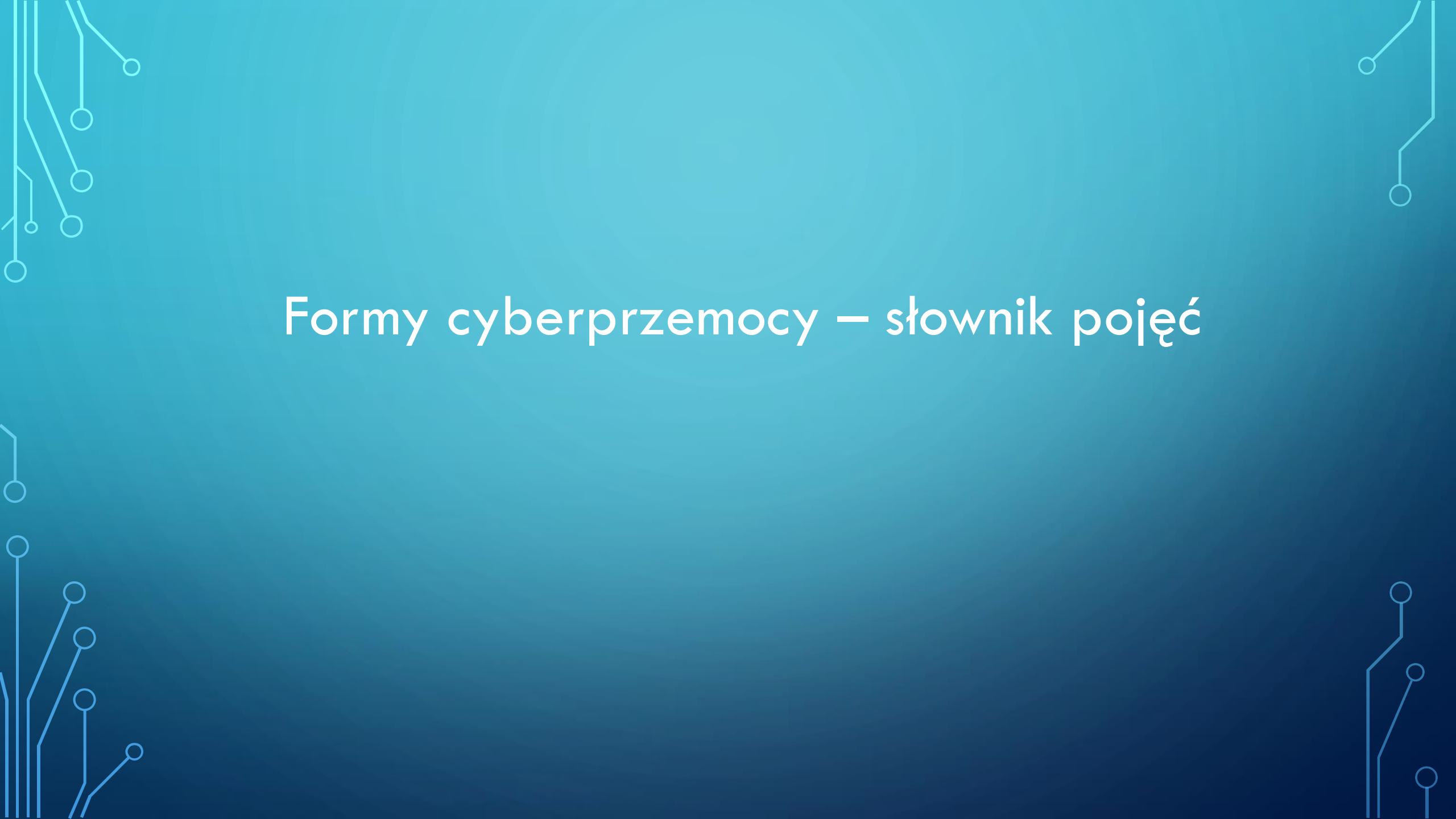
Zdecydowanie tak – 86%

Raczej powinno – 9%

Częste rozmawianie w portalu społecznościowym o swoich zainteresowaniach	68
Regularne prowadzenie bloga	6,5
Regularna gra w gry online	40
Szukanie informacji nt. osobistego problemu tam, gdzie piszą specjaliści	50
Szukanie informacji nt. osobistego problemu na forach	44
Prowadzenie strony internetowej/fanpage jakiejś organizacji	15
Zgłaszanie niewłaściwych treści	32
Prowadzenie innej strony własnej niż profil na Facebooku	20
Regularne wykorzystanie internetu do nauki	76 😊

Poza online i offline

	Cyber - nie	Cyber – raz	Cyber-2-3 razy	Cyber - 4 razy lub więcej
Bullying - nie	95	4	1	0
Bullying - raz	80	18	2	0
Bullying – 2-3 razy	74	15	10	1
Bullying – 4 razy lub więcej	60	17	9	15

