Colloquium 2(58)/2025
ISSN 2081-3813, e-ISSN 2658-0365
CC BY-NC-ND.4.0
DOI: http://doi.org/10.34813/29coll2025

SZKOŁA JAKO ŚRODOWISKO ZAPEWNIANIA CYBERBEZPIECZEŃSTWA DZIECI I MŁODZIEŻY – ZAGROŻENIE PATOSTREAMINGIEM

School as an environment for ensuring cybersecurity for children and youth – trash stream threat

Marian Kopczewski
Akademia Wojsk Lądowych im. gen. Tadeusza Kościuszki
e-mail: marian.kopczewski@interia.pl
ORCID 0000-0002-0402-0477

Aleksandra Paprotny
Akademia Wojsk Lądowych im. gen. Tadeusza Kościuszki
e-mail: aleksandraapaprotny@gmail.com
ORCID 0000-0001-9592-2734

Streszczenie

Celem artykułu jest scharakteryzowanie roli i znaczenia szkoły w zapewnieniu cyberbezpieczeństwa dzieci i młodzieży w kontekście zagrożenia patostreamingiem. Przedstawiono zjawisko patostreamingu i możliwości działań, które szkoła powinna podejmować w przypadku kontaktu uczniów z treściami prezentowanymi podczas patostreamów. Szczególną uwagę poświęcono procedurze interwencyjnej, której wdrożenie obok działań profilaktycznych stanowi zasadnicze działanie placówki oświatowej w zakresie realizacji szkolnej strategii cyberbezpieczeństwa.

Słowa kluczowe: patostreaming, edukacja, szkoła, profilaktyka, procedura reagowania.

Abstract

The aim of the considerations in the article is to characterize the role and importance of the school for ensuring cybersecurity for children and youth in the context of trash streaming. Authors presented trash streaming threat and possibilities of school activities in the event of contact of students with the phenomena. Special attention was given to the intervention procedure and preventive activities carried out by the school as part of the school cybersecurity strategy.

Keywords: trash streaming, education, school, prevention, intervention procedure.

Wstęp

Bezpieczeństwo użytkowników przestrzeni wirtualnej jest obecnie jednym z najpoważniejszych wyzwań. Wraz z oddaniem Internetu do użytku publicznego stale wzrasta poziom rozpowszechnienia wykorzystania technologii informacyjnych zarówno przez instytucje państwowe i podmioty gospodarcze, jak również społeczeństwa. Rozwój cyberprzestrzeni determinuje rozwój zagrożeń, na które narażeni są użytkownicy Internetu. Katalog cyberzagrożeń nie jest zamknięty, wciąż pojawiają się nowe niebezpieczeństwa, a te, które już są znane ewoluują i zmieniają swoją formę. Jednym z nowych zjawisk w cyberprzestrzeni jest patostreaming, który postrzegany jest w kategoriach zagrożeń związanych z dostępem do niebezpiecznych, szkodliwych treści. Grupą szczególnie narażoną na negatywne oddziaływanie treści prezentowanych podczas patostreamów są dzieci i młodzież, ponieważ to właśnie w tej grupie internautów patostreaming cieszy się największą popularnością. W artykule wykorzystano następujące metody badawcze: krytyczną analizę literatury przedmiotu i dokumentów normatywnych oraz analizę wtórnych danych statystycznych. Na podstawie otrzymanych wyników przedstawiono kluczową rolę szkoły w zwalczaniu i minimalizowaniu negatywnych skutków oglądania patostreamów przez dzieci i młodzież.

Patostreaming jako nowe, niebezpieczne zjawisko w cyberprzestrzeni

Zdefiniowanie patostreamingu jest zadaniem złożonym i choć pierwsze wzmianki o tym cyberzagrożeniu pojawiają się w literaturze przedmiotu już w 2018 roku, to do dziś nie doczekało się ono uniwersalnej definicji. Pierwsza próba usystematyzowania wiedzy na temat patostreamingu została podjęta przez Fundację Dajemy Dzieciom Siłę, która w 2019 roku opublikowała dokument *Patotreści. Raport o problemie*. W raporcie tym przedstawiono pierwszą definicję patostreamingu, która przyjęła brzmienie:

> […] to treści prezentowane w sieci w postaci transmisji internetowej (*stream*), fragmentów transmisji (*shoty*), filmów, zdjęć i innych form przekazu, w których nadawca lub grupa nadawców prezentują zachowania sprzeczne z normami społecznymi, niosące demoralizujący przekaz, obejmujący zachowania takie jak: przemoc fizyczna, psychiczna, seksualna, libacje alkoholowe, poniżanie, zażywanie narkotyków i inne. (Wójcik i in., 2019, s. 7)

