Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.72.2025
Warszawa, 07 lipca 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 23 kwietnia br. Posłanki na Sejm RP Pani Olgi Ewy Semeniuk – Patkowskiej w sprawie braku systemowego wsparcia dla szkół w zakresie cyberbezpieczeństwa i ochrony przed cyberprzemocą (interpelacja nr 9395)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłanki pytania.

Ad 1) Czy Ministerstwo Cyfryzacji planuje stworzenie systemowego programu wsparcia dla szkół w zakresie cyberbezpieczeństwa, który obejmowałby zarówno infrastrukturę, jak i szkolenia dla kadry?

Na początku należ zaznaczyć, że prowadzenie polityki państwa w obszarze oświaty i wychowania znajduje się w kompetencjach Ministerstwa Edukacji Narodowej. Niezależnie jednak rozwój kompetencji cyfrowych, w tym z obszaru cyberbezpieczeństwa całego społeczeństwa jest jednym z priorytetów Ministerstwa Cyfryzacji. Jednym ze sztandarowych przedsięwzięć, które odpowiadają na potrzeby i wyzwania współczesnej szkoły jest projekt pn. Ogólnopolska Sieć Edukacyjna (OSE), który jest realizowany na mocy ustawy o Ogólnopolskiej Sieci Edukacyjnej[1]. OSE to kluczowy projekt z punktu widzenia modernizacji polskiej szkoły, który kształtuje kompetencje cyfrowe dzieci i młodzieży. OSE jest wirtualną, publiczną siecią telekomunikacyjną, która daje szkołom dostęp do szybkiego, bezpłatnego i bezpiecznego internetu. Do programu przystąpiło 20,5 tys. szkół – zarówno z dużych miast, jak i mniejszych miejscowości. Tym samym placówki te uzyskały równe szanse i możliwości techniczne, by realizować swoje obowiązki edukacyjne z wykorzystaniem bezpiecznych narzędzi cyfrowych.

OSE, oprócz szybkiego, bezpłatnego dostępu do sieci, zapewnia także dostęp do profesjonalnych usług bezpieczeństwa teleinformatycznego – podstawowych i zaawansowanych. Chronią one użytkowników przed szkodliwym oprogramowaniem, wykrywają i blokują wirusy komputerowe oraz ataki sieciowe.

- Bezpieczny Internet OSE - to usługa, która jest aktywna w każdej szkole podłączonej do OSE. Zapewnia zabezpieczenie sieci i jej użytkowników przed dostępem do treści potencjalnie szkodliwych, szkodliwym oprogramowaniem, atakami sieciowymi oraz wirusami na poziomie podstawowym.
- OSE plus - to pakiet usług bezpieczeństwa składających się na zaawansowany poziom ochrony użytkowników sieci szkolnej. W skład pakietu wchodzą:
  - Ochrona przed szkodliwym oprogramowaniem - usługa monitoruje, wykrywa i blokuje wirusy komputerowe podczas przeglądania stron internetowych czy pobierania plików z sieci. Dodatkowo zapewnia ochronę przed zaawansowanymi atakami sieciowymi oraz blokuje transmisję szkodliwego oprogramowania na poziomie sieci OSE. W ramach tej usługi dyrektorowi szkoły udostępniane są raporty zawierające dane o wykrytych zagrożeniach.

[1] Ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej (Dz.U. z 2024 r. poz. 1768)

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

- Ochrona użytkowników OSE -to bezpłatna usługa, która chroni przed dostępem do stron zawierających treści potencjalnie szkodliwe i nielegalne, w tym materiały pornograficzne czy pokazujące agresję i przemoc. W ramach tej usługi dyrektorowi szkoły udostępniane są raporty zawierające dane o wykrytych potencjalnych zagrożeniach.
- Bezpieczne treści - usługa pozwala na uzyskanie informacji o trendach związanych z dostępem do treści potencjalnie szkodliwych w sieci szkolnej. Dzięki algorytmom uczenia maszynowego (ML), klasyfikuje materiały, z którymi zetknęli się użytkownicy (teksty, obrazy, wideo) i przypisuje je do odpowiednich kategorii. W ramach tej usługi dyrektorowi szkoły udostępniane są raporty zawierające dane o wykrytych potencjalnych zagrożeniach.

