Wiedza jest naszą tarczą!
„Czynnik ludzki” w bezpieczeństwie informacyjnym: między słabością a potencjałem

Juliusz Sikorski

Wydział Prawa i Bezpieczeństwa
Akademia im. Jakuba z Paradyża
w Gorzowie Wielkopolskim

ORCID 0000-0002-0579-0158

Streszczenie

Artykuł podkreśla, że w bezpieczeństwie informacyjnym kluczową rolę odgrywa człowiek, nie tylko jako potencjalne „najsłabsze ogniwo”, ale przede wszystkim jako zasób wzmacniający odporność systemów. Większość incydentów wynika z błędów użytkowników, jednak skuteczna ochrona wymaga systemowego podejścia, łączącego technologię, organizację i kulturę bezpieczeństwa. Autor wskazuje, że właściwie zaprojektowana edukacja i interaktywne szkolenia mogą znacząco podnieść świadomość oraz odpowiedzialność, przekształcając słabości w siłę organizacji i społeczeństwa

Słowa kluczowe: bezpieczeństwo informacyjne, czynnik ludzki, kultura bezpieczeństwa, edukacja i szkolenia, interakcja człowiek – technologia

1. Wprowadzenie

W warunkach powszechnej cyfryzacji wiedza jawi się jako jeden z kluczowych zasobów determinujących poziom bezpieczeństwa jednostek, organizacji oraz społeczeństw. To właśnie świadomy i odpowiednio wykształcony użytkownik dysponuje większym potencjałem w zakresie identyfikacji zagrożeń, co umożliwia skuteczniejsze ich unikanie oraz podejmowanie adekwatnych działań zaradczych. Dynamiczny rozwój technologii powoduje jednak, iż relacje pomiędzy człowiekiem a systemami informatycznymi nabierają coraz większej złożoności. Generuje to zarówno nowe możliwości, sprzyjające podnoszeniu efektywności ochrony, jak i kolejne wyzwania w postaci nieprzewidzianych podatności oraz zagrożeń. W centrum tego złożonego ekosystemu pozostaje człowiek, którego decyzje i zachowania mogą przesądzać o skuteczności nawet najbardziej zaawansowanych rozwiązań zabezpieczających[1].

2. Metodologia

Celem niniejszego artykułu jest ukazanie roli człowieka w systemach bezpieczeństwa informacyjnego. Autor podejmuje próbę zidentyfikowania ograniczeń oraz zagrożeń wynikających z interakcji człowieka z technologią, a także wskazania, iż skuteczność systemów ochrony warunkowana jest nie tylko przez zastosowane rozwiązania techniczne, lecz również przez poziom wiedzy, postawy oraz kulturę bezpieczeństwa użytkowników. Autor zmierza tym samym do przesunięcia akcentu z perspektywy traktującej człowieka wyłącznie jako „najsłabsze ogniwo" na postrzeganie go w kategoriach kluczowego zasobu, który, poprzez odpowiednią edukację, podnoszenie świadomości bezpieczeństwa oraz kształtowania dojrzałości informacyjnej, może znacząco wzmacniać zarówno organizacyjną, jak i społeczną odporność na zagrożenia informacyjne.

Niniejsze rozważania wpisują się w nurt krytycznych studiów nad bezpieczeństwem w ujęciu emancypacyjnym (tzw. szkoła walijska), w których założony zostaje normatywny cel w postaci uwolnienia człowieka spod wszelkich zagrożeń jako warunku pełnego bezpieczeństwa. W odróżnieniu od tradycyjnych analiz koncentrujących się na państwie i strukturach militarnych, taka perspektywa poszerza agendę badawczą o czynniki społeczne i kulturowe, obejmując także edukację oraz świadomość jako jej fundamentalne komponenty[2]. Przyjęta rama teoretyczna sprzyja analizie roli człowieka w systemach bezpieczeństwa informacyjnego, gdyż umożliwia ukazanie, iż kompetencje, poziom świadomości oraz kultura bezpieczeństwa użytkowników stanowią elementy równie istotne, jak rozwiązania technologiczne.

Artykuł ma charakter przeglądowo-teoretyczny i został oparty na krytycznej analizie literatury przedmiotu, obejmującej zarówno klasyczne koncepcje roli człowieka w systemach bezpieczeństwa informacyjnego, jak i najnowsze opracowania naukowe oraz raporty branżowe. W pracy zastosowano również metodę porównawczą (desk research), polegającą na zestawieniu oraz interpretacji wyników badań empirycznych, zarówno akademickich, jak i branżowych, które ukazują wielowymiarowe aspekty czynnika ludzkiego w bezpieczeństwie informacyjnym. Na tej podstawie dokonano syntezy teoretycznej, prowadzącej do sformułowania wniosków zaprezentowanych w części końcowej artykułu.

3. Człowiek jako słabe ogniwo – klasyczne ujęcie

Od końca lat dziewięćdziesiątych, a z całą pewnością od publikacji Bruce'a Schneiera, amerykańskiego kryptografa i eksperta ds. bezpieczeństwa, zatytułowanej „Secrets and Lies: Digital Security in a Networked World" (2000), upowszechnia się pogląd, iż to ludzie „często stanowią najsłabsze ogniwo w łańcuchu bezpieczeństwa i są chronicznie odpowiedzialni za

awarie systemów bezpieczeństwa” [3]. Do popularyzacji tej tezy w istotnym stopniu przyczynił się również Kevin Mitnick, znany haker i specjalista w obszarze inżynierii społecznej. Już niemal ćwierć wieku temu wskazywał on, iż wyrafinowane mechanizmy ochronne mogą zostać skutecznie ominięte dzięki odpowiednio zaplanowanym manipulacjom społecznym: „Nie myśl, że zabezpieczenia sieci i firewalle ochronią twoje informacje. Szukaj najsłabszego ogniwa. Zwykle okazuje się nim być człowiek”[4]. W swojej książce „Sztuka podstępu. Łamałem ludzi, nie hasła” podkreślał jednak kilkukrotnie, iż człowiek nie zawsze musi być tym ogniwem. Powodzenie ataku zależy przede wszystkim od zidentyfikowania elementu systemu wykazującego największą podatność na ingerencję. Mogą nim być chociażby niezabezpieczone kopie zapasowe[5].

Przekonania o roli człowieka jako najsłabszego ogniwa w systemie bezpieczeństwa potwierdzają liczne analizy oraz raporty branżowe. W opublikowanym w 2014 roku „IBM Cyber Security Intelligence Index” zwrócono uwagę, iż „fascynujące – i zarazem przygnębiające – jest to, że ponad 95% wszystkich zbadanych incydentów wskazuje na błąd ludzki jako czynnik przyczyniający się do awarii”[6]. Do najczęściej rejestrowanych uchybień zaliczono wówczas: nieprawidłową konfigurację systemów, niewłaściwe zarządzanie aktualizacjami, stosowanie domyślnych nazw użytkowników i haseł lub haseł zbyt prostych, gubienie urządzeń mobilnych, a także nieuprawnione ujawnianie informacji chronionych w wyniku korzystania z niewłaściwych adresów e-mail. Na czele tej swoistej listy błędów znajdowało się jednak tzw. „podwójne kliknięcie”, tj. otwarcie zainfekowanego załącznika bądź aktywacja niebezpiecznego adresu URL[7].

4. Empiryczne potwierdzenie problemu

Analiza dostępnych badań wskazuje, iż mimo upływu lat problem słabości czynnika ludzkiego w systemach bezpieczeństwa informacyjnego pozostaje aktualny. Zespół ghańsko-chińskich badaczy w opublikowanym w 2021 roku artykule dowodził, że czynnik ludzki w dalszym ciągu stanowi element krytyczny. Według ich ustaleń aż 71,4% incydentów było powodowanych przez użytkowników[8]. Autorzy wskazywali m.in. na błędy popełniane podczas obsługi systemów, niedbalstwo wynikające z rutyny bądź braku koncentracji, liczne przypadki nieprzestrzegania polityk bezpieczeństwa oraz błędy konfiguracyjne, często wynikające z pośpiechu lub niedostatecznych kompetencji. Zjawiska te, zdaniem badaczy, były konsekwencją niewystarczającej świadomości zagrożeń, uwarunkowanej nieadekwatnym zakresem szkoleń, o ile w ogóle były one realizowane. Wszystkie te czynniki zwiększały podatność organizacji na ataki socjotechniczne, co w efekcie prowadziło do sytuacji, w której

nawet najbardziej zaawansowane technologicznie środki ochrony mogły zostać zniweczone przez działania lub zaniechania człowieka. Mimo to, jak podkreślali autorzy, większość badanych organizacji konsekwentnie ignorowała potrzebę rozwijania potencjału defensywnego własnych pracowników, koncentrując się niemal wyłącznie na kontroli i wdrażaniu rozwiązań technologicznych[9].

Podobne wnioski w 2025 roku sformułowali badacze z Uniwersytetu Sapienza w Rzymie, którzy stwierdzili, że aż 72% naruszeń bezpieczeństwa było wynikiem działań bądź zaniechań pracowników. Wśród najczęstszych przyczyn uwzględniono podatność na ataki socjotechniczne, błędy w obsłudze systemów oraz nieprzestrzeganie obowiązujących procedur bezpieczeństwa. Zdaniem autorów, ograniczenie skali tego zjawiska wymaga przede wszystkim zmiany kultury organizacyjnej, podnoszenia poziomu świadomości użytkowników oraz wdrożenia systematycznych szkoleń adekwatnych do realnych zagrożeń[10].

Jeszcze wyraźniej problem ten akcentuje badaczka z Republiki Południowej Afryki, Tabisa Ncubukezi. Wyniki jej badań z 2022 roku, przeprowadzonych wśród małych przedsiębiorstw, wykazały, że aż 81% analizowanych firm doświadczyło błędów wynikających z ignorancji pracowników oraz nieprawidłowego podejmowania decyzji. Ponadto 80% incydentów wiązało się z naruszaniem polityk bezpieczeństwa, a 73% z niewłaściwym zarządzaniem hasłami i danymi wrażliwymi. Autorka wskazała również na częste występowanie tzw. błędów technicznych, takich jak brak tworzenia kopii zapasowych (78%), ignorowanie aktualizacji oprogramowania (64%) czy pobieranie nieautoryzowanego oprogramowania (47%). Choć działania te w wielu przypadkach miały charakter niezamierzony, w istotnym stopniu naruszały podstawowe zasady bezpieczeństwa informacji, w tym poufność, integralność i dostępność danych[11].

Wnioski te korespondują z najnowszymi danymi branżowymi. Według „Verizon Data Breach Investigations Report 2025" czynnik ludzki, obejmujący błędy, manipulacje społeczne oraz działania użytkowników, odpowiadał za 60% naruszeń bezpieczeństwa[12]. Rok wcześniej odsetek ten wynosił 68%, co może wskazywać na niewielką tendencję spadkową[13]. Równocześnie w „ENISA Threat Landscape 2024" podkreślono, że błąd ludzki pozostaje jedną z najczęściej eksploatowanych podatności, szczególnie w kontekście ataków phishingowych prowadzących do nieuprawnionego dostępu do danych[14].

Problematykę tę ujmuje także w perspektywie teoretycznej Włodzimierz Fehler. Badacz ten, wskazując zarówno na niezamierzone, jak i celowe intencje, wśród kluczowych zagrożeń antropogenicznych wymienia m.in. wytwarzanie i rozpowszechnianie informacji niskiej jakości, błędy i braki w procesach percepcji i dystrybucji danych, a także fałszowanie, kradzież,

manipulowanie, niszczenie czy wykorzystywanie informacji nieaktualnych. Fehler podkreśla przy tym znaczenie czynników psychologicznych i kompetencyjnych, wynikających z ograniczeń umiejętności użytkowników oraz stanów psychicznych, które mogą utrudniać podejmowanie racjonalnych decyzji i sprzyjać wykluczeniu informacyjnemu. Zaznacza przy tym, iż mimo postępującej informatyzacji człowiek pozostaje najważniejszym elementem polityki bezpieczeństwa informacji, gdyż skuteczność stosowanych zabezpieczeń w decydującej mierze zależy od jego świadomości, wiedzy i odpowiedzialności[15].

5. Systemowe podejście do incydentów

To właśnie swoista synergia pomiędzy człowiekiem, jego zdolnościami i uwarunkowaniami psychologicznymi, a technologią odgrywa fundamentalną rolę w kształtowaniu bezpieczeństwa informacyjnego[16]. Zwrócono na to uwagę m.in. w raporcie „Cyentia Institute", w którym podkreślono, że przyczyny słabości systemów wynikają przede wszystkim ze wzajemnego oddziaływania błędów ludzkich i podatności technologicznych[17].