Problem ograniczania dostępu małoletnim użytkownikom Internetu do tego rodzaju materiałów wynika przede wszystkim ze specyficznego sposobu ich transmitowania – *streamingu*, tzn. relacji na żywo. Istotą transmisji w czasie rzeczywistym jest możliwość aktywnego uczestnictwa odbiorcy w prowadzonej audycji. Odbiorca, korzystając z urządzenia elektronicznego z dostępem do Internetu, może dodawać komentarze i reakcje na temat treści nagrania prezentowanego w czasie *streamu*. Również nadawca ma możliwość nawiązywania interakcji ze swoimi odbiorcami. Interakcje pomiędzy patostreamerami a ich widzami są realizowane w ramach tzw. *social streamingu*, którego

nazwa pochodzi od rodzaju stron internetowych należących do kategorii mediów społecznościowych, za pośrednictwem których jest prowadzona transmisja. Obecnie usługę *social streamingu* umożliwiają między innymi Facebook, X (dawniej Twitter), YouTube i Instagram, jednak patostreamerzy do nadawania patostreamów najczęściej wykorzystują YouTube (Paprotny, 2022, ss. 112–115)

Nie ma reguły dotyczącej czasu trwania i tematyki patostreamu. Treść prowadzonej transmisji zależy od patostreamera i, co zdarza się bardzo często, jego odbiorców. Do najbardziej popularnych rodzajów patostreamów należą:

- *drunkstream*, podczas którego patostreamer, najczęściej w towarzystwie znajomych, spożywa znaczne ilości alkoholu, robiąc „kociołek meneliksa" (wlewając do jednego naczynia różne rodzaje alkoholi i spożywając go na wizji);
- dymy, w czasie których dochodzi do różnego rodzaju aktów przemocy;
- *raidy*, których istota polega na atakowaniu przez patostreamera innych zarejestrowanych użytkowników YouTube poprzez mobilizowanie swoich odbiorców do odwiedzania kanału danego youtubera i zamieszczanie na nim obraźliwych, wulgarnych komentarzy. Celem *raidu* jest wywołanie reakcji, najlepiej wrogiej i równie agresywnej u atakowanego streamera (Wojtasik, 2019; Wojtyna, 2019).

Zaprezentowany podział rodzajowy dotyczący patostreamów jest umowny. Charakterystyka drunkstreamów, dymów i raidów wskazuje na przenikanie się tematów podejmowanych przez patostreamerów. Jedyna zasada obowiązującą w patotransmisjach brzmi – im bardziej kontrowersyjnie treści, tym lepiej. W kwestii długości trwania transmisji nie obowiązują limity czasowe. Najczęściej czas nadawania transmisji mieści się w przedziale od kilkunastu minut do kilku godzin. W Internecie jednak pojawiały się także patostreamy, które nadawane były bez przerwy przez kilka dni. (Paprotny 2022, s. 114)

Kontrowersyjność i brutalność treści prezentowanych podczas patostreamów wynika z chęci pozyskania przez patostreamera jak największego grona odbiorców, co wiąże się nie tylko ze zwiększeniem popularności, ale ma również przełożenie na korzyści finansowe. Średnie zarobki twórców internetowych regularnie publikujących w serwisie YouTube kształtują się na poziomie 9–10 tys. zł. Składają się na to dochody:

- z reklam, wypłacane przez serwis YouTube,
- pochodzące ze współpracy youtubera z konkretnymi firmami,
- z prowadzenia sklepów internetowych z gadżetami promującymi twórczość danego youtubera,
- z systemu Patronite, czyli comiesięcznych wpłat od osób wspierających aktywność danego youtubera (Paprotny 2022, s. 116).