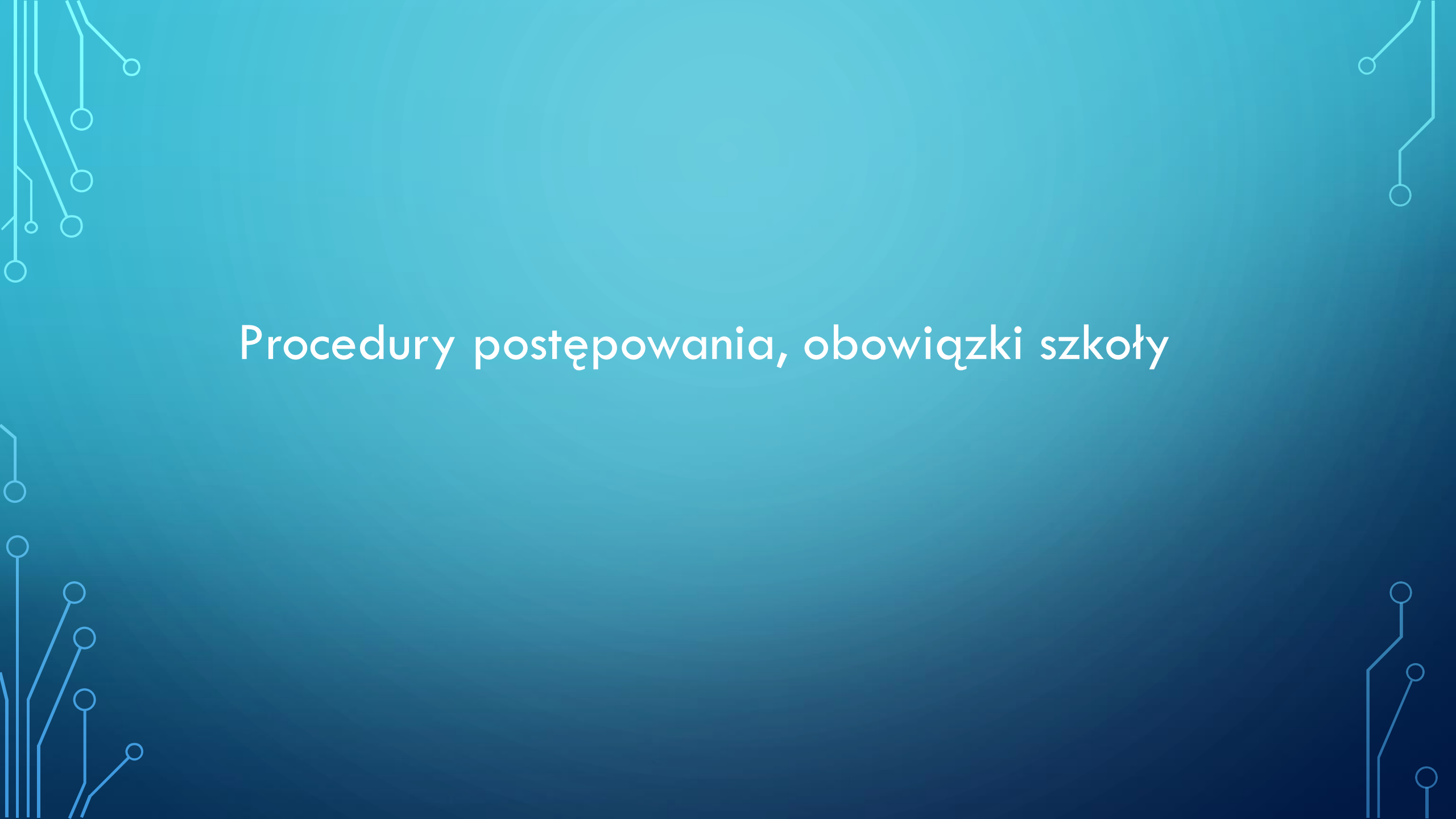
The background is a blue gradient. In the corners, there are white line-art illustrations of circuit boards or neural networks, with lines connecting to small circles.

Formy cyberprzemocy – słownik pojęć

- **phishingiem** określa się nakłanianie użytkowników metodami socjotechnicznymi do ujawniania swoich wrażliwych danych (identyfikatorów i haseł, numerów i dat ważności kart kredytowych) w celu ich późniejszego wykorzystania do dokonywania oszustw przez cyberprzestępców,
- spektakularnym przykładem infekcji jest typ wirusa zwany „ransomware”, który próbuje wymusić okup na użytkowniku, który w pewnym momencie od zarażenia, otrzymuje na ekranie informację, że zablokowano mu dostęp do danych na dysku i musi zapłacić przez Internet sporą kwotę (np. kilkaset złotych) aby ten dostęp odzyskać,

- **seksting** to przesyłanie za pomocą Internetu i urządzeń mobilnych swoich zdjęć, filmów lub wiadomości o charakterze seksualnym. Zjawisko to dotyczy całej grupy internautów - dorosłych, dzieci i młodzieży. Szczególnie w przypadku tej ostatniej grupy możemy mówić o poważnym zagrożeniu i konsekwencjach wiążących się z tym zjawiskiem,
- **flaming** – agresywna wymiana zdań na czacie lub w grupie dyskusyjnej,
- **griefing** – prześladowanie kogoś w grze,
- **trolling** – uparte umieszczanie złośliwych wobec kogoś komentarzy w sieci,
- **maskarada** – tworzenie przez osobę prześladowującą fałszywych profili internetowych celem zaszkodzenia komuś,

- **fraping** - zmiana detali czyjegoś konta celem upokorzenia go,
- **dising** – umieszczanie w Internecie okrutnych informacji, zdjęć, filmów dotyczących dzieci,
- grooming – zaprzyjaźnianie się z dziećmi, aby obniżyć poziom zahamowania dziecka na napastowanie seksualne,
- **sexcasting** – wymienianie się filmami o seksualnym kontekście bez wiedzy i zgody ofiary,
- **księgi obelg** – elektroniczne zapiski krążące wśród młodzieży mające na celu udzielanie złośliwych komentarzy mających na celu prześladowanie

The background is a blue gradient. In the corners, there are white line-art illustrations of circuit boards or neural networks, with lines and small circles representing nodes.