Sieć OSE jest również chroniona przez mechanizmy detekcji i mitygacji ataków typu DDoS, które w ostatnich latach przybrały na sile. Poszczególne elementy architektury sieci są monitorowane 24/7 przez zespoły NSOC (Security Operation Center).

Ponadto, Ministerstwo Cyfryzacji prowadzi działania wspierające edukację o bezpieczeństwie online wśród dzieci i młodzieży oraz kadry pedagogicznej. Jednym z takich projektów są Cyberlekcje. Projekt, który szerzej został opisany w odpowiedzi na pyt. 3 adresowany jest do nauczycieli i pedagogów chcących podczas swoich zajęć przekazywać dzieciom i młodzieży zasady i wskazówki dotyczące bezpiecznego poruszania się w internecie. O Cyberlekcjach więcej w odpowiedzi na pytanie nr 3.

Ad 2) Czy resort prowadzi obecnie monitoring incydentów cyberbezpieczeństwa w sektorze edukacji? Jeśli tak – ile takich incydentów zostało zgłoszonych w ostatnich 12 miesiącach?

Monitoring incydentów cyberbezpieczeństwa w sektorze edukacji prowadzony jest przez CSIRT NASK[2]. W 2024 r. liczba incydentów w sektorze Oświata i wychowania[3] (oznaczenie sektora wg. wewnętrznej klasyfikacji CSIRT NASK) wyniosła 733 incydentów (co stanowi 0,7% ogólnej liczby incydentów w 2024 r.).

Ad 3) Czy planowane jest wdrożenie dedykowanego komponentu „cyberedukacji" w ramach podstawy programowej lub jako odrębnego modułu zajęć w szkołach?

Jak zostało już wspomniane w odp. na pyt. 1, za politykę edukacyjną w Polsce odpowiada Ministerstwo Edukacji Narodowej. Ministerstwo Cyfryzacji natomiast prowadzi działania wspierające rozwój umiejętności cyfrowych, ze szczególnie położnym akcentem na wspieranie uczniów i nauczycieli w zakresie bezpiecznego poruszania się w cyfrowym środowisku oraz krytycznej analizy informacji dostępnych w internecie. Co istotne, „Wspieranie rozwoju umiejętności cyfrowych uczniów i nauczycieli, ze szczególnym uwzględnieniem bezpiecznego poruszania się w sieci oraz krytycznej analizy informacji dostępnych w Internecie. Poprawne metodycznie wykorzystywanie przez nauczycieli narzędzi i materiałów dostępnych w sieci, w szczególności opartych na sztucznej inteligencji, korzystanie z zasobów Zintegrowanej Platformy Edukacyjnej" jest jednym z celów Podstawowych kierunków realizacji polityki oświatowej państwa w roku szkolnym 2024/2025. Polityka ta stanowi podstawę do planowania przez organy nadzoru

[2] CSIRT NASK - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego poziomu krajowego. Obowiązki CSIRT NASK, o których mowa w ustawie z dn. 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077) zostały powierzone zespołowi CERT Polska funkcjonującego w strukturze NASK-PIB nadzorowanego przez Ministra Cyfryzacji.
[3] Należy jednak podkreślić, że monitoring CSIRT NASK obejmują cały system oświaty i wychowania, tj. przedszkola, szkoły podstawowe i ponadpodstawowe, zespoły szkół, ośrodki wychowawcze, biblioteki, a także uczelnie (260 zgłoszonych incydentów).

pedagogicznego, a także placówki doskonalenia nauczycieli, działań w danym roku szkolnym.

Tematyka przestrzegania zasad bezpieczeństwa podczas korzystania z narzędzi cyfrowych została uwzględniona w podstawach programowych dla szkół podstawowych[4] i ponadpodstawowych[5].

Niezależnie od powyższego, Ministerstwo Cyfryzacji inicjuje i realizuje projekty w zakresie cyberedukacji. Jednym z takich projektów są wspomniane w odp. na pyt. 1 Cyberlekcje. Realizacja tego zadania została powierzona NASK-PIB. W ramach projektu Cyberlekcje powstały już 22 gotowe scenariusze zajęć lekcyjnych o cyberbezpieczeństwie dostosowane do grup wiekowych uczniów w szkołach podstawowych i ponadpodstawowych. Scenariusze, to gotowe narzędzia wspomagające nauczycieli w kompleksowym edukowaniu o bezpieczeństwie online. Scenariusze obejmują różne tematy, takie jak: bezpieczeństwo online, prywatność, relacje w sieci, zagrożenia online, zarządzanie danymi, nadużywanie nowych technologii i dobrostan psychiczny. W ramach projektu powstały również dodatkowe materiały, jak: infografiki, prezentacje, animacje oraz filmy z ekspertami. W 2024 r. zrealizowano pilotażowo kolejną odsłonę projektu Cyberlekcje 3.0, w której wszystkie scenariusze przystosowano do metodologii nauczania PBL (ang. *Problem-Based Learning*), mającą na celu m.in. upowszechnienie przygotowanych materiałów w latach poprzednich, poprzez bezpośredni kontakt z pedagogami.

W ramach pilotażu zrealizowano:

- 7 całodniowych szkoleń dla nauczycieli z zakresu cyberbezpieczeństwa w miastach województwa mazowieckiego (Warszawa, Radom, Płock, Siedlce, Pruszków, Maków Mazowiecki oraz Mława);
- 2-godzinne szkolenia w placówkach oświatowych dla kadry pedagogicznej;
- Lekcje pokazowe dla uczniów szkół podstawowych i ponadpodstawowych;
- 4 nowe scenariusze (2 dla klas I-III oraz 2 dla klas IV-VI).

Przeprowadzone w 2024 r. przez NASK-PIB pilotażowe szkolenia kadry pedagogicznej oraz lekcje pokazowe na bazie scenariuszy Cyberlekcji 3.0, wskazały na dużą potrzebę kontynuacji projektu na terenie całej Polski, a także rozszerzenie jego zakresu o nowe scenariusze.

Realizacja projektu w latach 2025/2026 obejmie:

1. 2-dniowe szkolenia dla dyrektorów oraz kadry pedagogicznej szkolnych placówek podstawowych i ponadpodstawowych.
2. Zajęcia bazujące na scenariuszach Cyberlekcji dla uczniów szkół podstawowych i ponadpodstawowych wraz ze szkoleniem dla kadry pedagogicznej oraz rodziców/opiekunów w placówkach, które zgłoszą potrzebę przeprowadzenia szkoleń w różnych regionach Polski.
3. Przeprowadzenie ogólnodostępnych lekcji online bazujących na scenariuszach Cyberlekcji dla uczniów szkół podstawowych i ponadpodstawowych: 22 w roku 2025 oraz 30 w roku 2026.
4. Opracowanie 15 nowych scenariuszy Cyberlekcji (nowe tematy to m.in. Sztuczna inteligencja w codziennym życiu, Cyberprzemoc, Dezinformacja).

W projekcie przyjęto, że w ramach szkoleń stacjonarnych w latach 2025-2026 przeszkolonych zostanie 1125 dyrektorów, 3450 nauczycieli i minimum 2400 uczniów.

[4] https://www.podstawaprogramowa.pl/Szkola-podstawowa-IV-VIII-1/Informatyka
[5] https://www.podstawaprogramowa.pl/Liceum-technikum/Informatyka

Kompletne materiały są dostępne do pobrania w powszechnie dostępnej bazie wiedzy cyberbezpieczeństwa na portalu gov.pl w zakładce CyberEdukacja, a także w Zintegrowanej Platformie Edukacyjnej, narzędziu prowadzonym przez Ministerstwo Edukacji Narodowej.

Kolejną inicjatywą z zakresu cyberedukacji realizowaną przez Ministerstwo Cyfryzacji we współpracy z NASK -PIB jest projekt „Bezpieczni w sieci" Stworzona w ramach projektu platforma zawiera treści edukacyjne promujące cyberbezpieczeństwo. Nauczyciele i uczniowie klas 7–8 szkół podstawowych i szkół ponadpodstawowych mogą korzystać łącznie z 24 e-kursów w 8 modułach (Cyberprzemoc, Cyberzagrożenia, Cyfrowe ślady i wizerunek online, Fake news, Nielegalne i szkodliwe treści w internecie, Prywatność w cyfrowym świecie, Cyfrowa higiena, nadużywanie internetu oraz nowych technologii oraz Bezpiecznie w grach Cyfrowych). Dodatkowo, na platformie znajdują się materiały pomocnicze – poradniki zawierające scenariusze lekcji, które ułatwią nauczycielom przeprowadzanie zajęć. Uczniowie i nauczyciele po zakończeniu poszczególnych modułów i uzyskaniu pozytywnego wyniku w teście sprawdzającym mają możliwość uzyskania certyfikatów.

Ponadto, ramach opisanego już w odp. na pyt.1 projektu OSE, prowadzone są także działania uzupełniające, jak na przykład kampania OSEhero. Ma ona na celu wspieranie oraz promocję aktywnych nauczycieli, a także rozwój nauczania z zastosowaniem cyfrowych narzędzi. Kolejnym takim dodatkowym działaniem jest OSE IT Szkoła[6], czyli platforma edukacyjna dla nauczycieli i uczniów, z dostępem do bezpłatnych materiałów i kursów e-learningowych. Obecnie na platformie dostępnych jest kilkaset kursów m.in. z zakresu: bezpieczeństwa w sieci, sztucznej inteligencji, programowania, sieci komputerowych i technologii internetowych.

Ad 4) Czy Ministerstwo współpracuje z NASK lub innymi instytucjami państwowymi w celu stworzenia centralnej „tarczy cyfrowej" chroniącej szkoły przed atakami z zewnątrz?

NASK-PIB jako instytucja nadzorowana, realizuje zadania publiczne powierzone przez Ministra Cyfryzacji. Jednym z takich zadań jest wspomniany wyżej projekt OSE. Ponadto, NASK-PIB odgrywa bardzo istotną rolę w tworzeniu i realizowaniu licznych programów, projektów i kampanii edukacyjnych dla dzieci i młodzieży na każdym etapie kształcenia. Działania profilaktyczne są realizowane m.in w ramach projektu Cyberprofilaktyki, której celem jest zapewnienie dzieciom bezpiecznych doświadczeń cyfrowych poprzez ochronę przed zagrożeniami, wzmocnienie ich kompetencji niezbędnych do dokonywania właściwych wyborów i wyrażania opinii w środowisku internetowym w sposób bezpieczny i odpowiedzialny oraz zapewnianie im aktywnego uczestnictwa w kształtowaniu środowiska cyfrowego. Działalność Cyberprofilaktyki NASK obejmuje m.in szkolenia, webinaria, wykłady, konferencje, opracowywanie i publikowanie materiałów edukacyjnych (infografiki, poradniki, raporty, artykuły, filmy), czy prowadzenie kampanii informacyjno-edukacyjnych.

Na podstawie ustawy o Ogólnopolskiej Sieci Edukacyjnej wszystkie szkoły w Polsce mogą korzystać z usług OSE, do których należy m.in. bezpłatny dostęp do internetu o symetrycznej przepustowości co najmniej 100 Mb/s oraz bezpieczeństwo sieciowe i teleinformatyczne. Operatorem OSE jest Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy.

Usługi bezpieczeństwa sieciowego i teleinformatycznego obejmują:

1) ochronę przed szkodliwym oprogramowaniem - usługa monitoruje, wykrywa i blokuje wirusy komputerowe podczas przeglądania stron internetowych czy

[6] https://it-szkola.edu.pl/

pobierania plików z sieci. Dodatkowo zapewnia ochronę przed zaawansowanymi atakami sieciowymi oraz blokuje transmisję szkodliwego oprogramowania na poziomie sieci OSE. W ramach tej usługi dyrektorowi szkoły udostępniane są raporty zawierające dane o wykrytych zagrożeniach. Do poprawnego działania usługi niezbędna jest instalacja certyfikatów na wszystkich urządzeniach podłączonych do sieci OSE w szkole;

2) ochrona użytkowników OSE - usługa, która chroni przed dostępem do stron zawierających treści potencjalnie szkodliwe i nielegalne, w tym materiały pornograficzne czy pokazujące agresję i przemoc. W ramach tej usługi dyrektorowi szkoły udostępniane są raporty zawierające dane o wykrytych potencjalnych zagrożeniach. Do poprawnego działania usługi niezbędna jest instalacja certyfikatów na wszystkich urządzeniach podłączonych do sieci OSE w szkole;
3) bezpieczne treści - usługa pozwala na uzyskanie informacji o trendach związanych z dostępem do treści potencjalnie szkodliwych w sieci szkolnej. Dzięki algorytmom uczenia maszynowego (ML), klasyfikuje materiały, z którymi zetknęli się użytkownicy (teksty, obrazy, wideo) i przypisuje je do odpowiednich kategorii. W ramach tej usługi dyrektorowi szkoły udostępniane są raporty zawierające dane o wykrytych potencjalnych zagrożeniach. Usługa Bezpieczne treści jest aktywowana automatycznie we wszystkich szkołach, które korzystają z usługi Ochrona użytkowników OSE.

Bardziej szczegółowe informacje dostępne są na stronie internetowej usługi OSE.

Ministerstwo Cyfryzacji wspiera działania min. związane z przygotowaniem i przeprowadzeniem w szkołach podstawowych lekcji o tematyce cyfrowej higieny oraz bezpieczeństwa w sieci, poprzez wsparcie zadania „Higiena cyfrowa 2025" realizowanego przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (NASK-PIB).

Nadrzędnym celem projektu jest promowanie cyfrowej higieny jako kluczowego elementu kompetencji cyfrowych, niezbędnych we współczesnym społeczeństwie. Cyfrowa higiena to zbiór wiedzy, umiejętności i nawyków, które pozwalają na bezpieczne, świadome i zrównoważone korzystanie z urządzeń elektronicznych oraz technologii cyfrowych. Ma to kluczowe znaczenie dla zdrowia fizycznego i psychicznego, zwłaszcza dzieci i młodzieży, szczególnie narażonych na skutki nadmiernej ekspozycji na ekrany oraz zagrożenia płynące z internetu. Projekt koncentruje się na kształtowaniu trwałych postaw i umiejętności, które pomogą młodym ludziom unikać mechanizmów uzależniających i podejmować świadome decyzje dotyczące czasu spędzanego online.

Projekt zakłada realizację działań takich jak:

- promowanie higieny cyfrowej jako elementu zdrowego stylu życia,
- pokazywanie zależności pomiędzy zdrowym i zrównoważonym trybem życia a codziennym samopoczuciem i ogólną kondycją w zakresie korzystania z internetu,
- promowanie postaw poprawiających koncentrację, efektywność, poziom energii i zdrowy sen,
- przekazywanie wiedzy na temat bezpieczeństwa w sieci, m.in. cyberzagrożeń i dezinformacji.

Dodatkowo, w ramach zadania przygotowany zostanie film edukacyjny dla rodziców dzieci ze szkół podstawowych.

Projekt będący kontynuacją zadania zrealizowanego w 2024 r. i ma na celu dalsze rozwijanie kompetencji cyfrowych wśród dzieci i młodzieży. W oparciu o pozytywne wyniki zadania zrealizowanego w ubiegłym roku i wysokie zainteresowanie tematem

zarówno wśród uczniów, jak i nauczycieli, zasadnym jest kontynuowanie działań, które przyniosły wymierne efekty edukacyjne i społeczne.

Ad 5) Jakie działania zostały dotąd podjęte w kontekście rosnącej liczby deepfake'ów z udziałem nieletnich i czy resort planuje rozwiązania legislacyjne w tej sprawie?

Od pierwszego pojawienia się technologii umożliwiających tworzenie sztucznie wygenerowanych treści, określonych zbiorczo jako „deepfake" minęło już kilka lat. Ze względu na bardzo szybki postęp technologiczny i rozwój AI, obecnie narzędzia wykorzystujące sztuczną inteligencję są powszechnie dostępne i pozwalają na tworzenie takich materiałów niemal każdemu internaucie. Rozwój i dostępność AI to z pewnością wiele nowych możliwości, ale jednocześnie wyzwań związanych z szeroko pojętym bezpieczeństwem.

Dlatego, w ramach działań i kampanii informacyjno-edukacyjnych Ministerstwo Cyfryzacji wspólnie z NASK-PIB publikuje różnego rodzaju materiały edukacyjne dotyczących problematyki dezinformacji i deepfaków w formie:

- artykułów
  - Deepfaki - prawdziwy problem z fałszywą rzeczywistością;
  - Deepfake: Jak sztuczna inteligencja może nas oszukiwać?;
  - Czy to nagranie może kłamać? Uwaga na deepfake!;
  - Analiza i wykrywanie syntetycznych materiałów audiowizualnych – deepfake,
- webinarów
  - Jak rozpoznać deepfake? Ekspertka NASK odpowiada;
  - Cybertematycznie: webinarium o deepfake.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa