



JOANNA MAJCHRZYK-MIKUŁA

Piotrków Academy, Poland

ORCID iD: 0000-0003-2920-0447

JOANNA WERNER

Piotrków Academy, Poland

ORCID iD: 0000-0001-8107-7330

MAREK CENDROWSKI

Piotrków Academy, Poland

ORCID iD: 0000-0003-1610-0375

ŚWIADOMOŚĆ SPOŁECZNA I EDUKACJA DLA BEZPIECZEŃSTWA W KONTEKŚCIE CYBERZAGROZEŃ

SOCIAL AWARENESS AND EDUCATION FOR SECURITY IN THE CONTEXT OF CYBER THREATS

ABSTRACT

In a world dominated by artificial intelligence (AI) and autonomous systems, cyberattacks are no longer just technical problems, but a real threat to our society and everyday life. Modern image and sound manipulation techniques have made cybersecurity a challenge that affects the very foundations of social functioning. The transfer of a significant part of our lives to the online sphere means more intense activity on the part of cybercriminals, who are constantly testing the resilience of the banking sector, among others, to ever newer methods of attack. The aim of this article is to identify potential threats in cyberspace and to determine what educational measures and solutions should be applied to raise awareness of existing cyber threats. The basic method used in the preparation of the publication was a critical analysis and synthesis of the literature on the subject, which formed the basis for further analytical work. A key tool supporting the research process was an approach focused on comparison and analogy within individual categories of threats. The research process is complemented by logical reasoning, which allowed for the formulation of key conclusions. It is assumed that traditional education models must be replaced by dynamic adaptive education, which not only provides knowledge about tools, but also shapes lasting resilience to disinformation and cybercrime. Therefore, the decisive factor in increasing the resilience of the state is the education of network users, assuming the optimization of the teaching model. Extensive teaching activities and educational initiatives are an essential tool for minimizing digital risk and permanently strengthening users' defense skills.

KEYWORDS: education, security, cyber threats, risk, prevention

STRESZCZENIE

W świecie zdominowanym przez sztuczną inteligencję (AI) i systemy autonomiczne ataki w sieci to już nie tylko problemy techniczne, lecz także realne zagrożenie dla społeczeństwa i codziennego życia. Współczesne techniki manipulacji obrazem i dźwiękiem sprawiły, że cyberbezpieczeństwo stało się wyzwaniem dotyczącym samych podstaw społecznego funkcjonowania. Przeniesienie znacznej części naszego życia do sfery online oznacza intensywniejsze działania ze strony cyberprzestępców, którzy stale testują odporność m.in. sektora bankowego na coraz to nowsze metody ataków. Celem niniejszego artykułu jest wskazanie potencjalnych zagrożeń występujących w cyberprzestrzeni oraz określenie, jakie należy zastosować środki i rozwiązania edukacyjne, aby podnieść świadomość występujących cyberzagrożeń. Podstawową metodą wykorzystaną w przygotowywaniu publikacji była krytyczna analiza oraz synteza literatury przedmiotu, co stanowiło fundament dla dalszych prac analitycznych. Kluczowym narzędziem wspierającym

proces badawczy było porównywanie i szukanie analogii w obrębie poszczególnych kategorii zagrożeń. Dopełnieniem całości stało się wnioskowanie logiczne, które pozwoliło na sformułowanie kluczowych konkluzji. Zakłada się, że tradycyjne modele kształcenia muszą zostać zastąpione przez dynamiczną edukację adaptacyjną, która nie tylko dostarcza wiedzy o narzędziach, lecz także kształtuje trwałą odporność na dezinformację i cyberprzestępczość. W związku z powyższym, decydującym czynnikiem wzrostu odporności państwa jest edukacja użytkowników sieci przy założeniu optymalizacji modelu nauczania. Szeroko zakrojone działania dydaktyczne i inicjatywy edukacyjne są niezbędnym instrumentem minimalizowania ryzyka cyfrowego oraz trwałego wzmacniania kompetencji obronnych użytkowników.

SŁOWA KLUCZOWE: edukacja, bezpieczeństwo, cyberzagrożenia, ryzyko, profilaktyka

WPROWADZENIE

W świecie zdominowanym przez sztuczną inteligencję (AI) i systemy autonomiczne ataki w sieci to już nie tylko problemy techniczne, lecz także realne zagrożenie dla większości społeczeństwa i codziennego życia. Współczesne techniki manipulacji obrazem i dźwiękiem sprawiły, że cyberbezpieczeństwo stało się wyzwaniem dotyczącym samych podstaw społecznego funkcjonowania. Szybki rozwój cyfryzacji gospodarki i społeczeństwa stworzył nowe możliwości cyberataków. Kluczowe sektory, do których należy zaliczyć: zdrowie, finanse, energetykę, administrację publiczną i telekomunikację opierają się na sieciach i systemach informatycznych, które są ze sobą coraz bardziej wzajemnie powiązane. Cyberzagrożenia przybierają różnorodne formy i obejmują zarówno klasyczne, jak i coraz bardziej zaawansowane techniki ataków. Przeniesienie znacznej części naszego życia do sfery online oznacza intensywniejsze działania ze strony cyberprzestępców, którzy stale testują odporność m.in. sektora bankowego na coraz to nowsze metody ataków. Literatura przedmiotu jednoznacznie wskazuje, że techniczne środki ochrony pozostają niewystarczające bez odpowiedniego poziomu kapitału poznawczego użytkowników.

METODOLOGIA

Celem niniejszego artykułu jest wskazanie potencjalnych zagrożeń występujących w cyberprzestrzeni. Główny problem badawczy został sformułowany w następujący sposób: Jakie należy zastosować środki i rozwiązania edukacyjne, aby podnieść świadomość występujących cyberzagrożeń? Realizacji tak sformułowanego celu posłużyły następujące problemy badawcze:

1. Jak współzależność sieciowa warunkuje rozwój nowych cyberzagrożeń?
2. W jakim stopniu wykorzystanie sztucznej inteligencji do personalizacji ataków oraz ataki phishingowe wpływają na skuteczność wyłudzeń danych od klientów instytucji finansowych?
3. W jaki sposób uwzględnienie świadomości społecznej jako kluczowego elementu systemu zarządzania ryzykiem wpływa na ograniczenie współczesnych cyberzagrożeń?
4. Czy intensyfikacja innowacyjnej edukacji w zakresie cyberbezpieczeństwa przekłada się bezpośrednio na gotowość społeczeństwa do podejmowania odpowiednich działań w obliczu zaawansowanych cyberzagrożeń?

Podstawową metodą wykorzystaną w przygotowywaniu publikacji była analiza krytyczna oraz synteza literatury przedmiotu, co stanowiło fundament dla kolejnych etapów pracy. Decydującym narzędziem wspierającym proces badawczy było podejście nakierowane na porównanie i analogię w obrębie poszczególnych kategorii i rodzajów zagrożeń. Szczegółowe zdefiniowanie ich typów i rodzajów miało na celu dostarczenie niezbędnej wiedzy do efektywnego tworzenia programów edukacji dla bezpieczeństwa, jednocześnie umożliwiając ich realne wykorzystanie w scenariuszach ochrony. Zastosowanie tej procedury umożliwiło wyodrębnienie poszczególnych właściwości analizowanych zjawisk. Dopełnieniem procesu badawczego jest wnioskowanie logiczne, które pozwoliło na sformułowanie kluczowych konkluzji. Zakłada się, że tradycyjne modele kształcenia muszą zostać zastąpione przez dynamiczną edukację adaptacyjną, która nie tylko dostarcza wiedzy o narzędziach, lecz także kształtuje trwałą odporność na dezinformację i cyberprzestępczość.

EWOLUCJA CYBERZAGROZEŃ W WARUNKACH WSPÓŁCZESNEJ WSPÓŁZALEŻNOŚCI SIECIOWEJ

We współczesnym cyberbezpieczeństwie współzależność sieciowa (ang. *network interdependence*) oznacza sytuację, w której systemy informatyczne, infrastruktura krytyczna i procesy społeczne są ze sobą tak ściśle powiązane, że działanie jednego elementu jest całkowicie uzależnione od poprawności działania innych. Współczesna cyberprzestrzeń przestała być jedynie obszarem wymiany informacji, stając się newralgicznym środowiskiem funkcjonowania państw, gospodarek i jednostek. W obliczu wyzwań, z jakimi boryka się świat, cyberataki znacząco ewoluowały pod względem złożoności i oddziaływania. Wraz z szybkim postępem technologicznym oraz transformacją cyfrową ataki te stają się coraz bardziej zróżnicowane i innowacyjne, co czyni je poważnym zagrożeniem dla osób fizycznych, firm i rządów (Salman, Alsajri, 2023, s. 73). Integralna współzależność systemów sprawia, że tradycyjne zabezpieczenia technologiczne stają się nieskuteczne wobec ataków wymierzonych w człowieka jako najsłabsze ogniwo. Tradycyjna ochrona systemowa traci na znaczeniu, gdy w złożonej strukturze wzajemnych powiązań to użytkownik, a nie błąd w kodzie, staje się głównym obiektem ataków ze strony cyberprzestępców. Punktem wyjścia powyższych rozważań jest analiza relacji między zagrożeniami systemowymi a odpowiedzialnością indywidualną. W tym ujęciu błąd ludzki przestaje być jedynie incydentem marginalnym, a staje się czynnikiem sprawczym procesów o znacznie szerszym zasięgu.

Pojęcie zagrożeń w cyberprzestrzeni obejmuje celowe ataki nastawione na zdobycie informacji bez zezwolenia lub destabilizację i uszkodzenie infrastruktury cyfrowej. Jakiegokolwiek zdarzenie lub działanie może doprowadzić do zakłócenia ciągłości funkcjonowania przedsiębiorstwa, utraty danych lub naruszenia bezpieczeństwa systemów w wyniku zamierzonego ataku lub błędu. Wektory ataków w cyberprzestrzeni mają zróżnicowaną genezę, począwszy od zorganizowanych operacji prowadzonych przez wroga państwa, po incydenty wywoływane przez osoby z najbliższego otoczenia systemu. W tym ostatnim przypadku kluczowym wyzwaniem staje się nadużycie zaufania i uprawnień przez personel lub kontrahentów w celach przestępczych. Dla pełnego

zrozumienia dynamiki tych zjawisk niezbędne jest przedstawienie charakterystyki zagrożeń, ich pochodzenia i potencjalnych skutków. Opublikowana w październiku 2025 r. najnowsza edycja raportu Threat Landscape autorstwa Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) stanowi kompleksowe podsumowanie incydentów odnotowanych między lipcem 2024 r. a czerwcem 2025 r. W zdecydowanej większości przypadków działalność cyberprzestępców była inicjowana przez kampanie phishingowe, gdzie atakujący wysyła wiadomości e-mail, podszywając się pod zaufane źródło. Phishing często polega na wysyłaniu fałszywych wiadomości e-mail do jak największej liczby użytkowników, ale może być również bardziej ukierunkowany. Tego typu ataki stanowiły ok. 60% wszystkich infekcji. Wykorzystanie technicznych niedoskonałości systemów oraz luk w oprogramowaniu stanowiło metodę wyjściową dla 21% analizowanych ataków, botnety, czyli sieci zainfekowanych komputerów ok. 10%, a złośliwe aplikacje 8%. Dominującą kategorię incydentów stanowiły ataki typu DDoS, polegające na celowym generowaniu nadmiarowego ruchu w celu sparaliżowania dostępności serwisów i serwerów. Odpowiadały one za 76% wszystkich zdarzeń.

Znacznie rzadziej, bo w 18% przypadków, dochodziło do nieuprawnionej penetracji systemów informatycznych. Pozostałe 5% incydentów zostało sklasyfikowane jako zdarzenia o nieustalonej charakterystyce dalszych etapów operacji. Do głównych trendów w krajobrazie zagrożeń w 2025 r. należy również zaliczyć ataki ransomware, które pod względem skali konsekwencji pozostają bezkonkurencyjne. Przy tego typu atakach użytkownik lub organizacja zostają pozbawieni dostępu do własnych systemów lub danych poprzez szyfrowanie. Atakujący zazwyczaj żąda okupu w zamian za klucz deszyfrujący, lecz nie ma gwarancji, że zapłacenie okupu faktycznie przywróci pełny dostęp lub funkcjonalność. Wykorzystanie sztucznej inteligencji stanowiło punkt zwrotny w ewolucji zagrożeń. Wdrożenie jej, jako katalizatora rozwoju technologii, uznaje się za moment przełomowy procesów gospodarczych, społecznych i politycznych, choć należy mieć na uwadze, że w rękach cyberprzestępców i wrogich państw może ona jeszcze bardziej skomplikować naturę cyberbezpieczeństwa (Albrycht i in., 2019, s. 7). Rola AI w cyberprzestrzeni ewoluowała w stronę kompleksowego wsparcia działań ofensywnych, począwszy od typowania ofiar, przez generowanie malware,

aż po modyfikowanie strategii uderzenia w czasie rzeczywistym. Według raportów unijnych z 2025 r. większość kampanii wyłudzenia danych wykorzystywała już treści wygenerowane automatycznie, co znacząco podniosło ich wiarygodność.