Procedury postępowania, obowiązki szkoły

Przestępstwa ścigane z urzędu

- zakłócanie pracy systemu informatycznego (art. 269a kk)
- przestępcze udostępnianie urządzeń, programów lub haseł komputerowych (art. 269b kk)
- oszustwa komputerowe (art. 287 kk par.1, 2)
- rozpowszechnianie pornografii (art. 202 kk)
- propagowanie ustrojów totalitarnych (art. 256 kk)
- znieważenie publiczne grupy osób (na tle np. etnicznym/religijnym) (art. 257 kk.)

**Obowiązek
Dyrektora placówki
do powiadomienia
Policji
lub prokuratury**

Przestępstwa wobec których pokrzywdzony występuje w roli oskarżyciela

- groźba karalna (art. 190 kk)
- uporczywe nękanie (art. 190a kk)
- utrwalenie wizerunku nagiej osoby bez jej zgody, naruszenie intymności seksualnej (art. 191a kk)
- bezprawne uzyskanie informacji (art. 267 kk)
- naruszenie prawa do zapoznania się z informacją (art. 268 kk)
- niszczenie danych informatycznych (art. 268a kk)

**Poinformowanie
pokrzywdzonego
i rodzica/opiekuna
prawnego
o możliwości
złożenia wniosku**

Przestępstwa ścigane na wniosek pokrzywdzonego

- zniesławienie (art. 212 kk)
- zniewaga (art. 216 kk)

**Poinformowanie
pokrzywdzonego
i rodzica/opiekuna
prawnego
o możliwości
złożenia wniosku**



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

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

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

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

OCHRONA PRAWNA §

Art. 267 i 268 Kodeksu karnego

Art. 23 i 24 Kodeksu cywilnego oraz art. 212 i 216 Kodeksu karnego

Art. 141 Kodeksu wykroczeń

Art. 190 a Kodeksu karnego i art. 107 Kodeksu wykroczeń

REAGOWANIE



Powiadomić administratora sieci, strony internetowej itp.

Zwrócić się do administratora sieci, strony internetowej itp. o usunięcie lub zablokowanie wpisów.

Zwrócić się do administratora sieci, strony internetowej itp. o usunięcie lub zablokowanie wpisów.

Zwrócić się do administratora sieci, strony internetowej itp. o usunięcie lub zablokowanie wpisów.

Złożyć wniosek o ściganie na policję lub do prokuratury.

Złożyć wniosek o ściganie na policję lub do prokuratury.

Powiadomić policję o popełnieniu wykroczenia.

Powiadomić policję o popełnieniu wykroczenia.

Złożyć pozew cywilny o odszkodowanie.

Powiadomić policję lub prokuraturę o popełnieniu przestępstwa.



Zjawisko groomingu,
czyli nagabywanie w
sieci dzieci do celów
seksualnych

Publikacja
materiałów
pornograficznych

Utrwalenie bez zgody
wizerunku nagiej
osoby, naruszenie
intymności
seksualnej

Zakłócenie
pracy systemu
komputerowego

OCHRONA PRAWNA §

Art. 200 a
Kodeksu karnego

Art. 202
Kodeksu karnego

Art. 191a Kodeksu
karnego, art. 23 i 24
Kodeksu cywilnego,
art. 81 Ustawy
o prawie autorskim

Art. 268 a, 269 a,
269 b Kodeksu
karnego, art. 415
Kodeksu cywilnego

REAGOWANIE



Powiadomić
administrатора
sieci, strony
internetowej itp.

Powiadomić
administrатора
sieci, strony
internetowej itp.

Zwrócić się
do administratora
sieci, strony
internetowej itp.
o usunięcie
lub zablokowanie
dostępu do zdjęcia
(wizerunku).

Złożyć wniosek
o ściganie
na policję
lub do
prokuratury.

Powiadomić
policję
lub prokuraturę
o popełnieniu
przestępstwa.

Powiadomić
policję
lub prokuraturę
o popełnieniu
przestępstwa.

Złożyć wniosek
o ściganie
na policję
lub do
prokuratury.

Złożyć pozew
cywilny
o naprawienie
szkody.

Zgłosić do
dyzurnet.pl
(możliwość
anonimowego
zgłoszenia).

Złożyć
pozew cywilny
o odszkodowanie.

The background is a blue gradient with decorative white circuit-like lines in the corners. The text is centered and reads:

Dokument Departamentu Wychowania i Kształcenia Integracyjnego MEN

Zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu

Podstawy prawne: Ustawa z dnia 14 grudnia 2016 r. – Prawo Oświatowe

Rodzaj zagrożenia – infoholizm (siecioholizm)

Przyjęcie zgłoszenia – rodzice/prawni opiekunowie

Zadania szkoły – zebranie informacji na temat skutków uzależnienia na zachowanie ucznia (niedojadanie, niedosypianie, apatia, gorszy kontakt z rówieśnikami, pogorszenie ocen). Współpraca z rodzicami

Aktywność wobec ofiary – opieka pedagoga/psychologa, specjalistyczne badania

Współpraca ze służbami – w przypadku zdiagnozowania przez psychologa zaawansowanego uzależnienia dziecko powinno zostać skierowane do placówki specjalistycznej oferującej program terapeutyczny

Bezkrytyczna wiara w treści zamieszczone w Internecie

Podstawy prawne: Ustawa z dnia 11 stycznia 2017 r. – Prawo Oświatowe

Rodzaj zagrożenia – brak umiejętności selekcjonowania informacji, prawda-fałsz, wiara we wszystkie treści umieszczone w Internecie np. diety, ściągki, rozwiązania zadań

Przyjęcie zgłoszenia – identyfikują najczęściej nauczyciele

Zadania szkoły – takie zachowanie powinno być zauważone przez nauczyciela, przeanalizowane i sprostowane

Aktywność wobec sprawcy – opublikowanie sprostowania

Aktywność wobec ofiar i świadków – szkoła powinna prowadzić działania profilaktyczne



Internet stał się trwałym elementem funkcjonowania placówek oświatowych. Wykorzystywany jest przede wszystkim w procesie nauczania, ale coraz częściej także jako element działania i funkcjonowania organizacyjnego oraz administracyjnego placówki. Do niedawna traktowany jako nowość, dziś jawi się nie tylko jako stały, ale także niezbędny element funkcjonowania szkoły.