Model zarabiania patostreamerów różni się jednak od tego, który jest najczęściej stosowany przez innych użytkowników serwisu YouTube publikujących filmy na swoich kanałach. Ze względu na kontrowersje wokół samego wizerunku patostreamerów oraz ich twórczości reklamodawcy nie decydują się na podjęcie z nimi współpracy w jakiejkolwiek formie. W celu uzyskania korzyści finansowych patostreamerzy namawiają swoich widzów do wpłacania tzw. donejtów, czyli finansowego wsparcia działalności patostreamera. Są to najczęściej niewielkie kwoty pieniężne (zazwyczaj od kilku do kilkudziesięciu złotych) wpłacane przez odbiorców w czasie trwania patostreamu. Cel i wysokość planowanej zbiórki pieniędzy określa patostreamer, najczęściej jeszcze przed rozpoczęciem transmisji. Najbardziej popularnym celem zbiórki jest zakup alkoholu i organizacja imprezy, podczas której będzie on spożywany, a przebieg której będzie tematem kolejnego streamu. Za pośrednictwem donejtów odbiorcy mogą wywierać wpływ na aktywność danego patostreamera. Do takiej interakcji dochodzi w chwili, gdy patostreamer zadaje swoim odbiorcom pytanie dotyczące tego, jakie treści chcą zobaczyć w prowadzonej przez niego transmisji, i wyznacza określoną kwotę, po zebraniu której podejmie się wykonania zaproponowanych przez widzów zadań. Odbiorcy mogą dokonywać przekazania donejtów anonimowo lub podając swoje imię, nazwisko, pseudonim. Ofiarodawcy decydujący się na podanie swoich danych mogą liczyć na wyświetlenie swojego nicku i wysokości wpłaconej kwoty w jednej z nakładek podczas transmisji live oraz odczytanie przez patostreamera lub syntezator mowy komentarza dołączonego do wpłaty (Paprotny 2022, ss. 116–117) Możliwość odczytania w czasie transmisji internetowej komentarza zamieszczonego przy wpłacaniu choćby niewielkiej kwoty jest niezwykle atrakcyjne dla dzieci i nastolatków, dla których przestrzeń wirtualna stanowi swego rodzaju naturalne środowisko funkcjonowania (Rigamonti, 2019).

Publikacja raportu dotyczącego patostreamingu i patotreści, a także powołanie przez Rzecznika Praw Obywatelskich Okrągłego Stołu do walki z patotreściami w Internecie zapoczątkowały ogólnopolską dyskusję na temat niebezpieczeństw związanych z dostępem dzieci i młodzieży do tego rodzaju treści w przestrzeni wirtualnej oraz sposób minimalizowania jego negatywnych skutków. W rekomendacjach uczestników Okrągłego Stołu do walki z patotreściami w Internecie uwzględniono między innymi kluczową rolę szkoły jako instytucji prowadzącej działalność edukacyjną.

Szkoła jako kluczowe środowisko kształtowania bezpiecznych zachowań w przestrzeni wirtualnej

Jak wskazują liczne wyniki badań (Lange, 2021; Pyżalski 2019; Pyżalski i.in., 2019), środowisko szkolne obok środowiska rodzinnego stanowi kluczową przestrzeń dla kształtowania wśród dzieci i młodzieży konstruktywnych sposobów korzystania z In-

ternetu oraz bezpiecznych zachowań w przestrzeni wirtualnej. Zgodnie z obowiązującym prawem oświatowym (Dz. U. 2017, poz. 59) szkoła jest podmiotem, na którym ciąży obowiązek upowszechniania wśród dzieci i młodzieży wiedzy o bezpieczeństwie, a także kształtowania właściwych postaw wobec zagrożeń, na które grupa ta narażona jest podczas podejmowania aktywności zarówno w świecie fizycznym, jak i wymiarze wirtualnym. O ile wdrażanie standardów i procedur bezpieczeństwa fizycznego uczniów jest zadaniem, które dyrekcja i kadra nauczycielska realizują, opierając się na wieloletnich doświadczeniach w tym zakresie, o tyle zapewnianie bezpieczeństwa cyfrowego uczniów stanowi stosunkowo nowy obszar działalności szkoły. Wynika to przede wszystkim z ewolucji technologii informacyjnych i cyberprzestrzeni oraz zmian zachodzących w społeczeństwie, w tym m.in. oddania Internetu do użytku publicznego, pojawienia się Internetu mobilnego, a także zmiana modelu korzystania przez dzieci i młodzież z urządzeń oraz mediów cyfrowych. Czynniki te sprawiają, że opracowanie i wdrażanie procedur zapewnianie uczniom bezpieczeństwa cyfrowego stanowi jedno z najpoważniejszych wyzwań, przed którym staje nowoczesna szkoła.

Szkoła jako placówka oświatowa prowadzi działalność edukacyjną w oparciu o trzy uzupełniające się obszary, do których należą:

- szkolny zestaw programów nauczania, który dotyczy pełnej działalności szkoły w zakresie dydaktycznym z uwzględnieniem wymiaru wychowawczego;
- program wychowawczy szkoły;
- program profilaktyczny obejmujący działania profilaktyczne dostosowane do potrzeb rozwojowych uczniów i potrzeb danego środowiska szkolnego (Dz.U. 2014, poz. 803).