Kwestia ta była wcześniej akcentowana także przez irlandzkiego cyberpsychologa Ciarána Mc Mahona, który wskazywał, że choć podatność systemu na zagrożenia faktycznie wzrasta w chwili interakcji z użytkownikiem, to inne komponenty „łańcucha bezpieczeństwa", takie jak oprogramowanie czy infrastruktura, są równie podatne na błędy i wymagają stałego serwisowania. Zamiast obwiniania użytkowników, badacz proponuje systemowe podejście do analizy incydentów, odwołując się do modelu „sera szwajcarskiego" Jamesa Reasona. Model ten ukazuje wypadki jako konsekwencję nałożenia się wielu luk w zabezpieczeniach, a nie pojedynczego błędu człowieka[18].

Mc Mahon zwraca również uwagę na psychologiczne skutki przerzucania winy na użytkowników, określając je mianem „victim blaming", czyli strategii prowadzącej do izolowania ofiar oraz osłabiającej ich gotowość do ostrzegania innych. W środowisku organizacyjnym takie podejście może dodatkowo pogarszać relacje pomiędzy pracownikiem a pracodawcą, obniżać poziom zaufania i sprzyjać nadużyciom. Badacz postuluje zatem, aby zamiast utrwalać negatywny stereotyp „najsłabszego ogniwa", budować należy kulturę bezpieczeństwa opartą na zasadach sprawiedliwości proceduralnej, transparentności oraz wsparcia dla użytkowników[19].

6. Kultura bezpieczeństwa informacyjnego

Na znaczenie kultury bezpieczeństwa informacyjnego w systemie ochrony zwraca uwagę wielu badaczy, w tym Hanna Batorowska, która podkreśla, iż człowiek zajmując

centralne miejsce w tej strukturze jest zarówno podmiotem wymagającym ochrony, jak i potencjalnym źródłem zagrożeń. Funkcjonując w infosferze, jednostka nie tylko korzysta z informacji, lecz także ją tworzy, przetwarza i rozpowszechnia, a brak kompetencji informacyjnych prowadzi do zwiększonej podatności na niebezpieczeństwa. Z tego względu kultura bezpieczeństwa informacyjnego, oparta na świadomości, refleksyjności i odpowiedzialności, staje się warunkiem utrzymania bezpieczeństwa jednostkowego i zbiorowego. Jej rozwój wymaga kształtowania dojrzałości informacyjnej obywateli, zdolnych nie tylko do krytycznej analizy treści, lecz również do dostrzegania konsekwencji własnych działań w infosferze. Bez takiego przygotowania człowiek staje się łatwym celem ataków i nie jest w stanie skutecznie uczestniczyć ani w procesie ochrony zasobów wiedzy, ani w budowaniu zbiorowego poczucia bezpieczeństwa[20].

7. Człowiek jako zasób – nowe podejścia

Potwierdzają to najnowsze badania, wskazujące, iż człowiek nie powinien być postrzegany wyłącznie jako „najsłabsze ogniwo" systemu, lecz jako kluczowy zasób zdolny wzmacniać odporność organizacji na zagrożenia. Odpowiednio kształtowana kultura bezpieczeństwa, oparta na świadomości i poczuciu odpowiedzialności, umożliwia przekształcanie potencjalnych słabości w elementy przewagi organizacyjnej. Wyniki badań zespołu rzymskich naukowców, przeprowadzonych z wykorzystaniem metody Delphi, doprowadziły do wyłonienia szesnastu działań menedżerskich pozwalających skuteczniej wykorzystać potencjał pracowników. Wśród nich znalazły się m.in.: kampanie podnoszące świadomość, szkolenia oparte na interaktywnych symulacjach, wzmacnianie poczucia osobistej odpowiedzialności, równoważenie obciążenia pracą, traktowanie raportowania incydentów jako wartości organizacyjnej oraz rozwój kultury bezpieczeństwa. Takie podejście wpisuje się w model socjotechniczny, zgodnie z którym skuteczność systemów bezpieczeństwa zależy zarówno od zastosowanych technologii, jak i od zachowań, motywacji i współpracy użytkowników[21].

8. Rola edukacji i szkoleń

Kluczową rolę w kształtowaniu kultury bezpieczeństwa informacyjnego należy przypisać właściwie projektowanej edukacji użytkowników, gdyż to właśnie ona posiada potencjał minimalizowania ryzyka wystąpienia zagrożeń. Z systematycznego przeglądu badań nad metodami szkoleń w tym obszarze, przeprowadzonego niedawno przez naukowców z Instytutu Bezpieczeństwa i Spraw Globalnych Uniwersytetu w Lejdzie, wynika, iż większość

programów szkoleniowych przynosi pozytywne efekty w kształtowaniu zachowań użytkowników, niezależnie od zastosowanego tematu czy formy. Najczęściej wykorzystywaną metodą były gry edukacyjne, które angażują uczestników i sprzyjają utrwalaniu treści, choć skuteczność wykazały również prezentacje, szkolenia wideo czy symulacje phishingowe. Autorzy podkreślają jednak, iż tradycyjne kampanie podnoszenia świadomości, oparte na ulotkach, plakatach czy newsletterach, okazują się mało efektywne, gdyż sama wiedza nie wystarcza do zmiany zachowań. Zwracają ponadto uwagę na brak spójności w projektowaniu interwencji, wiele programów powstawało intuicyjnie, bez oparcia w teoriach psychologicznych, a ich skuteczność oceniano głównie w krótkim horyzoncie czasowym i na niewielkich próbach. Rzadko prowadzono również ewaluacje w realnym środowisku pracy, co ogranicza możliwość uogólniania wyników. Z tego względu badacze postulują rozwijanie szkoleń opartych na teoriach zmiany zachowań, prowadzenie długoterminowych badań terenowych oraz stosowanie obiektywnych miar zachowań, aby skuteczniej budować odporność organizacyjną na zagrożenia informacyjne[22].

9. Wnioski i rekomendacje

Przeprowadzona analiza wskazuje, iż czynnik ludzki odgrywa centralną rolę w systemach bezpieczeństwa informacyjnego. Pomimo dynamicznego rozwoju technologii to właśnie błędy użytkowników, ich nieuwaga, brak wiedzy czy nieprzestrzeganie procedur pozostają głównymi źródłami incydentów. Klasyczne podejście, traktujące człowieka jako „najsłabsze ogniwo”, okazuje się jednak nadmiernie uproszczone, gdyż nie uwzględnia faktu, że użytkownik może także wzmacniać kulturę bezpieczeństwa i podnosić odporność organizacyjną. Istotne jest zatem, aby incydenty analizować w sposób systemowy, z uwzględnieniem wzajemnych zależności między człowiekiem, technologią i organizacją, zamiast redukować problem wyłącznie do błędów jednostek. Stąd wynika potrzeba rozwijania kultury bezpieczeństwa informacyjnego opartej na świadomości i odpowiedzialności, bez której zarówno jednostki, jak i całe społeczeństwa pozostają podatne na manipulacje oraz zagrożenia. Szczególne znaczenie należy w tym kontekście przypisać edukacji i szkoleniom, które, jeśli zostaną właściwie zaprojektowane i oparte na metodach interaktywnych, mogą realnie ograniczać ryzyko incydentów. Należy jednak podkreślić, że nie jest to reguła, gdyż wiele programów szkoleniowych powstaje w sposób intuicyjny, bez solidnych podstaw teoretycznych, co istotnie ogranicza ich skuteczność w długim horyzoncie.

Rekomendacje wynikające z powyższych ustaleń koncentrują się na konieczności zmiany podejścia do roli człowieka w bezpieczeństwie informacyjnym. Po pierwsze,

użytkownik powinien być postrzegany nie jako zagrożenie, lecz jako zasób, którego kompetencje i poczucie odpowiedzialności mogą wzmacniać system ochrony. Po drugie, należy konsekwentnie budować kulturę bezpieczeństwa opartą na zaufaniu, transparentności i współpracy, zamiast stosować praktyki obwiniania pracowników, prowadzące do izolacji i obniżenia poziomu zaufania w organizacji. Po trzecie, edukacja i szkolenia powinny być projektowane w oparciu o teorie psychologiczne oraz modele zmiany zachowań, tak aby realnie wpływały na praktyki użytkowników i przynosiły trwałe rezultaty. W tym celu warto wykorzystywać metody interaktywne, takie jak gry edukacyjne, symulacje ataków czy studia przypadków, które dzięki zaangażowaniu uczestników zwiększają skuteczność przekazu. Równocześnie programy szkoleniowe winny być systematycznie ewaluowane w naturalnym środowisku pracy, z wykorzystaniem obiektywnych miar zachowań. Wreszcie, niezbędne jest także wspieranie rozwoju społecznej dojrzałości informacyjnej, umożliwiającej nie tylko świadome korzystanie z technologii, lecz również krytyczną analizę treści, przewidywanie konsekwencji własnych działań i odpowiedzialne uczestnictwo w infosferze.

---

[1] Por. J. Rossa, T. Marcinkowski, *Wprowadzenie oraz tezy o socjologii bezpieczeństwa*, [w:] *Rozwój na peryferiach? Rozwój czy maldevelopment?*, T. III, red. J. Rossa, T. Marcinkowski, Gorzów Wielkopolski: Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim, 2020, s. 22.

[2] Columba L. Peoples, Nick Vaughan-Williams, *Critical Security Studies: An Introduction*, 3rd ed., Routledge, Abingdon 2021, s. 28-40.

[3] Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, New York: John Wiley & Sons, 2000, s. 255.

[4] Kevin Mitnick, William L. Simon, *Sztuka podstępu. Łamałem ludzi, nie hasła*, Gliwice: Helion, 2003, s. 100.

[5] Ibidem, s. 126, 337.

[6] IBM Global Technology Services. *IBM Security Services 2014 Cyber Security Intelligence Index: Analysis of cyber attack and incident data from IBM's worldwide security operations*. Somers, NY, IBM Corporation, May 2014, s. 3.

[7] Ibidem.

[8] Kwesi Hughes-Lartey, Meng Li, Francis E. Botchey, Zhen Qin, *Human factor, a critical weak point in the information security of an organization's Internet of things*, "Heliyon" 2021, 7(3), s. 1, e06524. DOI: 10.1016/j.heliyon.2021.e06524.

[9] Ibidem, s. 2-5.

[10] Silvia Colabianchi, Francesco Costantino, Fabio Nonino, Giulia Palombi, *Transforming threats into opportunities: The role of human factors in enhancing cybersecurity*, "Journal of Innovation & Knowledge" 2025, Vol. 10, No. 1, s. 65-66, DOI: 10.1016/j.jik.2024.100511.

[11] Tabisa Ncubukezi, *Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses*, [w:] *Proceedings of the 17th International Conference on Information Warfare and Security*. Academic Conferences International Limited, 2022, s. 395-403.

[12] MIMECAST. *Verizon: 60% of breaches involve human error*. *Mimecast Blog*, 1.5.2025, https://www.mimecast.com/blog/verizon-60-of-breaches-involve-human-error/ (25.8.2025).

[13] VERIZON. *2024 Data Breach Investigations Report. Executive Summary.* Verizon, 2024, s. 7, https://www.verizon.com/business/resources/reports/2024-dbir-executive-summary.pdf (25.8.2025).

[14] ENISA. *ENISA Threat Landscape 2024. Key Findings.* European Union Agency for Cybersecurity, 27.9.2024, https://www.data-rover.com/blog/thoughts-on-the-industry-5/enisa-cyber-threat-landscape-report-2024-key-findings-39.html (25.8.2025).

[15] Włodzimierz Fehler, *Podstawy bezpieczeństwa informacyjnego*, Siedlce: Uniwersytet Przyrodniczo-Humanistyczny, 2021, s. 115-119, 128, 189-190, 224.

[16] Por. J. Rossa, T. Marcinkowski, *Wprowadzenie oraz tezy o socjologii bezpieczeństwa*, op. cit., s. 18.
[17] Cyentia Institute, *Information Risk Insights Study: It's About Time (IRIS 2025)*, s. 6, 24, 33, www.cyentia.com/wp-content/uploads/2025/06/IRIS-2025.pdf (15.8.2025).
[18] Ciarán Mc Mahon, *In Defence of the Human Factor*, "Frontiers in Psychology" 2020, vol. 11, art. 1390. DOI: 10.3389/fpsyg.2020.01390; zob.: James Reason, *Human error: models and management,* "British Medical Journal" 2000, Vol. 320, No. 7237, s. 769, DOI: 10.1136/bmj.320.7237.768.
[19] Ciarán Mc Mahon, *In Defence of the Human Factor…*, op. cit., s. 4-5.
[20] Hanna Batorowska, *Kultura bezpieczeństwa informacyjnego*. „Edukacja – Technika – Informatyka" 2018, T. 23, nr 1, s. 94-95, 97-99, DOI: 10.15584/eti.2018.1.11.
[21] S. Colabianchi, F. Costantino, F. Nonino, G. Palombi, *Transforming threats into opportunities…*, op. cit., s. 2-4, 7-10.
[22] Julia Prümmer, Tommy van Stehen, Bibi van den Berg, *A systematic review of current cybersecurity training methods*. "Computers & Security" 2024, Vol. 136, Art. 103585, s. 3-9. DOI: 10.1016/j.cose.2023.103585.