Gwałtowna ekspansja sieci, coraz większa jej obecność w edukacji i w procesach komunikowania, w naturalny sposób nie szły w parze z tworzeniem zasad, procedur i norm postępowania. Należy zauważyć, iż rozwojowi sieci towarzyszy pojawienie się w Internecie niebezpiecznych zjawisk i przestępczości.



Mamy do czynienia zarówno z zagrożeniami o charakterze technicznym, jak i społecznym. Te pierwsze to między innymi wykradanie danych, blokowanie dostępu, wszelkiego rodzaju szkodliwe programy komputerowe, takie jak niszczące zasoby lub przejmujące kontrolę nad komputerami użytkowników. Zagrożenia o charakterze społecznym wiążą się przede wszystkim z pojawianiem się w sieci niebezpiecznych i nielegalnych treści.

The background is a blue gradient. In the corners, there are white line-art illustrations of circuit boards or neural networks, with lines connecting to small circles.

Standard bezpieczeństwa online placówek oświatowych



Standard obejmuje także etapy takie jak:

- diagnostykę,
 - działania o charakterze informacyjnym,
 - profilaktykę,
 - reagowanie po wystąpieniu incydentu
 - działania wychowawcze
- 
- 



Źródło: opracowanie Marcin Bochenek

Działania diagnostyczne

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

Do zadań lidera bezpieczeństwa online należy:

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

Działania szkoleniowe i edukacyjne

W ślad za działaniami informacyjnymi powinny iść działania szkoleniowe i edukacyjne. Także i ta aktywność kierowana jest zarówno do pracowników placówki, uczniów oraz rodziców. Tematyka zajęć powinna dotyczyć informacji o zagrożeniach i metodach przeciwdziałania, jak i zagadnienia szeroko rozumianej edukacji medialnej.

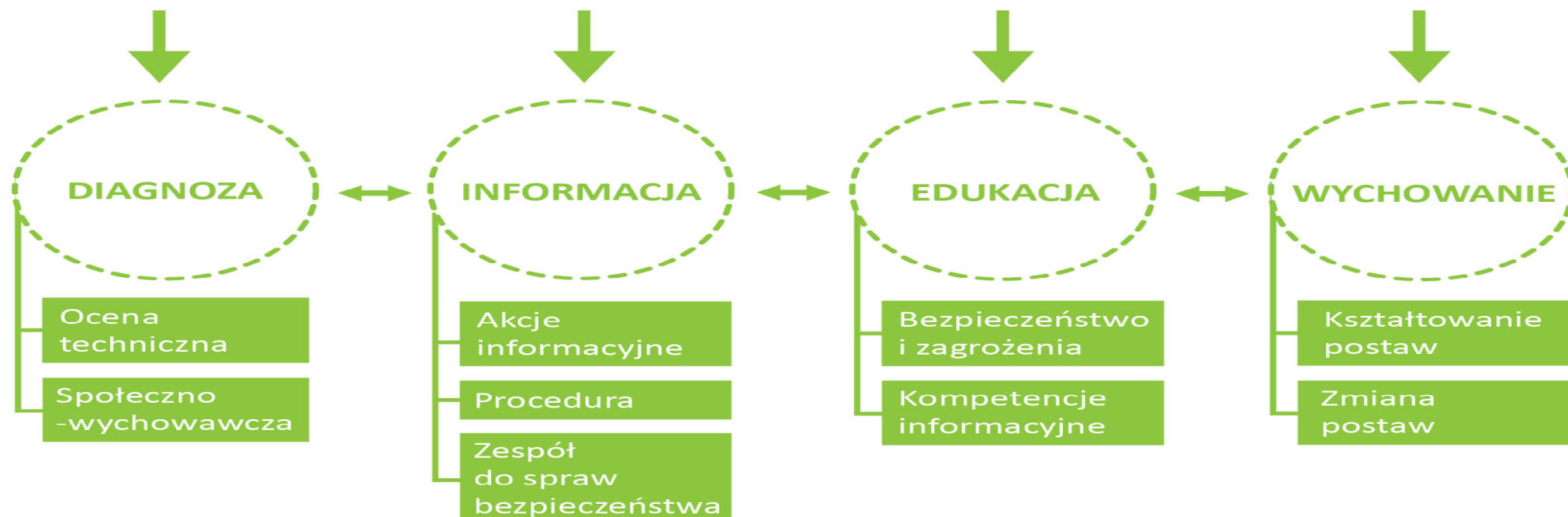
Profilaktyka - Zapobieganie wystąpieniu cyberproblemów

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

Działania informacyjne

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

DZIAŁANIA PROFILAKTYCZNE



UCZEŃ



DOROŚLI
- NAUCZYCIELE/RODZICE

WSPÓŁPRACA ŚRODOWISKA SZKOLNEGO
WEW. (ZBO + WYCHOWAWCY I DYREKCJA) I ZEWN. (POLICJA, SĄD, SPECJALIŚCI)