Obowiązek zapewnienia przez szkołę bezpieczeństwa cyfrowego uczniów wpisuje się w programy profilaktyczne, które powinny uwzględniać działania wobec i z udziałem całości społeczności szkolnej, tj. uczniów i rodziców oraz wszystkich pracowników szkoły (dyrekcji, nauczycieli, psychologów, pedagogów). Według zaleceń działania w zakresie cyberbezpieczeństwa dzieci i młodzieży powinny mieć charakter systemowy, ciągły, wieloletni i skoordynowany. Z tego względu opracowano zbiór wytycznych, rekomendacji i standardów, których właściwa implementacja (adekwatna do potrzeb danego środowiska szkolnego i realizowana w ramach szkolnych programów: wychowawczego i profilaktycznego) pozwoli na wzmocnienie roli szkoły w kształtowaniu bezpiecznych i konstruktywnych sposobów korzystania przez dzieci i młodzież z Internetu oraz budowaniu dobrego klimatu społecznego szkoły, który w kontekście występowania zachowań ryzykownych wśród nieletnich jest jedynym z czynników chroniących. Psychologowie podkreślają, że w działaniach profilaktycznych istotna jest także integracja środowiska szkolnego poprzez budowanie przyjaznych relacji między uczniami i nauczycielami oraz wewnątrz grupy rówieśniczej. Zapobieganie incydentom wykluczania, a także uprzedzeniom, które często mają miejsce w środowisku uczniów,

przy jednoczesnej integracji uczniów przez organizację wspólnych wyjść lub pracę w grupach pozwala skutecznie obniżyć ryzyko wystąpienia różnego rodzaju zagrożeń, w tym także cyberzagrożeń, na przykład cyberbullyingu, którego ofiarą jest co piąty polski nastolatek (Paprotny 2022, ss. 168–169; Lange, 2021, ss. 79–90). Jedną ze skutecznych metod profilaktyki pozytywnej jest wspieranie uczniów w efektywnym i celowym wykorzystywaniu mediów cyfrowych do rozwoju zainteresowań i wspomagania procesu nauki. Innym, coraz powszechniejszym obszarem działań profilaktycznych jest także promowanie akcji społecznych, takich jak np. Dzień Bezpiecznego Internetu (dalej: DBI) obchodzony corocznie od 2004 roku z inicjatywy Komisji Europejskiej. Celem wydarzenia jest inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych, zaznajomienie rodziców, nauczycieli i wychowawców z problematyką bezpieczeństwa online oraz promocja pozytywnego wykorzystywania Internetu (Paprotny 2022, s. 169). Dyrekcja lub nauczyciele mogą zgłosić chęć zaangażowania się danej szkoły w obchody DBI i w ramach tego wydarzenia zorganizować w swojej placówce zajęcia edukacyjne, happeningi, konkursy i kampanie informacyjne. Instytucje, które zdecydują się na udział w DBI i wypełnią formularz na stronie internetowej wydarzenia otrzymują materiały edukacyjne i promocyjne, między innymi scenariusze zajęć profilaktycznych, zeszyty ćwiczeń, ścieżki edukacyjne.

Aktywne uczestnictwo szkół w kampaniach na rzecz bezpieczeństwa w sieci przyczynia się nie tylko do podnoszenia poziomu kompetencji cyfrowych dzieci i młodzieży oraz zdobywania przez nie nowych umiejętności w zakresie bezpiecznego korzystania z nowoczesnych technologii, ale stanowi również element rozwoju kompetencji kadry pedagogicznej w podejmowaniu działań profilaktycznych w zakresie kształtowania bezpiecznych postaw uczniów wobec wyzwań i zagrożeń, z którymi mają do czynienia, korzystając z Internetu. Najpowszechniejszą praktyką profilaktyczną stosowaną w wielu polskich szkołach jest ograniczanie uczniom dostępu do Internetu i urządzeń elektronicznych w przestrzeni szkolnej na przykład poprzez limitowany dostęp w wybranych salach lub wprowadzenie zakazu korzystania z własnych urządzeń elektronicznych w trakcie lekcji lub na terenie szkoły. Działania takie, choć prowadzone w celu przeciwdziałania niekorzystnemu wpływowi zaangażowania uczniów w świat wirtualny w celach niezwiązanych z nauką, budują obraz jedynie pozornego bezpieczeństwa cyfrowego w środowisku szkolnym. Psychologowie i pedagodzy podkreślają, że system zakazów dotyczących korzystania z mediów cyfrowych w zderzeniu z modelem niemal stałej obecności dzieci i młodzieży w sieci sprawia, że uczniowie zaczynają postrzegać szkołę jako środowisko wykluczenia, restrykcji i anachronizmu (Paprotny 2022, s. 170). Według rekomendacji realizacja założeń pozytywnej profilaktyki w środowisku szkolny powinna przebiegać przede wszystkim na drodze rozmowy na temat cyberbezpieczeństwa. Regularnie organizowane pogadanki o bezpiecznych zachowaniach w sieci i konstruktywnym korzystaniu z Internetu są przejawem zainteresowania życiem

dzieci i młodzieży, co pozytywnie wpływa na budowanie relacji uczeń–nauczyciel. Ponadto bezpośrednie rozmowy z uczniami o cyberbezpieczeństwie pozwalają na właściwe określenie obszaru funkcjonowania podopiecznych online. Umożliwia to między innymi rozpoznanie e-aktywności podejmowanych przez uczniów danej szkoły, obserwację trendów w tym zakresie oraz identyfikację cyberzagrożeń (Piechna, 2019). Jak podkreślają psychologowie, istotnym warunkiem efektywnego prowadzenia dyskusji z uczniami na temat ich zaangażowania w świat wirtualny jest stworzenie atmosfery zaufania i akceptacji. Tylko w momencie przezwyciężenia obaw dzieci i młodzieży przed ewentualną krytyką i karami zostanie stworzona właściwa przestrzeń do wymiany myśli i refleksji na temat rzeczywistych problemów, z którymi się zmagają jako użytkownicy nowoczesnych technologii. Skuteczność działań profilaktycznych w środowisku szkolnym zależy przede wszystkim od stałej obecności problematyki cyberbezpieczeństwa w procesie nauczania oraz wychowania dzieci i młodzieży (Rywaczyńska i Wójcik, 2018). Wśród rekomendacji Ministerstwa Edukacji i Nauki w zakresie zapewnienia bezpieczeństwa cyfrowego dzieciom i młodzieży znajdują się wytyczne dotyczące prowadzenia zajęć uświadamiających. Kwestie bezpieczeństwa cyfrowego powinny zostać wpisane w stały harmonogram przedsięwzięć szkoły i być poruszane np. w czasie zebrania całej szkolnej społeczności, podczas tzw. apelu szkolnego, lekcji wychowawczej czy organizacji szkolnego dnia bezpieczeństwa cyfrowego. Zaangażowanie dzieci i młodzieży w dyskusje oraz działania w tym zakresie pozytywnie wpływają na środowisko uczniowskie, pobudzając poczucie współodpowiedzialności za bezpieczeństwo cyfrowe szkoły (Paprotny 2022, s. 171). W związku z tym należy także wspierać wspomniany już wcześniej rozwój kompetencji kadry pedagogicznej. Szkolenia dla nauczycieli w zakresie przeciwdziałania negatywnym zjawiskom w cyberprzestrzeni, których ofiarami mogą stać się ich podopieczni, powinny mieć charakter wielopłaszczyznowy i obejmować swoim zakresem między innymi:

- rozwijanie kompetencji cyfrowych w celu zwiększenia świadomości na temat urządzeń oraz usług wykorzystywanych przez uczniów, a także korzystania z rozwiązań nowoczesnych technologii w edukacji;
- poszerzanie i aktualizowanie wiedzy na temat cyberbezpieczeństwa poprzez udział w konferencjach, webinarach, seminariach organizowanych dla opiekunów i nauczycieli (Lizut i Wrońska, 2018)

Mimo mnogości rozwiązań, które oferuje pozytywna profilaktyka, dzieci i młodzież w codziennym użytkowaniu mediów cyfrowych spotykają się z różnego rodzaju cyberzagrożeniami. Aby zminimalizować ich negatywne oddziaływanie należy szybko i efektywnie reagować. Uzupełnienie działań profilaktycznych w tym zakresie stanowi wypracowanie procedur postępowania w przypadku incydentów dotyczących aktywności uczniów w sieci oraz powołanie z kadry pedagogicznej osoby odpowiedzialnej za nadzór nad wdrożeniem i przestrzeganiem tychże procedur.

Szkolna procedura reagowania na zagrożenia związane z patostreamingiem

Procedury reagowania na wypadek wystąpienia incydentów zagrażających cyberbezpieczeństwu w środowisku uczniowskim są kluczowym elementem szkolnej strategii bezpieczeństwa, której opracowanie i wdrożenie stanowi podstawową rekomendację Ministerstwa Edukacji i Nauki w zakresie zapewnienia cyberbezpieczeństwa uczniom. Działania placówki oświatowej w sytuacji wystąpienia jakiegokolwiek zdarzenia w przestrzeni wirtualnej, mającego negatywny wpływ na poziom bezpieczeństwa uczniów, powinny charakteryzować się otwartością w celu szybkiej i właściwej identyfikacji problemu oraz adekwatnością reakcji w stosunku do poziomu zagrożenia. Opracowanie tzw. szkolnej procedury postępowania zapewnia optymalizację działań interwencyjnych, na które składają się działania wobec: aktu lub zdarzenia, uczestników zdarzenia oraz instytucji, organizacji, służb pomocowych i współpracujących m.in. policji, podmiotów wymiaru sprawiedliwości i służb społecznych (Lizut i Wrońska, 2018). Działania wobec aktu/zdarzenia obejmują swoim zakresem pozyskanie informacji na temat wystąpienia incydentu, przyjęcie zgłoszenia o incydencie, ustalenie okoliczności jego wystąpienia, analizę zdarzenia, zabezpieczenie dowodów oraz stworzenie dokumentacji i monitoringu pointerwencyjnego. Każde zgłoszenie powinno zostać zarejestrowane, przeanalizowane, a także odpowiednio udokumentowane. Dowodem w sprawie mogą być wiadomości e-mail, SMS-y i MMS-y, bilingi rozmów, wiadomości nagrane na pocztę głosową, zrzuty ekranu. Zgromadzony materiał stanowiący dowód wystąpienia incydentu zagrożenia bezpieczeństwu online powinien zostać zabezpieczony i opisany, a w sytuacji pojawienia się przesłanek świadczących o możliwości naruszenia prawa przekazany odpowiednim organom ścigania. Kolejnym elementem procedury są działania podejmowane wobec uczestników zdarzenia: osób poszkodowanych, sprawców i świadków zdarzenia. Na tym etapie, ze względu na niepełnoletność uczestników zdarzenia, należy uwzględnić rolę uczestniczącą rodziców/opiekunów prawnych. Zgodnie z rekomendacjami MEiN kolejność działań podejmowanych wobec uczestników incydentu to: rozmowa z poszczególnymi uczestnikami adekwatna do charakteru zdarzenia i ich roli, powiadomienie rodziców/opiekunów prawnych uczestników zdarzenia, poinformowanie o przewidzianych konsekwencjach, a także przedstawienie propozycji wsparcia i pomocy; zastosowanie konsekwencji regulaminowych wobec zidentyfikowanego sprawcy i prowadzenie działań wychowawczych, otoczenie opieką psychologiczno-pedagogiczną wszystkich uczestników zdarzenia. Jeśli występuje podejrzenie naruszenia przepisów prawa, dyrekcja szkoły ma obowiązek powiadomić o zdarzeniu organy ścigania (Paprotny 2022, ss. 179–181).

Rekomendacje w zakresie opracowania i wdrożenia procedur interwencyjnych są jedynie wskazówkami dla dyrekcji szkół, które powinny przygotować modele interwencyjne dla poszczególnych cyberzagrożeń, uwzględniając przy tym specyfikę danego środowiska szkolnego, w tym zdiagnozowane wcześniej problemy uczniów w obszarze

cyberbezpieczeństwa. Z uwagi na to, że dostęp dzieci i młodzieży do treści prezentowanych podczas patostreamów jest stosunkowo nowym wyzwaniem w zakresie zapewnienia bezpieczeństwa w wymiarze cyfrowym, opracowanie procedury interwencyjnej placówki oświatowej na zagrożenia związane z patostreamingiem jest zadaniem wymagającym rozpoznania potrzeb uczniów w tym zakresie, a także zdefiniowania metod, narzędzi i sposobów podejmowania efektywnych działań. Procedura reagowania na incydenty cyberbezpieczeństwa z udziałem uczniów składa się z następujących części:

- nazwa procedury,
- podstawa prawna,
- definicja zagrożenia objętego procedurą,
- opis poszczególnych działań podjętych w przypadku wystąpienia zagrożenia, w tym pozyskanie informacji i przyjęcie zgłoszenia o incydencie, ustalenie okoliczności zdarzenia, analiza zdarzenia, zebranie i zabezpieczenie dowodów, identyfikacja sprawców, działania wobec uczestników incydentu, współpraca z instytucjami/organizacjami/służbami pomocowymi i współpracującymi, sporządzenie dokumentacji ze zdarzenia oraz wprowadzenie monitoringu pointerwencyjnego (Lizut i Wrońska, 2018).

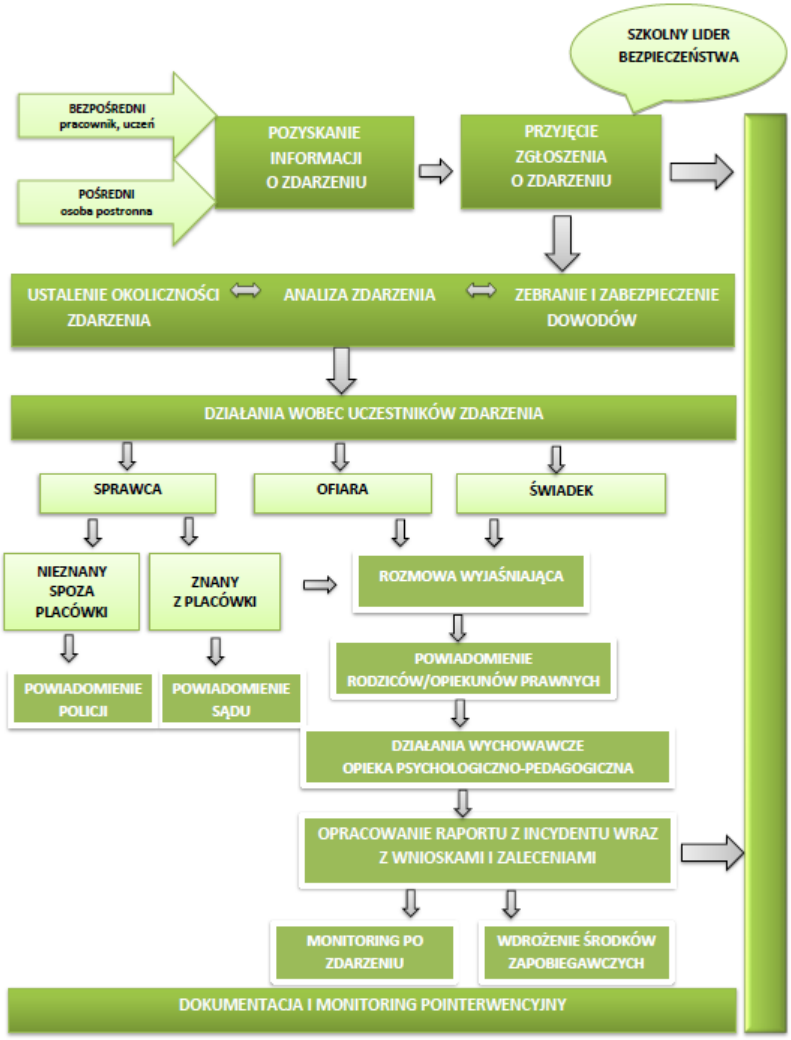
Istotą prawidłowego wdrożenia procedury jest właściwe zdefiniowanie zagrożenia i syntetyczne przedstawienie potencjalnych skutków jego oddziaływania na uczniów. Jak wskazano już w artykule, patostreaming jest zjawiskiem złożonym, które ewoluuje, dlatego jego definicja przyjęta w procedurze powinna być stale aktualizowana, tak aby zapewnić zasadność i efektywność dalszych działań określonych w stosunku do zdarzenia z udziałem dzieci i młodzieży. W kontekście podejmowanych działań wobec uczestników incydentu związanego z dostępem do patostreamów kluczową rolę odgrywa analiza zdarzenia, a także zebranie i zabezpieczenie dowodów. Jest to konieczne dla właściwego sklasyfikowania uczestników zdarzenia w kategoriach osób poszkodowanych, sprawców oraz świadków. Bez względu na rolę, jaką w zdarzeniu odgrywają podopieczni danej placówki oświatowej, szkoła zobowiązana jest otoczyć wszystkich uczestników incydentu opieką psychologiczno-pedagogiczną a także poinformować o ich udziale w zdarzeniu rodziców i opiekunów prawnych. Istotnym elementem działań wobec uczestników zdarzenia jest pouczenie o szkodliwości patostreamów i możliwościach wystąpienia negatywnych skutków rozpowszechniania tego rodzaju treści oraz odpowiedzialności karnej w przypadku prezentowania i rozpowszechniania materiałów nielegalnych. W przypadku gdy to uczeń jest odpowiedzialny za nadawanie materiałów, które można sklasyfikować jako patostreaming i które spełniają kryteria demoralizujących zachowań, należy wyciągnąć konsekwencje przewidziane w regulaminie szkoły i szkolnej strategii zapewnienia bezpieczeństwa cyfrowego, a także powiadomić odpowiednie organy, tj. sąd rodzinny i policję (Paprotny 2022, s. 180). Ze względu na szkodliwość treści prezentowanych podczas patostreamów, które mogą naruszać dobra podopiecznych szkoły, dyrekcja może zwrócić się do administratora strony internetowej, za pośrednictwem której uczniowie

mieli dostęp do materiałów, w celu usunięcia patostreamów, zablokowania kont patostreamerów, a także wprowadzenia ograniczeń wiekowych w dostępie do materiałów. W przypadku podejrzenia popełnienia czynu karalnego w związku z incydentem zagrożenia bezpieczeństwa w postaci dostępu dzieci i młodzieży do treści prezentowanych podczas patostreamów dyrekcja szkoły jest zobowiązana do zgłoszenia zdarzenia na policję. Z całości podjętych działań szkoła zobowiązana jest prowadzić dokumentację i monitoring pointerwencyjny. Powinno się to odbywać z poszanowaniem prywatności uczestników incydentu zagrażającego bezpieczeństwu oraz zachowaniem poufności przechowywanych i przetwarzanych danych. Działanie takie ma na celu zapewnienie ochrony uczestnikom zdarzenia, zarówno ofiarom i świadkom zdarzenia, jak i sprawcom naruszenia bezpieczeństwa przed stygmatyzacją w środowisku uczniowskim.

Graficzne zobrazowanie procedury interwencyjnej, której zastosowanie powinno mieć miejsce w przypadku wystąpienia zagrożenia patostreamingiem w środowisku uczniowskim przedstawia rysunek nr 1.

Rysunek 1

Procedura interwencyjna w przypadku wystąpienia zagrożenia patostreamingiem



Źródło: A. Paprotny, *Bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni: zagrożenie patostreamingiem*, Akademia Wojsk Lądowych im. gen. Tadeusz Kościuszki, s. 183.

Zakończenie

Podsumowując wyniki prowadzonych badań w zakresie roli i znaczenia szkoły jako środowiska kształtowania bezpieczeństwa cyfrowego dzieci i młodzieży w kontekście zagrożenia patostreamingiem, należy wskazać, że środowisko szkolne obok środowiska rodzinnego jest jednym z kluczowych dla kształtowania bezpiecznych postaw i zachowań

niepełnoletnich użytkowników Internetu. Szkoła jako placówka oświatowa została zobowiązana do prowadzenia szkolnej strategii cyberbezpieczeństwa, której kluczowymi elementami są działania profilaktyczne, a także procedury reagowania na cyberzagrożenia występujące w środowisku uczniowskim. Właściwe realizowana szkolna strategia bezpieczeństwa w wymiarze cyfrowym pozwala kształtować wśród najmłodszej grupy internautów konstruktywne sposoby korzystania z sieci, a także buduje poczucie odpowiedzialności dzieci i młodzieży za aktywności podejmowane w cyberprzestrzeni.

BIBLIOGRAFIA

Lange, R. (red.). (2021). *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów*. Warszawa.

Lizut, J., Wrońska, A. (red.). (2018). *Standard bezpieczeństwa online placówek oświatowych*. Ministerstwo Cyfryzacji.

Paprotny, A. (2022). *Bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni: zagrożenie patostreamingiem*. Akademia Wojsk Lądowych im. generała Tadeusz Kościuszki.

Piechna, J. (2019). *Szkodliwe treści w Internecie. Nie akceptuję, reaguję! Poradnik dla rodziców*. NASK Państwowy Instytut Badawczy.

Pyżalski, J. (2019). Elektroniczna przemoc rówieśnicza (cyberprzemoc). W: J. Pyżalski, A. Zdrodowska, Ł. Tomczyk, K. Abramczuk, Pol*skie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski*. https://fundacja.orange.pl/files/user_files/EU_Kids_Online_2019_v2.pdf.

Pyżalski, J. Zdrodowska, A. Tomczyk, Ł. Abramczuk, K. (2019). *Polskie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski*. https://doi.org/10.14746/amup.9788323234098

Rigamonti, M. (2019). *Porno, bijatyki i pijatyki. Dlaczego bycie patostreamerem jest pociągające? [WYWIAD]*. Pobrane z: https://forsal.pl/artykuly/1420578,porno-bijatyki-i-pijatyki--dlaczego-byciepatostreamerem-jest-pociagajace-wywiad.html.

Rozporządzenie Ministra Edukacji Narodowej z dnia 30 maja 2014 r. zmieniające rozporządzenie w sprawie podstawy programowej wychowania przedszkolnego oraz kształcenia ogólnego w poszczególnych typach szkół (Dz.U. 2014, poz. 803).

Rywaczyńska, A., Wójcik, Sz. (red.). (2018). *Bezpieczeństwo dzieci i młodzieży online. Kompendium dla rodziców i profesjonalistów*. Polskie Centrum Programu Safer Internet.

Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2017 r. poz. 59).

Wojtasik, Ł. (2019). Problem szkodliwych treści w Internecie a zjawisko patotreści. W: S. Wójcik, Ł. Wojtasik (red.), *Patotreści w Internecie. Raport o problemie* (5–7). Fundacja Dajemy Dzieciom Siłę.

Wojtyna, M. (2019). Nuda, dymy, podmiotowość: patostream jako gatunek. *Tekstualia*, *3*(58), 55–70. https://doi.org/10.5604/01.3001.0013.6423

Wójcik, S., Wojtasik, Ł. (red.). (2019). *Patotreści w Internecie. Raport o proble*mie. Fundacja Dajemy Dzieciom Siłę.