Kluczowa jest tu analiza mechanizmów kaskadowego paraliżu, która dowodzi, że w erze całkowitej współzależności sieciowej to nie technologia, ale świadomość społeczna i systematyczna edukacja na rzecz bezpieczeństwa stanowią ostateczną barierę chroniącą państwo przed destabilizacją. Paraliż kaskadowy, często określany jako efekt domina w cyberbezpieczeństwie, jest definiowany jako proces, w którym pojedyncza awaria lub atak na jeden element sieci wywołuje sekwencję kolejnych incydentów w systemach zależnych. Prowadzi to do zakłócenia całego ekosystemu infrastruktury krytycznej państwa. Analiza ewolucji zagrożeń prowadzi do wniosku, że procesy te najsilniej uwidaczniają się w obszarach o najwyższym stopniu cyfryzacji i zaufania społecznego. W dobie globalnej informatyzacji, także sfery publicznej, w warunkach rozwoju portali społecznościowych, wszechobecnego mailingu, czyli wiadomości rozsyłanych na wiele adresów e-mail zgromadzonych w wielkich zasobach danych, często dochodzi do nieuprawnionych działań, które mogą stanowić naruszenie dóbr osobistych, prawa własności czy praw konsumenckich (Chałubińska-Jentkiewicz, 2025, s. 5). Szczególnym polem doświadczalnym dla współczesnych cyberzagrożeń są sektory finansowy i bankowy. To właśnie w tej sferze, będącej fundamentem współzależności ekonomicznej, najpełniej uwidacznia się symbioza ataków technicznych z socjotechniką, co zostanie poddane szczegółowej analizie. Ewolucja zagrożeń dowodzi, że powszechna cyfryzacja i budowanie relacji na zaufaniu zwiększają wrażliwość danego obszaru na cyberataki. Konieczność przeciwdziałania tak zdefiniowanym zagrożeniom znajduje swoje odzwierciedlenie w działaniach legislacyjnych na poziomie ponadnarodowym, gdyż obecnie Europa stoi w obliczu codziennych cyberataków i ataków hybrydowych na podstawowe usługi i instytucje demokratyczne, przeprowadzanych przez grupy państwowe i przestępcze. Komisja Europejska zaproponowała nowy pakiet dotyczący cyberbezpieczeństwa, aby jeszcze bardziej wzmocnić odporność i zdolności UE w zakresie cyberbezpieczeństwa w obliczu tych rosnących zagrożeń. Pakiet zawiera wniosek dotyczący zmienionego aktu o cyberbezpieczeństwie, który

zwiększa bezpieczeństwo unijnych łańcuchów dostaw technologii informacyjno-komunikacyjnych (ICT) (Komisja Europejska, 2026). Optymalizacja procesów certyfikacji sprawia, że produkty trafiające na rynek unijny zawierają wbudowane mechanizmy ochronne już od wczesnych faz projektowania, co realnie podnosi poziom bezpieczeństwa obywateli.

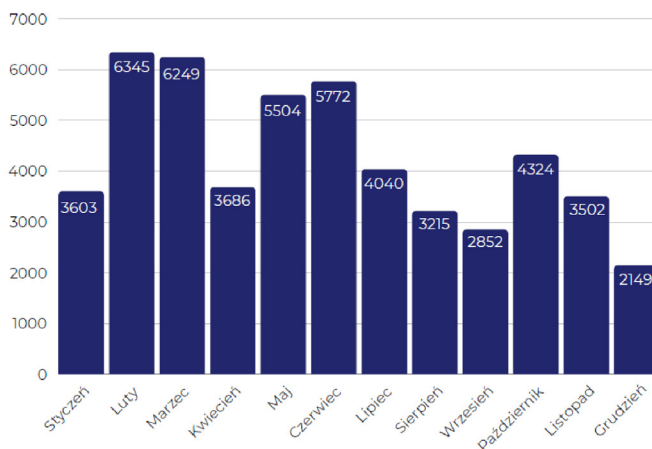
CYBERZAGROŻENIA SEKTORA FINANSOWEGO

Sektor finansowy ma strategiczne znaczenie dla funkcjonowania oraz stabilności kraju, co czyni go głównym celem ataków cyberprzestępców. Procesy zarządzania ryzykiem w bankowości muszą obecnie sprostać coraz to nowszym wyzwaniom, które bezpośrednio dotyczą klientów, codziennych użytkowników cyberprzestrzeni. Transformacja cyfrowa sprawiła, że obywatele stali się aktywnymi uczestnikami i osobami współodpowiedzialnymi za procesy autoryzacji transakcji, czyniąc z nich jednocześnie najsłabiej chronione ogniwo w łańcuchu bezpieczeństwa. Coraz większą skalę zagrożeń, z którymi mierzą się użytkownicy cyberprzestrzeni, ukazuje rosnąca liczba wykrywanych przez CSIRT KNF (Computer Security Incident Response Team Komisji Nadzoru Finansowego) domen phishingowych. Często zwraca się uwagę na wykorzystywanie w tej metodzie ataku socjotechniki. Ma ona na celu pozbawienie użytkowników czujności na występujące zagrożenie. Phishing to próba oszustwa, w której atakujący działa jako zaufana osoba lub podmiot w celu uzyskania poufnych informacji od użytkownika internetu. Ofiary ataków phishingowych stają się celem fałszywej korespondencji zawierającej złośliwe załączniki lub prowadzącej do precyzyjnie zaprojektowanych stron internetowych phishingowych (Gallo i in., 2024, s. 1–2). Potencjalna ofiara ataku bez wahania udostępnia swoje dane uwierzytelniające w odpowiednich polach, tym samym wpadając w pułapkę atakujących. Przestępcy śledzą te dane i wykorzystują je, aby uzyskać dostęp do właściwego konta użytkownika (Safi Singh, 2023, s. 590). Szczególnym rodzajem phishingu, który zdecydowanie jest uznawany za bardziej niebezpieczny, jest tzw. spear phishing. Atak ten ukierunkowany jest na konkretnego adresata. Ma on na celu wywarcie określonego wpływu lub wymuszenie działania w stosunku do odbiorcy. Cyberprzestępcy mogą podszywać się pod partnerów biznesowych, z którymi

adresat ataku współpracuje, za pomocą spersonalizowanej wiadomości. Przed realizacją ataku przestępcy zazwyczaj przeprowadzają szczegółowe rozpoznanie celu, analizując strukturę organizacji na podstawie informacji dostępnych np. w mediach społecznościowych.

Liczba zidentyfikowanych oszukańczych domen wzrosła z 17 200 w 2022 r. do 30 140 w 2023 r. oraz do 51 241 w 2024 r., co przedstawia wykres 1 i 2.

Wykres 1. Domeny zgłoszone do CSIRT NASK przez CSIRT KNF w 2024 r. w poszczególnych miesiącach

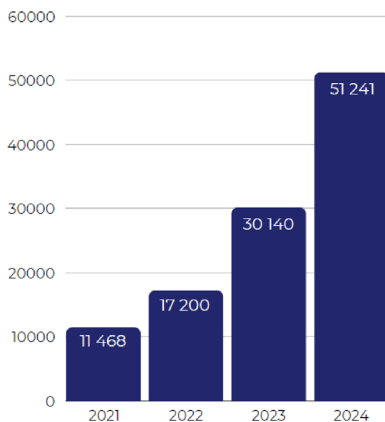


Źródło: raport roczny CSIRT KNF 2024, s. 9, https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_Roczny_CSIRT_KNF_2024_93226.pdf (dostęp: 2.09.2025).

Świat cyfrowy szybko się rozwija i ewoluuje, podobnie jak cyberprzestępcy, którzy polegają na nielegalnym wykorzystaniu zasobów cyfrowych. Phishing finansowy jest jednym z najpopularniejszych narzędzi wykorzystywanych przez cyberprzestępców oraz jedną z najczęstszych prób ataku na klientów bankowości elektronicznej. Atakujący, podszywając się pod pracowników banku w rozmowie telefonicznej, starają się ich nakłonić do udostępnienia wrażliwych informacji lub przelania środków finansowych na wskazane konto, co określane jest mianem voice phishingu. Dynamiczny rozwój sieci sprawił, że ludzie coraz częściej udostępniają swoje dane osobowe online. Masowe udostępnianie danych osobowych i transakcji finansowych sprawia,

że użytkownicy stają się łatwym celem dla hakerów. CSIRT KNF w 2024 r. zidentyfikował 175 domen związanych z oszustwami bankowymi.

Wykres 2. Liczba zgłoszonych przez CSIRT KNF domen phishingowych w latach 2021–2024



Źródło: raport roczny CSIRT KNF 2024, s. 10, https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_Roczny_CSIRT_KNF_2024_93226.pdf (dostęp: 2.09.2025).

Technologie oparte na sztucznej inteligencji pozwalają na przeprowadzanie kampanii phishingowych szybciej i łatwiej niż było to możliwe wcześniej. AI daje możliwość zastosowania poprawnej pisowni, a także wykorzystuje wiele taktyk manipulacyjnych, takich jak sugerowanie pilności lub wykorzystywanie informacji już udostępnionych online w celu zwiększenia trafności (Leyden, 2025). Szerokie spektrum możliwości wykorzystania i zastosowania sztucznej inteligencji do tworzenia przekonujących materiałów reklamowych, w tym szybkiego tworzenia stron internetowych, dodatkowo spotęgowało ten proceder. W miarę jak cyberprzestępcy doskonalą swoje umiejętności, zmieniają się również ich metody ataków phishingowych, a jedną z nich jest catphishing. Jest to podstępna taktyka, w której atakujący tworzą fałszywe postacie online w celu skłonienia użytkowników do lokowania kapitału, co w ostateczności umożliwia przestępcom przejęcie ich środków oraz wrażliwych informacji. Cyberprzestępcy coraz częściej wykorzystują generatywną sztuczną inteligencję do naśladowania stylu pisania, a nawet potrafią personalizować fałszywe

wiadomości e-mail na podstawie publicznie dostępnych danych. Podatność na phishing różni się u poszczególnych osób w zależności od ich zdolności postrzegawczych oraz poziomu świadomości. W związku z powyższym w większości ataków przestępcy wykorzystują ludzkie emocje i ich słabości do hakowania, zamiast wykorzystywać zaawansowane technologie. Wdrożenie kompleksowej strategii bezpieczeństwa i edukacja użytkowników usług bankowych oraz pracowników są kluczowymi elementami ochrony przed phishingiem również w środowisku biznesowym.

ŚWIADOMOŚĆ SPOŁECZNA W SYSTEMIE ZARZĄDZANIA RYZYKIEM

Świadomość społeczna w systemie zarządzania ryzykiem w cyberprzestrzeni ma charakter fundamentalny. Taki model działania pozwala na wyraźne przesunięcie punktu ciężkości z rozwiązań technologicznych na rzecz budowania odporności obywatelskiej w kontekście dynamicznie ewoluujących cyberzagrożeń. Nowoczesny model zarządzania ryzykiem cyfrowym powinien priorytetowo uwzględniać kapitał ludzki. Świadome zagrożenie społeczeństwo zmienia model ochrony z technologicznego na taki, w którym głównym ogniwem odporności jest użytkownik. W kontekście cyberzagrożeń świadomość można rozumieć jako gotowość do podejmowania działań w obliczu możliwych zdarzeń w przestrzeni internetu, jak również narzędzi cyfrowych. Przejawia się ona zdolnością do szybkiego rozpoznawania sytuacji zagrażającej, potencjalnie niebezpiecznej, jej oceny klasyfikowanej jako zagrażającej i prawidłowego reagowania w sytuacji jej doświadczenia (Siemieniecka, Grubicka, 2025, s. 99). Ludzie stali się najbardziej podatnym celem ataków, co wykorzystują cyberprzestępcy. W rezultacie zagrożenia są teraz skierowane głównie na osoby, a nie na systemy. Należy przy tym pamiętać, że klasycznie ryzyko w cyberprzestrzeni definiuje się jako miarę prawdopodobieństwa wystąpienia niepożądanych zjawisk w środowisku teleinformatycznym. Dotyczy ono podatności zasobów cyfrowych zarówno na czynniki zewnętrzne, jak wewnętrzne. Zagrażają one poufności, integralności oraz dostępności, generując tym samym ryzyko powstania dotkliwych strat po stronie firmy i osób prywatnych. Ryzyko stanowi nieodłączny element

naszego codziennego życia, wpływając również na funkcjonowanie sektora biznesowego oraz instytucji. W literaturze istnieje wiele różnych definicji ryzyka, z których większość koncentruje się na koncepcji niepewności lub prawdopodobieństwa wystąpienia niepożądanego zdarzenia. W kontekście biznesowym ryzyko jest nieodłącznie związane z działalnością każdej organizacji, a jego minimalizacja jest kluczowa dla zapewnienia stabilności i zrównoważonego rozwoju firmy (Kramarz, Korpysa, 2023, s. 4844). Wśród artykułów naukowych i publikacji eksperckich, które poddają analizie związek między świadomością społeczną a ryzykiem cyberzagrożeń, podkreśla się kluczową rolę czynnika ludzkiego w cyberbezpieczeństwie oraz stale rosnące znaczenie edukacji w obliczu zaawansowanych zagrożeń, także tych generowanych przez AI. Rozwój cyfryzacji stworzył przestępcom możliwość dostępu do wrażliwych danych obywateli, firm i instytucji. Jednak to nie ich nadmiar czy luki w technologii są kluczowym problemem. Prawdziwym wyzwaniem okazał się fakt, iż najskuteczniejszym narzędziem ataku stało się sterowanie ludzkim postrzeganiem rzeczywistości i wykorzystywanie ich słabości psychologicznych. Największego zagrożenia nie stanowi ani nadmiar informacji, ani trudności we wdrażaniu środków bezpieczeństwa, lecz zdolność do manipulowania ludzką percepcją (Stylianou i in., 2025, s. 1–2). Zarządzanie ryzykiem stanowi systematyczny proces identyfikacji, analizy, oceny i kontroli potencjalnych zagrożeń oraz szans. Mają one na celu zapewnienie stabilnych wyników, jak również ciągłości działania i realizacji celów organizacji, instytucji oraz osób prywatnych poprzez utrzymanie ryzyka na akceptowalnym poziomie. Proces ten obejmuje kluczowe etapy, takie jak: planowanie, identyfikacja zagrożeń, analiza jakościowa i ilościowa oraz monitorowanie ryzyka. Zarządzanie ryzykiem oraz zapewnienie bezpieczeństwa to komplementarne procesy, które dzięki szczegółowej analizie i ocenie zagrożeń minimalizują straty oraz umożliwiają podejmowanie świadomych, strategicznych decyzji (Damayanti, 2023, s. 1116–1117). Identyfikacja zagrożeń i podatności to nie tylko skanowanie systemów w poszukiwaniu luk w kodzie, lecz przede wszystkim zrozumienie, że największą podatnością jest ludzka percepcja. Cyberzagrożenia nie dotyczą tylko wirusów, ale obejmują one również zaawansowaną socjotechnikę wspieraną przez AI, np. deepfake, która celuje bezpośrednio w obywatela.

Tabela 1. Skala oceny ryzyka

Prawdopodobieństwo	Niskie: mało prawdopodobne, że ryzyko się zmaterializuje
	Średnie: możliwe, że ryzyko się zmaterializuje
	Wysokie: bardzo prawdopodobne, że ryzyko się zmaterializuje
Wpływ	Niski: minimalny wpływ na realizację celów KSC
	Średni: znaczący, ale zarządzalny wpływ na realizację celów KSC
	Wysoki: poważny wpływ na realizację celów KSC, mogący prowadzić do poważnych zakłóceń

Źródło: opracowanie własne na podstawie sprawozdania Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za rok 2024, <https://pliki.telepolis.pl/file/220984/original.pdf> (dostęp: 20.10.2025).

Tabela 2. Wybrane elementy matrycy oceny ryzyka dla Krajowego Systemu Cyberbezpieczeństwa

Ryzyko	Prawdopodobieństwo	Wpływ	Ocena ryzyka
Polityczne			
Zmiany legislacyjne	Wysokie	Wysokie	Wysokie
Geopolityczne napięcia	Wysokie	Wysokie	Wysokie
Polityka wewnętrzna	Niskie	Niskie	Niskie
Społeczne			
Świadomość społeczna	Wysokie	Wysokie	Wysokie
Zaufanie publiczne	Średnie	Średnie	Średnie
Edukacja	Średnie	Średnie	Średnie
Technologiczne			
Szybki rozwój technologii	Wysokie	Wysokie	Wysokie
Złożoność infrastruktury	Wysokie	Wysokie	Wysokie
Nowe zagrożenia	Wysokie	Wysokie	Wysokie
Prawne			
Zgodność z regulacjami	Wysokie	Wysokie	Średnie
Ochrona danych osobowych	Wysokie	Wysokie	Średnie
Sankcje	Średnie	Średnie	Niskie
Operacyjne			
Zarządzanie incydentami	Wysokie	Wysokie	Wysokie
Ciągłość działania	Wysokie	Wysokie	Wysokie
Bezpieczeństwo fizyczne	Średnie	Średnie	Średnie
Techniczne			
Wady systemów	Wysokie	Wysokie	Wysokie
Integracja systemów	Średnie	Średnie	Średnie
Zarządzanie aktualizacjami	Wysokie	Wysokie	Wysokie

Źródło: opracowanie własne na podstawie sprawozdania Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za rok 2024, <https://pliki.telepolis.pl/file/220984/original.pdf> (dostęp: 20.10.2025).

W sprawozdaniach rządowych z roku 2024 przedstawione zostały kluczowe inicjatywy i przedsięwzięcia oraz rekomendacje na kolejne lata, mające na celu dalsze wzmacnianie cyberbezpieczeństwa w Polsce. Przy opracowaniu skali i matrycy ryzyka dla Krajowego Systemu Cyberbezpieczeństwa (KSC) zastosowana została skala trzystopniowa, która obejmuje poziomy niskiego, średniego oraz wysokiego ryzyka (Tabela 1). Badania dotyczące *Postawy Polaków wobec cyberbezpieczeństwa* zrealizowane w 2024 r. na zlecenie Fundacji Warszawski Instytut Bankowości (WIB) dowodzą, iż 62% Polaków deklaruje, że czuje się bezpiecznie w świecie cyfrowym. Jest to jednak spadek w porównaniu z latami ubiegłymi, co świadczy o wzroście świadomości realnych zagrożeń. Matryca oceny ryzyka dla Krajowego Systemu Cyberbezpieczeństwa w sposób szczególnie uwzględnia ryzyko świadomości społecznej, co prezentuje poniższe zestawienie (Tabela 2).

W odniesieniu do świadomości społecznej ujętej w matrycy ryzyka KSC należy zwrócić uwagę, iż niski poziom świadomości na temat zagrożeń cyfrowych może w konsekwencji prowadzić do podejmowania niewłaściwych działań i zachowań użytkowników, co w rezultacie może przyczynić się do zwiększenia ryzyka incydentów bezpieczeństwa. Do potencjalnych skutków braku świadomości oraz wiedzy w tym obszarze należy zaliczyć wzrost liczby udanych cyberataków, utratę danych osobowych oraz finansowych, co przekłada się na zmniejszenie ogólnego poziomu bezpieczeństwa systemów informacyjnych. W celu zapobiegania oraz przeciwdziałania powyższym zagrożeniom wskazane jest wdrożenie kampanii edukacyjnych i informacyjnych na temat cyberbezpieczeństwa. Niezbędne są również regularne szkolenia dla obywateli i pracowników instytucji publicznych, budujące odporność oraz bezpieczne nawyki reagowania w sytuacjach zagrożeń. W celu zwiększenia świadomości społecznej bardzo istotnym elementem jest współpraca z mediami oraz dostosowanie przekazu do konkretnej grupy wiekowej odbiorców. Zaufanie publiczne, które zostało określone jako średnie, należy odczytywać jako brak pełnego zaufania do systemów cyfrowych oraz instytucji, które odpowiadają za cyberbezpieczeństwo. Jest to bardzo niepokojąca sytuacja, ponieważ z dużym prawdopodobieństwem może prowadzić do wielu wątpliwości i obaw dotyczących naruszenia prywatności oraz bezpieczeństwa danych, co w dalszej perspektywie może powodować niechęć do korzystania

z usług cyfrowych oraz nowych technologii. Za działania priorytetowe należy uznać wdrożenie przedsięwzięć mających na celu poprawę obecnego stanu poczucia bezpieczeństwa poprzez transparentną komunikację w zakresie cyberbezpieczeństwa oraz budowanie zaufania, przejawiającego się w szybkim i skutecznym reagowaniu na incydenty. Brak odpowiedniej edukacji w zakresie cyberbezpieczeństwa, która została określona jako średnie ryzyko, może prowadzić do niskiego poziomu wiedzy oraz umiejętności wśród obywateli, co zwiększa ryzyko cyberataków. Wraz z nieustannym rozwojem nowych technologii oraz wykorzystaniem sztucznej inteligencji konieczne jest wprowadzenie programów edukacyjnych z zakresu cyberbezpieczeństwa w szkołach i uczelniach. Za zasadne należy uznać organizowanie warsztatów oraz szkoleń dla różnych grup wiekowych i społecznych, a także doskonalenia zawodowego w zakresie cyberbezpieczeństwa uwzględniającego aktualne zagrożenia w tym obszarze. Za obszary o najniższym prawdopodobieństwie zmaterializowania się ryzyka uznano politykę wewnętrzną, sankcje i zmiany klimatyczne. Ryzyko polityki wewnętrznej, obejmujące zmiany rządów czy kierunków politycznych na szczeblu krajowym, mogące wpłynąć na priorytety i finansowanie działań, w dalszym ciągu wymaga jednak ustanowienia międzyresortowych zespołów do spraw cyberbezpieczeństwa w celu zapewnienia spójności działań oraz warunków długoterminowego finansowania. Natomiast naruszenie międzynarodowych sankcji może prowadzić do poważnych konsekwencji prawnych i finansowych. Zalecane jest monitorowanie zmian w przepisach dotyczących sankcji oraz wdrożenie systemów zarządzania zgodnością z sankcjami. Ryzyko związane ze zmianami klimatycznymi przejawia się w rosnącej częstotliwości anomalii pogodowych, zdolnych do sparaliżowania infrastruktury krytycznej oraz zasobów informatycznych. Jako rekomendacje do zastosowania działań i środków zaradczych zostało uwzględnione wdrożenie planów awaryjnych na wypadek gwałtownych anomalii pogodowych oraz inwestycje w infrastrukturę i technologie odporne na skutki zmian klimatu. W ocenie ryzyka dotyczącego zmian klimatycznych znalazło się również regularne testowanie i aktualizacja planów zarządzania kryzysowego, które stanowią nieodzowny element bezpieczeństwa państwa.

DZIAŁANIA EDUKACYJNE NA RZECZ BUDOWANIA ŚWIADOMOŚCI ZAGROŻEŃ I WZMACNIANIA POZIOMU CYBERBEZPIECZEŃSTWA

W literaturze przedmiotu zwraca się uwagę, że cyberprzestrzeń jest środowiskiem dynamicznym, pozbawionym granic fizycznych i podatnym na zakłócenia (Foulon, Meibauer, 2024, s. 431). Cyberbezpieczeństwo stanowi obecnie jeden z najważniejszych filarów funkcjonowania państwa i społeczeństwa informacyjnego. Krajowe zespoły CSIRT odnotowały w 2024 r. ponad 111 tys. incydentów, a w 2025 r. tylko CSIRT NASK otrzymał ok. 50 tys. zgłoszeń miesięcznie, co świadczy o eskalacji zagrożeń. Zakres pojęcia edukacji dla bezpieczeństwa wyznaczają przemiany społeczne, kulturowe, ekonomiczne i oświatowe oraz zmiany zachodzące w otoczeniu. To one stanowią o aktywności jednostki, grupy społecznej, społeczeństwa, a także pozwalają wartościować ten proces (Rutkowski, 2018, s. 112–113). Należy mieć na uwadze, iż cyberzagrożenia przybierają różnorodne formy i obejmują zarówno klasyczne, jak i coraz bardziej zaawansowane techniki ataków. Współcześnie obserwuje się wzrost społecznej świadomości w zakresie bezpieczeństwa, które stało się fundamentem stabilnego funkcjonowania większości grup społecznych. Systematyczne monitorowanie nowych zagrożeń, szczególnie w sferze cyfrowej, oraz wdrażanie adekwatnych mechanizmów obronnych umożliwi skuteczne ograniczanie szkód i podniesienie standardów bezpieczeństwa.

Polska skutecznie rozwinęła swój potencjał obronny w cyberprzestrzeni, opierając strategię na budowaniu kompetencji obywateli oraz tworzeniu trwałych sojuszków międzynarodowych. Jednak nadal istnieją znaczące luki, szczególnie w świadomości społecznej i dostępności edukacji, co stanowi słaby punkt w naszej krajowej obronie przed cyberzagrożeniami (Krajowa Izba Gospodarki Cyfrowej, 2024). Działania edukacyjne powinny zatem opierać się na budowaniu holistycznej odporności cyfrowej poprzez nowoczesne metody szkoleniowe i kampanie społeczne. Należy pamiętać, że edukacja dla bezpieczeństwa jest nierozdzielnie związana z systemem bezpieczeństwa narodowego. Najważniejszą funkcją każdego państwa demokratycznego jest zapewnienie bezpieczeństwa narodowego państwu jako instytucji, a zwłaszcza bezpieczeństwa obywateli (Pieczywok, 2012, s. 458).

Istnieje potrzeba wskazania, iż globalizacja procesów informacyjnych, obok korzyści płynących z międzynarodowej wymiany danych, wygenerowała nowe ryzyka w postaci profesjonalizacji środowisk hakerskich oraz proliferacji złośliwego oprogramowania. Co istotne, współczesne wektory ataków w cyberprzestrzeni coraz częściej wykorzystują techniki socjotechniczne, w tym manipulację psychologiczną, a nie jedynie luki w infrastrukturze teleinformatycznej. W związku z powyższym kluczowym czynnikiem wzrostu odporności państwa jest edukacja użytkowników sieci w następujących obszarach:

- Budowanie świadomości ontologicznej zagrożeń – identyfikacja typologii ryzyk jako warunek wstępny kreowania strategii defensywnych.
- Wdrożenie kompetencji technicznych – operacjonalizacja wiedzy w zakresie administrowania zasobami cyfrowymi oraz konfiguracji parametrów prywatności.
- Instytucjonalizacja kultury bezpieczeństwa – promowanie modelu współpracy opartego na zbiorowej odpowiedzialności za integralność i poufność zasobów informacyjnych organizacji.

Kluczowym wyzwaniem dla systemów edukacyjnych staje się zatem optymalizacja modelu nauczania, który powinien obejmować następujące obszary kompetencyjne:

- Teoretyczne podstawy bezpieczeństwa informacyjnego – systematyka i opis fundamentalnych zagrożeń sieciowych, ze szczególnym uwzględnieniem wektorów ataków, takich jak phishing, oprogramowanie złośliwe, czyli malware, oraz oprogramowanie szantażujące ransomware.
- Zarządzanie bezpieczeństwem danych osobowych – implementacja standardów ochrony prywatności oraz wykształcenie zdolności do krytycznej analizy i oceny ryzyka związanego z dystrybucją informacji w przestrzeni cyfrowej.
- Operacjonalizacja kompetencji obronnych – nabywanie praktycznych umiejętności w zakresie stosowania kryptograficznych mechanizmów ochrony danych oraz zaawansowanych procedur uwierzytelniania.

- Kształtowanie świadomości społeczno-cyfrowej – rozwijanie zdolności do identyfikacji i niwelowania zagrożeń występujących w mediach społecznościowych, a także promowanie racjonalnych i bezpiecznych postaw w ramach interakcji zachodzących w środowisku online.

Skuteczność działań zarówno edukacyjnych, jak i profilaktycznych zależy od ich adekwatności do dynamicznie zmieniających się realiów cyberprzestrzeni. Natomiast cele i treści edukacji dla bezpieczeństwa powinny dostarczać gotowych rozwiązań i wzorów postępowania w możliwych sytuacjach zagrożeń, zmieniając się wraz z etymologiczną ewolucją samego pojęcia *bezpieczeństwo* (Zadornia, 2018, s. 99). Analiza aktualnych trendów w cyberprzestępczości wskazuje na potrzebę głębokiej restrukturyzacji kapitału ludzkiego w jednostkach odpowiedzialnych za cyberbezpieczeństwo. Bezpieczeństwo cyfrowe w dobie sztucznej inteligencji wymaga gruntownej redefinicji modelu kompetencji. Ze względu na szybki postęp technologiczny, doskonalenie wiedzy ekspertów ds. cyberbezpieczeństwa stało się kluczowe. Konieczna jest zatem kompleksowa reforma szkoleń na każdym poziomie organizacyjnym, łącząca potencjał sztucznej inteligencji z codzienną praktyką ochrony danych (Palani i in., 2024, s. 7).

Nabywanie tych kompetencji wykracza poza sferę indywidualną, tym samym wzmacniając odporność całego systemu społecznego na zagrożenia cyfrowe. Z tego powodu edukacja w obszarze cyberbezpieczeństwa musi stać się strategicznym priorytetem zarówno dla systemu oświaty, jak i podmiotów odpowiedzialnych za rozwój umiejętności technologicznych. Wdrażanie edukacji dla bezpieczeństwa wymaga konsekwentnych, długoterminowych działań, prowadzonych przez różne podmioty, które mają możliwość edukacyjnego oddziaływania na społeczeństwo. Powinna ona obejmować wszystkich obywateli, począwszy od dzieci w przedszkolu i szkole podstawowej, przez młodzież i studentów, po osoby dorosłe zarówno czynne zawodowo, jak i emerytów (Skrabacz, 2019, s. 74). Reasumując, szeroko zakrojone działania dydaktyczne i inicjatywy edukacyjne są niezbędnym instrumentem minimalizowania ryzyka cyfrowego oraz trwałego wzmacniania kompetencji obronnych użytkowników.

WNIOSKI KOŃCOWE

Podsumowując rozważania nad rolą edukacji dla bezpieczeństwa, należy podkreślić, że budowanie odporności cyfrowej musi opierać się na fundamencie stabilnej strategii rządowej. Integracja kompetencji technicznych z edukacją społeczną znajduje swoje odzwierciedlenie w najnowszych planach legislacyjnych, które wykraczają poza doraźne reagowanie na incydenty. W tym kontekście kluczowe znaczenie ma fakt, iż Ministerstwo Cyfryzacji prowadzi prace nad dokumentem o charakterze strategicznym w dziedzinie informatyzacji państwa, zwanym dalej Strategią Cyfryzacji, określającym kierunki procesu transformacji cyfrowej państwa w perspektywie do 2035 r. Nadrzędnym celem, który realizować ma Strategia Cyfryzacji jest poprawa jakości życia obywateli za pomocą technologii cyfrowych. Jednym z podstawowych zamierzeń jest założenie, że w 2035 r. przynajmniej podstawowe kompetencje cyfrowe będzie miało 85% obywateli. Strategia kładzie duży nacisk na budowanie systemowych rozwiązań do walki z fake newsami i kampaniami dezinformacyjnymi, które zagrażają stabilności państwa. Ważnym aspektem polityki i działań na rzecz cyberbezpieczeństwa, nad którym należałoby się szczególnie pochylić, jest cyberbezpieczeństwo dzieci i młodzieży. Internet jest przestrzenią, w której dochodzi do zachowań naruszających prawo, takich jak cyberprzemoc, hejt, oszustwa, groźby czy rozpowszechnianie nielegalnych treści. Hejt stał się powszechnym zjawiskiem w przestrzeni cyfrowej, na które narażone są zarówno osoby publiczne, jak i prywatni użytkownicy sieci. Niezmiernie istotne jest zatem przeprowadzanie zajęć profilaktycznych, warsztatów dla młodzieży ukierunkowanych na odporność emocjonalną oraz na sposoby radzenia sobie z negatywnymi komentarzami. Należy zatem uświadamiać dzieci i młodzież, że czyny popełniane w świecie wirtualnym niosą za sobą konsekwencje prawne, a pełna anonimowość w internecie w rzeczywistości nie istnieje. Konieczne jest zatem zastąpienie tradycyjnych modeli kształcenia dynamiczną edukacją adaptacyjną. Ma ona nie tylko dostarczać wiedzę o narzędziach, lecz przede wszystkim kształtować trwałą odporność na dezinformację i cyberprzestępczość.

REFERENCES

- Albrycht, I., Autolianto, S., Gęborys, P., Krawczyk, M., Marczyk, P., Mednis, A., Siudak, R., Świątkowska, J. (2019). *Wyzwania w cyberprzestrzeni przykłady rozwiązań, zagrożenia, regulacje*. Instytut Kościuszki, Kraków.
- Chałubińska-Jentkiewicz, K. (2025). Cyberbezpieczeństwo – zagrożenia definicje. *Cybersecurity and Law*, 1(13), 5.
- Damayanti, E.S. (2023). Risk Management: In an Overview of Literature Review. *Formosa Journal of Science and Technology*, 2(4), 1116–117.
- European Union Agency For Cybersecurity, Enisa Threat Landscape. 2025, <https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf> (dostęp: 2.01.2026).
- Foulon, M., Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*, 45(3), 431.
- Gallo, L., Gentile, D., Ruggiero, S., Botta, A., Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers & Security*, 139, 1–2.
- Komisia Europejska, Cyberbezpieczeństwo dostaw. 2026, https://poland.representation.ec.europa.eu/news/cyberbezpieczenstwo-dostaw-2026-01-20_pl (dostęp: 10.01.2026).
- Krajowa Izba Gospodarki Cyfrowej. (2024). Raport *Cyberbezpieczny Obywatel 2025/2026, Priorytety Transformacji Cyfrowej w Polsce Wyzwania i rekomendacje na lata 2025–2028 Perspektywa Obywatela*, https://kigc.pl/wp-content/uploads/KIGC_raport_26.11.2024.pdf, (dostęp: 15.12.2025).
- Kramarz, K., Korpysa, J. (2023). The evolution of the concept of risk management in IT+ organizations. *Procedia Computer Science*, 225, 4844.
- Leyden, L. (2025). *11 ways cybercriminals are making phishing more potent than ever*, <https://www.csoononline.com/article/3850783/11-ways-cybercriminals-are-making-phishing-more-potent-than-ever.html> (dostęp: 18.11.2025).
- Palani, K., Kethar, J., Prasad, S., Torremocha, V. (2024). Impact of AI and Generative AI in Transforming Cybersecurity. *Journal of Student Research*, 13(2), 7, <https://doi.org/10.47611/jsrhs.v13i2.6710>.
- Pieczywok, A. (2012). Bezpieczeństwo jako wartość edukacyjna i badawcza. W: Pieczywok, A. (red.). *Edukacja dla bezpieczeństwa wobec zagrożeń i wyzwań współczesności* (s. 457–480). Wydawnictwo Akademii Obrony Narodowej, Warszawa.
- Raport roczny CSIRT KNF. (2024), https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_Roczny_CSIRT_KNF_2024_93226.pdf, (dostęp: 02.09.2025).
- Rutkowski, C. (2018). *Podstawy nauk o bezpieczeństwie z elementami naukoznawstwa*. Wydawnictwo Szkoły Głównej Służby Pożarniczej, Warszawa.

- Safi, A., Singh, S. (2023). A systematic literature review on phishing website detection techniques. *Journal of King Saud University – Computer and Information Sciences*, 35, 590–591, <https://doi.org/10.1016/j.jksuci.2023.01.004>.
- Salman, H.A., Alsajri, A. (2023). The Evolution of Cybersecurity Threats and Strategies for Effective Protection. A review. *Shifra*, 2023, 73, <https://doi.org/10.70470/SHIFRA/2023/009>
- Siemieniecka, D., Grubicka, J.K. (2025). Płeć i wykształcenie a świadomość zagrożeń związanych z korzystaniem z Internetu – perspektywa relacji interpersonalnych. *Journal of Modern Science*, 1(61), 99, <https://doi.org/10.13166/jms/202386>.
- Skrabacz, A. (2019). Edukacja dla bezpieczeństwa młodzieży wobec wyzwań i zagrożeń współczesności. *Annales Universitatis Mariae Curie-Skłodowska sectio J – Paedagogia-Psychologia*, 32(3), 67, 74, <http://dx.doi.org/10.17951/j.2019.32.3.67-82>.
- Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa.(2024), <https://pliki.telepolis.pl/file/220984/original.pdf>, (dostęp: 20.10.2025).
- Stylianou, I., Bountakas, P., Zarras, A., Xenakis, C. (2025). Suspicious minds: Psychological techniques correlated with online phishing attacks. *Computers in Human Behavior Reports*, 19, 1–2, <https://doi.org/10.1016/j.chbr.2025.100694>.