POZIOM MINIMALNY

- infrastruktura niskobudżetowa, rozwinięta w stopniu minimalnym, realizowany jest dostęp do Internetu
- musi spełniać minimalne wymagania technicznego bezpieczeństwa
- jest zapewniona opieka nad infrastrukturą oraz osoba administrująca infrastrukturą IT (może pochodzić z zewnątrz)

POZIOM PODWYŻSZONY

- bardziej rozwinięta infrastruktura, wykorzystywane są aplikacje, systemy informatyczne i sieć lokalna
- poziom minimalny bezpieczeństwa jest niewystarczający, rekomendowane są zabezpieczenia klasy firmowej*
- ustanowiony administrator infrastruktury IT
- ustanowiona polityka bezpieczeństwa

POZIOM PROFESJONALNY

- funkcjonuje profesjonalnie utrzymany Intranet
- dodatkowe systemy bezpieczeństwa (m.in. centralny AV, IDS)
- audyty bezpieczeństwa, także z wykorzystaniem zewnętrznych pentesterów

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

Poziom minimalny

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

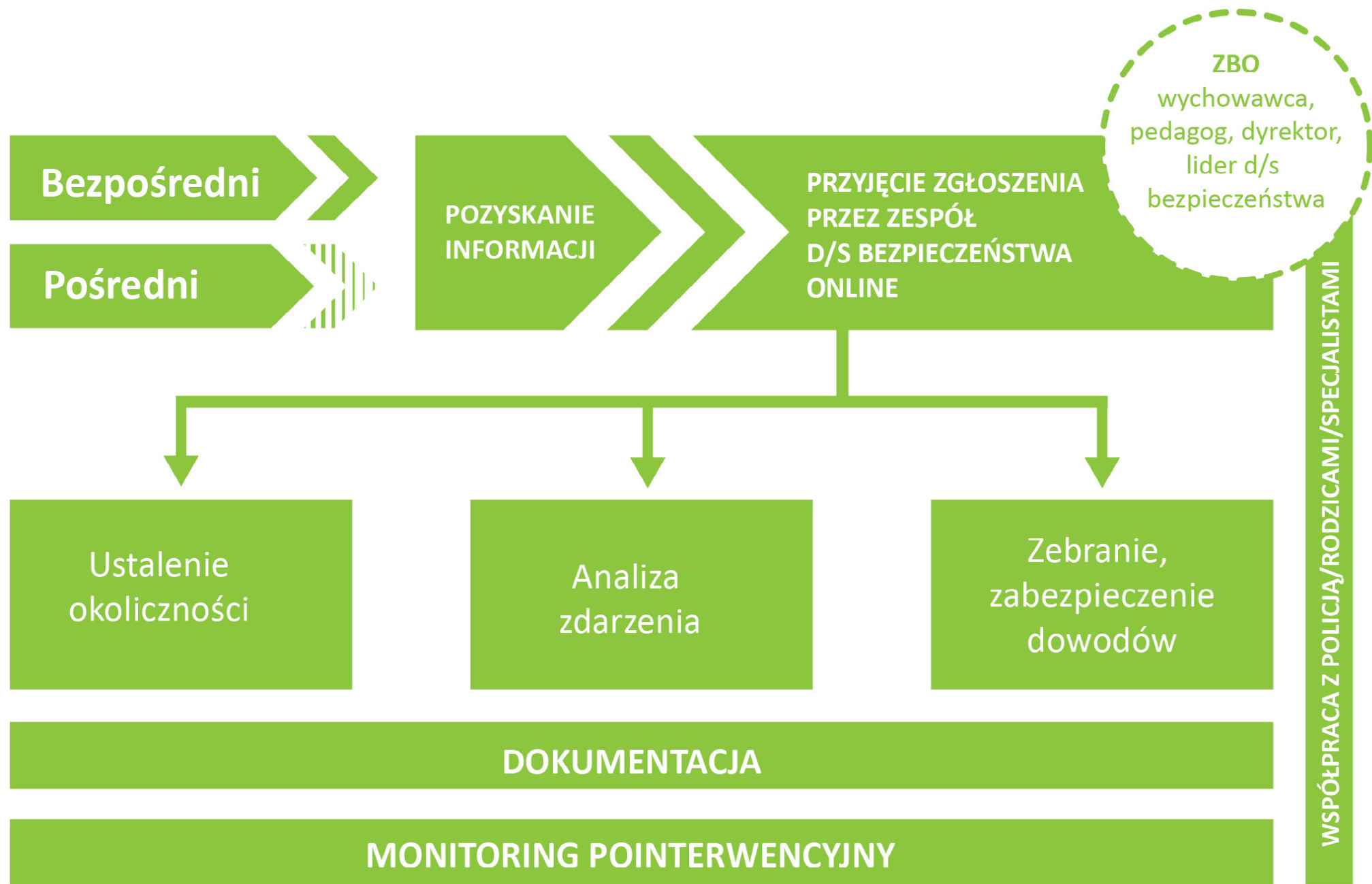
W ramach zapewniania minimalnego poziomu bezpieczeństwa oraz właściwej opieki nad infrastrukturą, zaleca się:

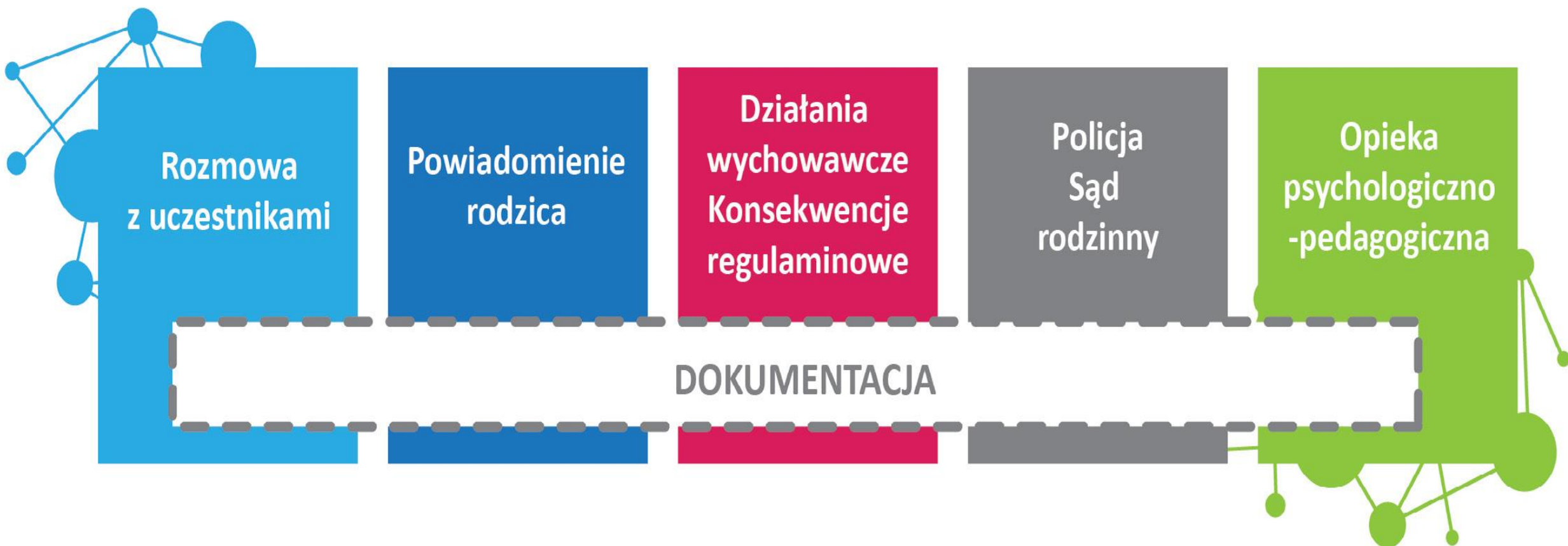
- Ustanowić administratora dbającego o prawidłowe funkcjonowanie infrastruktury komputerowej,
- Lokalne urządzenie dostępowe (router) zapewniające mechanizm ochrony danych oparty o standard szyfrowania, sieć bezprzewodowa (WiFi) dostępna tylko na hasło,
- Dodatkowo zaleca się zastosowanie przy dostępie WiFi tzw. strony startowej, na której powinny znaleźć się informacje o zasadach bezpiecznego korzystania z Internetu,
- Na routerze powinna zostać włączona usługa przegrody firewall,
- Strona WWW powinna zostać posadowiona na serwerze hostingowym operatora zapewniającego odpowiedni poziom bezpieczeństwa.

- Na komputerach szkolnych powinny być zainstalowane programy antywirusowe,
- Korzystanie z usług chmurowych jest dopuszczalne pod warunkiem spełnienia określonych wymagań, takich jak: weryfikacja dostawcy, zapoznanie się z regulaminem usługi, zapoznanie się zasadami zapewniania prywatności danych,
- W placówce powinien powstać uproszczony dokument polityki bezpieczeństwa oraz regulamin korzystania z sieci komputerowej i dostępu do Internetu.

Model interwencji

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





Może się przydać 😊

Dokumentacja procedury interwencyjnej

Przepisy regulujące zasady współpracy placówki z policją, sądem

Jak reagować na cyberprzemoc

Broszura - zapobieganie, reagowanie

Broszura - reagowanie

Dobre praktyki

<https://web.facebook.com/cyberprzemocwolnastrefa/videos/1818977348357659/?rdc=1&rdp=1>

Dobre praktyki

www.fundacja.orange.pl

www.dyzurnet.pl

www.sieciaki.pl

www.saferinternet.pl

www.fdds.pl

www.cert.pl

www.kidprotect.pl

www.dzieckowsieci.pl

www.cybernauci.edu.pl

BEZPIECZEŃSTWO W INTERNECIE - CO TRZEBA WIEDZIEĆ O INTERNECIE, ABY CZUĆ SIĘ BEZPIECZNIE?

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

Dostawca Internetu

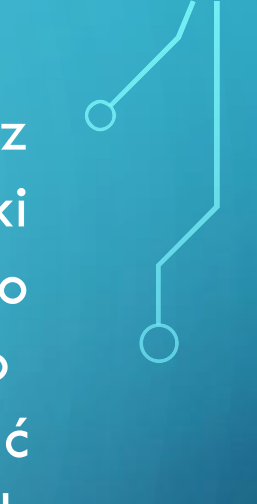
Dostęp do Internetu jest usługą, która jest oferowana przez rozmaite podmioty takie jak: operatorzy telekomunikacyjni, wyspecjalizowani dostawcy Internetu, operatorzy sieci kablowych, lokalni dostawcy bezprzewodowego Internetu i inni. Jest istotne aby mieć świadomość, iż wszystkie te podmioty muszą zgłosić działalność telekomunikacyjną w Polsce i podlegają rygorom Prawa Telekomunikacyjnego (także w obszarze stosowania zasad bezpieczeństwa). Zawierając umowę na dostawę Internetu, **należy sprawdzić, czy dany podmiot znajduje się w rejestrze Urzędu Komunikacji Elektronicznej¹.**

Dostawca treści

Do tej grupy można zaliczyć serwisy społecznościowe, sklepy internetowe, portale, serwisy chmurowe oraz inne formy. Dostawcy treści mogą być zlokalizowani gdziekolwiek na świecie i podlegają prawu lokalnemu, w miejscu gdzie usługodawca zarejestrował działalność. Ma to znaczenie w przypadku, kiedy w danym serwisie zajdzie jakieś zdarzenie naruszające bezpieczeństwo. **Korzystając z usług dostawców treści należy dokładnie przestudiować regulaminy korzystania z usługi a także warunków umownych danej usługi.** W Polsce świadczenie usług wykorzystujących komunikację internetową podlega ustawie o świadczeniu usług drogą elektroniczną².

Dostawcy kolokacji, hostingu lub rozwiązań chmurowych

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

- 
- 
- Wszelkie systemy komputerowe, te z których zbudowany jest Internet oraz urządzenia i sieci klientów, nie mogą sprawnie działać bez zapewnienia opieki technicznej w postaci osób administrujących danymi systemami. Bez stałego i uporządkowanego procesu utrzymania i zarządzania systemy komputerowe po pewnym czasie zaczęłyby pracować wadliwie, przestałyby zapewniać jakikolwiek poziom bezpieczeństwa oraz nie nadążałyby za wymaganiami ich użytkowników.

Nie można zatem pozwolić, by infrastruktura klienta Internetu była pozbawiona opieki technicznej. Jeśli w danej instytucji nie ma odpowiednich zasobów kadrowych, taką opiekę należy powierzyć osobom lub firmom zewnętrznym.



Świadomość podstawowych pojęć związanych z bezpieczeństwem

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

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

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

Szyfrowanie

Zapewnienie poufności przesyłanych (lub składowanych) danych wrażliwych (takich jak loginy, hasła, numery kart płatniczych, dane osobowe) wymaga stosowania mechanizmów takich jak szyfrowanie, które przetwarzają chronione dane na zakodowany ciąg znaków, niemożliwy do zinterpretowania przez potencjalnych intruzów. Popularną implementacją szyfrowania, jest w codziennej praktyce tzw. „zielona kłódeczka” w pasku adresowym przeglądarki internetowej, która świadczy o tym, że połączenie z serwerem jest szyfrowane.

Aktualizacje

Aktualizacjami nazywamy wszelkie czynności ręczne lub zadania realizowane automatycznie polegające na wprowadzeniu (zazwyczaj poprzez Internet) nowych wersji oprogramowania (systemu operacyjnego bądź aplikacji), które usuwają zauważone przez producenta błędy w oprogramowaniu lub podatności na zagrożenia.

Kopie zapasowe

Kopie zapasowe, podobnie jak aktualizacje, powinny być wykonywane cyklicznie. Można wykonywać duplikaty całej zawartości dysku, bądź tylko określonych zasobów (partycji dysku, katalogów plików, danych kontaktowych itp.) Istotne jest to aby dostosować częstotliwość wykonywania kopii do częstości zmian naszych danych oraz poziomu ich istotności. Wersje zapasowe koniecznie należy przechowywać w innym miejscu niż znajdują się dane oryginalne.

Systemy bezpiecznego uwierzytelniania

Bezpieczne uwierzytelnienie polega na zastosowaniu takich mechanizmów przy podawaniu loginu i hasła aby jak najtrudniejsze było ich przechwycenie i nieuprawnione użycie przez inne osoby lub szkodliwe oprogramowanie. Klasyczne hasła zwane są hasłami statycznymi. Ich siła opiera się na doborze odpowiednio długiego ciągu znaków, różnego typu (litery, cyfry, znaki specjalne).

Jednak takie hasło, nawet jeśli jest trudne do odgadnięcia, może zostać podsłuchane. Bezpieczniejszym rozwiązaniem, jest stosowanie systemów haseł jednorazowych (stosowanie generatorów haseł jednokrotnych – tzw. tokenów bądź wprowadzanie kodów otrzymanych SMSem w trakcie logowania).

Bezpieczeństwo w chmurze

Usługami chmurowymi nazywamy wszelkie usługi internetowe, które polegają na przechowywaniu bądź przetwarzaniu danych użytkownika w rozproszonym środowisku serwerowym usługodawcy. Mogą to być usługi wykonywania i przechowywania kopii zapasowych w chmurze przechowywanie plików, czy korzystanie z rozmaitych aplikacji bez potrzeby ich lokalnego instalowania (np. edytory tekstów). Przy korzystanie z usług chmurowych należy dokładnie zapoznać się regulaminem usługi aby poznać ofertę, także od strony bezpieczeństwa.

Rodzaje zagrożeń:

- zarażanie poprzez surfowanie - jednym z najczęstszych ataków z wykorzystaniem szkodliwego oprogramowania jest zarażanie urządzeń użytkowników sieci Internet, korzystających z przeglądarki. Wiele stron WWW, ale także portali społecznościowych, zawiera w miejscach odwiedzanych przez internautów kody szkodliwych programów, które użytkownik nieświadomie ściąga na swe urządzenia,
- każdy system oparty na pracy komputerów oraz wykorzystujący aplikacje może zostać zainfekowany szkodliwym oprogramowaniem. Istnieje wiele typów takich zagrożeń w postaci: wirusów komputerowych, koni trojańskich, oprogramowania szpiegującego czy atakującego użytkowników bankowości elektronicznej. Szkodliwe programy mogą wniknąć poprzez połączenia z Internetem, są przynoszone przez niefrasobliwych użytkowników (np. na pamięciach USB),

Rodzaje zagrożeń dla szkoły

Wykorzystanie szkolnej infrastruktury do nielegalnej lub szkodliwej działalności

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

Zagrożenia ze strony przenośnych nośników pamięci

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

Zagrożenia związane z WiFi

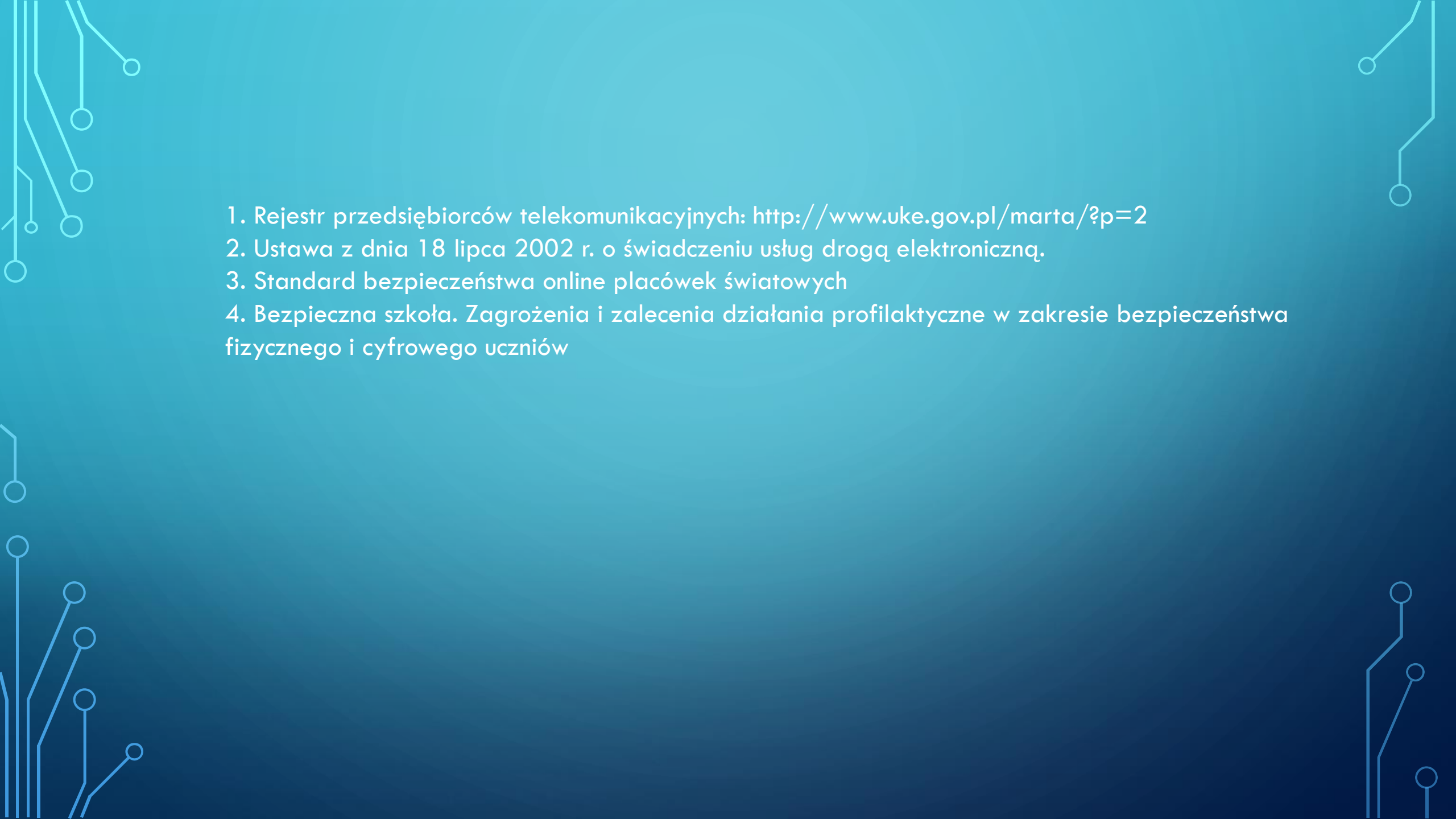
Jest niezwykle istotne, by przemyśleć fakt i zakres udostępniania WiFi. W szczególności szyfrowanie dostępu do hotspotów i rejestracja użytkowników korzystających jest pierwszym krokiem do ograniczania zagrożeń. Jeśli bowiem ktokolwiek mógłby anonimowo skorzystać z szkolnej sieci WiFi należy się spodziewać, że zostanie to niewłaściwie wykorzystane.

CERT Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet. CERT Polska działa od 1996 roku. Zespół CERT Polska działa w strukturach Naukowej i Akademickiej Sieci Komputerowej (NASK). Do głównych zadań zespołu należy m.in.: rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci, alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń, prowadzenie działań zmierzających do wzrostu świadomości dotyczącej bezpieczeństwa teleinformatycznego, prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów internetu, a także niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego.

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

- odpowiednia architektura IT (separacja segmentów przeznaczonych do różnych zastosowań)
- stosowanie systemów firewall (FW), antywirusowych (AV)
- stosowanie filtrów treści szkodliwych
- wykonywanie kopii zapasowych
- przeprowadzanie automatycznych aktualizacji.

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

- 
- The background is a solid blue gradient. In the corners, there are decorative white line art elements resembling circuit boards or fiber optic paths, with small circles at the end of the lines.
1. Rejestr przedsiębiorców telekomunikacyjnych: <http://www.uke.gov.pl/marta/?p=2>
 2. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
 3. Standard bezpieczeństwa online placówek światowych
 4. Bezpieczna szkoła. Zagrożenia i zalecenia działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów