Barbara Drapikowska[1], Sylwia Borawska[2]
Akademia Sztuki Wojennej w Warszawie

https://doi.org/10.29316/9788368103359_4

ROLA UŻYTKOWNIKA W KSZTAŁTOWANIU CYBERBEZPIECZEŃSTWA ORGANIZACJI

THE USER'S ROLE IN SHAPING AN ORGANIZATION'S CYBERSECURITY

Streszczenie

Rozdział poświęcono analizie roli użytkownika w kształtowaniu cyberbezpieczeństwa organizacji, ze szczególnym uwzględnieniem znaczenia kompetencji cyfrowych jako czynnika warunkującego odporność na zagrożenia cybernetyczne. Problem badawczy sformułowano w postaci pytania: w jakim stopniu kompetencje cyfrowe użytkowników warunkują odporność organizacji na cyberataki? Celem rozdziału było określenie roli kompetencji cyfrowych użytkowników w budowaniu odporności organizacji na zagrożenia w cyberprzestrzeni. Przyjęto hipotezę badawczą, zgodnie z którą wyższy poziom kompetencji cyfrowych użytkowników istotnie zwiększa zdolność organizacji do zapobiegania, wykrywania oraz reagowania

[1] https://orcid.org/0000-0002-6852-2791, e-mail: b.drapikowska@akademia.mil.pl
[2] https://orcid.org/0009-0006-6851-9492, e-mail: borawska.sylwia@o2.pl

na incydenty cyberbezpieczeństwa. W rozdziale zastosowano teoretyczne metody badawcze, obejmujące analizę i ocenę literatury przedmiotu, analizę dokumentów strategicznych i raportów instytucjonalnych (m.in. ENISA, CERT Polska, IBM Security), a także metodę syntezy i porównania istniejących ujęć kompetencji cyfrowych w kontekście bezpieczeństwa informacji. Przeprowadzone rozważania wykazały, że kompetencje cyfrowe obejmujące wiedzę, umiejętności oraz postawy użytkowników w znacznym stopniu determinują poziom cyberodporności organizacji. W konsekwencji kompetencje cyfrowe należy traktować jako jeden z kluczowych czynników kształtujących poziom bezpieczeństwa informacji oraz stabilność funkcjonowania organizacji we współczesnym środowisku cyfrowym.

Słowa kluczowe: kompetencje cyfrowe, cyberbezpieczeństwo, odporność, edukacja

Abstract

The chapter is devoted to the analysis of the role of the user in shaping the cybersecurity of the organization, with particular emphasis on the importance of digital competences as a factor determining resilience to cyber threats. The research problem was formulated in the form of a question: to what extent do users' digital competencies determine the resilience of an organization to cyberattacks? The aim of the chapter was to determine the role of digital competences of users in building the organization's resilience to threats in cyberspace. The research hypothesis was adopted, according to which a higher level of digital competence of users significantly increases the organization's ability to prevent, detect and respond to cybersecurity incidents. The chapter uses theoretical research methods, including analysis and critical evaluation of the literature on the subject, analysis of strategic documents and institutional reports (m.in. ENISA, CERT Polska, IBM Security), as well as a method of synthesizing and comparing existing approaches to digital competences in the context of information security. The conducted considerations have shown that digital competencies, including the knowledge, skills and attitudes of users, significantly determine the level of cyber resilience of an organization. As a consequence, digital competences should be treated as one of the key factors shaping the level of information security and the stability of the organization's functioning in the modern digital environment.

Keywords: digital competences, cybersecurity, resilience, education

Wstęp

Dynamiczny rozwój technologii informacyjno-komunikacyjnych sprawił, że cyberbezpieczeństwo stało się jednym z kluczowych obszarów funkcjonowania współczesnych organizacji. Złożoność środowiska cyfrowego, rosnąca liczba zagrożeń oraz powszechne wykorzystywanie narzędzi sieciowych powodują, że ochrona informacji przestaje być wyłącznie zagadnieniem technicznym. W raportach branżowych wskazuje się, iż znaczna część incydentów bezpieczeństwa ma swoje źródło w działaniach użytkowników, a nie w niedoskonałości samych systemów informatycznych (Verizon, 2024).

Jednocześnie obserwuje się wyraźne zróżnicowanie poziomu przygotowania pracowników do funkcjonowania w środowisku zagrożeń cyfrowych. Europejska Agencja ds. Cyberbezpieczeństwa zwraca uwagę, że kompetencje użytkowników w zakresie bezpiecznego korzystania z technologii nie zawsze nadążają za tempem cyfryzacji procesów organizacyjnych (ENISA, 2020). Z kolei raport IBM Security (2024) podkreśla, że organizacje charakteryzujące się wyższym poziomem przygotowania personelu skuteczniej ograniczają skutki incydentów.

W tym kontekście zasadne staje się podjęcie refleksji nad zależnością pomiędzy poziomem kompetencji cyfrowych użytkowników a zdolnością organizacji do funkcjonowania w warunkach rosnących zagrożeń. Rozważania te prowadzą do sformułowania problemu badawczego dotyczącego tego, w jakim stopniu kompetencje cyfrowe warunkują odporność organizacji na cyberataki? a także do wyznaczenia celu niniejszego rozdziału, którym jest określenie roli kompetencji cyfrowych użytkowników w budowaniu odporności organizacji na cyberataki.

Znaczenie kompetencji cyfrowych użytkowników

Współczesne cyberbezpieczeństwo nie może być rozpatrywane wyłącznie przez pryzmat technologii – coraz więcej badań wskazuje, że czynnik ludzki jest kluczowym determinantem sukcesu lub porażki systemów ochrony informacji. Tradycyjne modele ochrony koncentrowały się na rozwiązaniach technicznych tj. zapory sieciowe, systemy wykrywania włamań czy zaawansowane algorytmy kryptograficzne, jednak praktyka

pokazuje, że najczęstsze naruszenia bezpieczeństwa wynikają z błędów lub niewłaściwych zachowań samych użytkowników.

W literaturze zjawisko to jest intensywnie analizowane jako zagadnienie interdyscyplinarne, łączące aspekty psychologii, organizacji i technologii – co pokazuje najnowsza przeglądowa analiza literatury w dziedzinie „human factors in cybersecurity" (Khadka, Barkat Ullah, 2025). Takie spojrzenie znajduje odzwierciedlenie w literaturze i praktyce: organizacje, które traktują bezpieczeństwo jako wspólną odpowiedzialność, osiągają lepsze wyniki w ograniczaniu incydentów niż te, które koncentrują się jedynie na technologii i procedurach formalnych (Verizon, 2024).

W tym kontekście rola pojedynczego użytkownika jest szczególnie istotna – to on codziennie podejmuje decyzje, które albo wzmacniają bariery ochronne, albo je osłabiają. W tak złożonym dzisiejszym środowisku same zabezpieczenie techniczne bez wsparcia odpowiednich zachowań użytkowników nie wystarczają. Tak więc użytkownicy systemów organizacyjnych pełnią dziś wiele ról: są operatorami, decydentami, klientami wewnętrznymi i pierwszą linią kontaktu z potencjalnymi zagrożeniami. W praktyce oznacza to, że każda interakcja użytkownika z systemem komputerowym może stać się momentem podatności lub przeciwnie, wzmocnienia bezpieczeństwa. Procesy tj. rozpoznawanie phishingu, stosowanie zasad haseł, aktualizowanie oprogramowania czy reagowanie na podejrzane zdarzenia stanowią integralne elementy organizacyjnej odporności.

W literaturze termin „human firewall" (Włodarczyk, 2020) został użyty właśnie po to, aby podkreślić, że świadome i kompetentne działania personelu mogą działać jak uzupełniający, aktywny element systemu ochrony, redukując zależność od pasywnych narzędzi IT.

Aby właściwie zrozumieć uwarunkowania omawianego problemu badawczego, konieczne jest doprecyzowanie pojęcia kompetencji cyfrowych. Zgodnie ze stanowiskiem Ministerstwa Cyfryzacji (2020) są one definiowane jako „harmonijna kompozycja wiedzy, umiejętności i postaw umożliwiających życie, uczenie się i pracę w społeczeństwie cyfrowym, tj. społeczeństwie wykorzystującym w życiu codziennym i pracy technologie cyfrowe".

W kontekście funkcjonowania organizacji kompetencje te warunkują zdolność użytkowników do efektywnego i bezpiecznego wykonywania obowiązków zawodowych w środowisku opartym na technologiach cyfrowych.

Oznacza to, że pracownik nie tylko potrafi posługiwać się narzędziami informatycznymi, lecz również rozumie konsekwencje swoich działań w cyberprzestrzeni, potrafi rozpoznawać sytuacje ryzykowne oraz świadomie stosuje zasady bezpieczeństwa informacji.

Vademecum Bezpieczeństwa Informacyjnego (2020) wydane przez Uniwersytet Komisji Edukacji Narodowej (UKEN) kompetencje cyfrowe należy postrzegać jako „zespół umiejętności, wiedzy i postaw umożliwiających świadome i krytyczne korzystanie z technologii cyfrowych (w tym z Internetu) w celu uczenia się, pracy i aktywnego udziału w społeczeństwie informacyjnym". Takie ujęcie akcentuje wielowymiarowy charakter kompetencji cyfrowych i wskazuje, że ich istotą nie jest jedynie biegłość techniczna, lecz zdolność do refleksyjnego funkcjonowania w środowisku cyfrowym.

Pierwszym komponentem, który wskazał UKEN jest wiedza, obejmująca rozumienie sposobu, w jaki technologie cyfrowe wspierają komunikację, kreatywność oraz innowacyjność, a także świadomość ich ograniczeń, potencjalnych konsekwencji i zagrożeń. Obejmuje ona znajomość podstawowych zasad działania technologii, rozumienie mechanizmów leżących u podstaw ich rozwoju oraz umiejętność krytycznej oceny wiarygodności informacji i danych rozpowszechnianych w środowisku cyfrowym, z uwzględnieniem aspektów prawnych i etycznych.

Drugim obszarem są umiejętności, które pozwalają użytkownikom nie tylko na bierne korzystanie z narzędzi cyfrowych, lecz także na aktywne uczestnictwo w procesach komunikacji, współpracy i tworzenia treści. Obejmują one zdolność do wyszukiwania, filtrowania, oceny i przetwarzania informacji, tworzenia i udostępniania zasobów cyfrowych, a także zarządzania własną tożsamością cyfrową oraz ochrony danych. W tym wymiarze istotne staje się również rozpoznawanie możliwości zastosowania nowych technologii, w tym rozwiązań opartych na sztucznej inteligencji, w sposób efektywny i bezpieczny.

Trzecim elementem są postawy, rozumiane jako refleksyjne, krytyczne i odpowiedzialne podejście do korzystania z technologii cyfrowych. Obejmują one otwartość na zmiany technologiczne, gotowość do uczenia się, a także etyczne i bezpieczne korzystanie z narzędzi cyfrowych, z poszanowaniem zasad ochrony prywatności, danych oraz innych użytkowników. Postawy te decydują o tym, czy posiadana wiedza i umiejętności zostaną

wykorzystane w sposób sprzyjający zarówno rozwojowi jednostki, jak i bezpieczeństwu organizacji.

Wskazane składowe kompetencji cyfrowych stanowią dziś nie tylko element indywidualnego rozwoju użytkowników, lecz również istotny zasób organizacyjny. Ich poziom wpływa na sposób realizacji codziennych procesów, jakość podejmowanych decyzji oraz zdolność organizacji do reagowania na sytuacje kryzysowe w cyberprzestrzeni. W praktyce oznacza to, że kompetencje cyfrowe pracowników przestają być wyłącznie kwestią sprawności obsługi narzędzi, a stają się jednym z filarów bezpieczeństwa. Warto podkreślić, że „umiejętności cyfrowe mają kluczowe znaczenie dla strategii cyfrowej UE na rzecz zapewnienia suwerenności technologicznej, zniwelowania przepaści cyfrowej i promowania środowiska cyfrowego skoncentrowanego na człowieku w całej UE" (Komisja Europejska, 2025).

Podstawowe kompetencje cyfrowe stanowią fundament aktywnego uczestnictwa w życiu społecznym oraz na rynku pracy. Dynamiczny rozwój przełomowych technologii – tj. sztuczna inteligencja, środowiska wirtualne, robotyka, technologie kwantowe czy sieci 6G – powoduje rosnące zapotrzebowanie na nowy zestaw zaawansowanych kwalifikacji cyfrowych.

Tak jak zostało już wskazane, współczesny użytkownik nie jest jedynie odbiorcą technologii, lecz aktywnym uczestnikiem procesów bezpieczeństwa, którego postawy i decyzje bezpośrednio wpływają na poziom ochrony zasobów informacyjnych. Według raportu Polskiej Agencji Rozwoju Przedsiębiorczości (PARP) kompetencje cyfrowe stały się jednym z kluczowych trendów rynku pracy, a ich brak jest często wymieniany jako bariera dla efektywnego wykonywania zadań w nowoczesnym środowisku cyfrowym (PARP, 2024).

Jednocześnie krajowe programy rozwoju kompetencji, tj. Poland Digital Competence Development Programme 2020-2030, podkreślają strategiczne znaczenie umiejętności cyfrowych nie tylko dla osób pracujących w sektorze IT, ale dla całej społeczności w różnych branżach (Digital Skills and Jobs Platform, 2020). Komisja Europejska wskazuje, że w ponad 90% miejsc pracy w UE wymagane są co najmniej podstawowe umiejętności cyfrowe. W perspektywie do 2030 roku takie kompetencje wymagane będą w 9 na 10 miejsc pracy. Ich znaczenie rośnie również w Polsce (Rogacka, 2022).

Użytkownik powinien posiadać zestaw pożądanych cech, które są pożądne, należy do nich przede wszystkim zdolność do szybkiego uczenia się technologii i narzędzi cyfrowych. Pracodawcy coraz częściej oczekują, że nowi pracownicy nie tylko będą potrafili korzystać z obecnych rozwiązań, lecz także będą gotowi do szybkiej adaptacji w obliczu nowych technologii oraz zagrożeń. Co idzie za tym do dalszych etapów rekrutacji będą przechodzi osoby, które właśnie ten zestaw cech posiadają, a pracodawca ewentualnie będzie dawał możliwości ich rozwoju. Ten rodzaj elastyczności i otwartości na rozwój jest kluczowy w środowisku, gdzie narzędzia, protokoły i standardy bezpieczeństwa zmieniają się bardzo dynamicznie (Pawłowska-Cyprysiak, Hildt-Ciupińska, 2024).

Równie istotna jest umiejętność oceniania informacji cyfrowych, co wiąże się bezpośrednio z rozpoznawaniem prób manipulacji, deepfake, phishingu czy dezinformacji. W kulturze organizacyjnej, w której cyberzagrożenia są coraz bardziej wyrafinowane, użytkownik musi umieć ocenić wiarygodność źródeł, komunikatów czy plików, zanim podejmie działania mogące mieć konsekwencje dla bezpieczeństwa sieciowego. Stworzenie automatycznego nawyku sprawdzania rzetelności informacji nie jest łatwe jednak jak mówi przysłowie „praktyka czyni mistrza", ilekroć znajdzie się informację należy najpierw ją zweryfikować.

Kolejną pożądaną kwalifikacją jest znajomość zasad bezpiecznego korzystania z technologii, obejmująca m.in. świadome zarządzanie hasłami, stosowanie uwierzytelniania wieloskładnikowego czy umiejętność właściwego reagowania na incydenty cybernetyczne. Tego rodzaju kompetencje nie są typowymi „umiejętnościami twardymi" jak programowanie, lecz należą do obszaru cyberhigieny (Ministerstwo Cyfryzacji, 2022) – codziennych praktyk, które znacząco ograniczają ryzyko naruszeń.

Nie mniej ważna jest umiejętność komunikacji i współpracy cyfrowej w zespole, co staje się kluczowe w sytuacjach wymagających szybkiej wymiany informacji i koordynacji działań reagowania na zagrożenia. Najważniejszym zasobem organizacji są ludzie, a jak ludzie to i komunikacja, która musi być jasna i zrozumiała dla każdego elementu tworzącego zespół. W pracy zespołowej kompetencje te umożliwiają nie tylko wydajną pracę, lecz także skuteczne wdrażanie procedur bezpieczeństwa i wymianę wiedzy.

Wreszcie, cechą coraz częściej wymienianą w kontekście rynku pracy jest odpowiedzialność cyfrowa – postawa zakładająca aktywne dbanie

o bezpieczeństwo własne i organizacji, zgodnie z zasadami etycznego i świadomego korzystania z technologii. Ta postawa obejmuje refleksję nad konsekwencjami własnych działań w cyberprzestrzeni oraz gotowość do stałego doskonalenia swoich kwalifikacji w odpowiedzi na nowe wyzwania. Tak rozumiane cechy i kwalifikacje użytkownika nie tylko zwiększają jego wartość jako pracownika cyfrowego, lecz również dają wartość dodatnią dla całej organizacji.

Warto również wskazać, że użytkownik tak jak wcześniej zostało podkreślone jest aktywnym użytkownikiem wirtualnej przestrzeni, co niesie za sobą również skutki. Błędy użytkowników rzadko mają charakter „drobnych potknięć" – w praktyce mogą uruchamiać łańcuch zdarzeń prowadzący do incydentu, kosztów operacyjnych, konsekwencji prawnych oraz długotrwałej utraty zaufania. Co istotne, liczne analizy pokazują, że komponent ludzki jest regularnie obecny w znaczącej części naruszeń: w ujęciu globalnym Verizon (2024) wskazuje, że human element był składową 68% naruszeń w analizowanym zbiorze danych. Na gruncie polskim rosnąca skala incydentów opartych na socjotechnice jest widoczna w danych CERT Polska: w 2024 r. liczba zgłoszeń przekroczyła 600 tys., a najczęstszym incydentem był phishing; sam phishing stanowił 40 120 zarejestrowanych incydentów (Kancelaria Prezesa Rady Ministrów, 2025).

Jedną z konsekwencji są przede wszystkim finanse, które obejmują zarówno koszty „twarde" (np. przywracanie działania systemów, usługi zewnętrzne, obsługa prawna), jak i koszty wtórne (np. utrata klientów, działania naprawcze, komunikacja kryzysowa). Raport IBM Security (2024) wskazuje, że ataki phishingowe (silnie zależne od reakcji użytkownika) należą do najbardziej kosztownych wektorów naruszeń. Błąd użytkownika bywa punktem wejścia do zdarzeń, które realnie zatrzymują procesy biznesowe: zainfekowanie stacji roboczej, przejęcie konta, nieuprawnione udostępnienie danych czy uruchomienie złośliwego załącznika. Skutkiem jest często nie tylko problem IT, ale przerwanie usług, opóźnienia operacyjne i konieczność pracy w trybie awaryjnym. IBM podkreśla, że w kosztach incydentu istotną rolę odgrywa system downtime (przestój), a „czas oznacza pieniądze" – dłuższy cykl wykrycia i opanowania incydentu wiąże się z wyższymi kosztami (IBM Security, 2024).

Błędy użytkowników są szczególnie kosztowne w ekosystemie oszustw „na człowieka" (phishing/smishing/vishing). W Polsce skala tego

zjawiska jest dobrze widoczna w danych CERT Polska: w 2024 r. odnotowano m.in. 355 tys. zgłoszeń podejrzanych SMS-ów, a działania ochronne oparte na zgłoszeniach i blokowaniu przez operatorów pozwoliły ograniczać skutki kampanii smishingowych (Kancelaria Prezesa Rady Ministrów, 2025). Z perspektywy organizacji oznacza to, że pojedynczy błąd pracownika może skutkować nie tylko incydentem jednostkowym, ale też „otwarciem drzwi" do kolejnych prób wyłudzeń w tej samej sieci relacji (podszycia pod współpracowników, przejęcia komunikacji, fałszywe faktury itp.). Warto również wskazać utratę zaufania interesariuszy (klientów, partnerów, obywateli) które jest skutkiem trudnym do szybkiego odwrócenia. Nawet gdy incydent zostanie technicznie opanowany, organizacja pozostaje z kosztami komunikacji kryzysowej, koniecznością informowania o naruszeniu (w przypadkach wymaganych prawem) oraz ryzykiem długofalowego osłabienia reputacji. IBM Security (2024) wprost ujmuje „lost customers" i „reputation damage" jako elementy kosztów ponoszonych po naruszeniu.

W świetle przedstawionych rozważań staje się oczywiste, że użytkownik przestaje być jedynie odbiorcą technologii, a staje się współtwórcą poziomu bezpieczeństwa organizacji. Ostateczny kształt ochrony informacji nie zależy wyłącznie od systemów i procedur, lecz od codziennych, często pozornie drobnych decyzji podejmowanych przez ludzi. To właśnie na styku kompetencji, postaw i praktyki organizacyjnej rozstrzyga się realna odporność na zagrożenia cyfrowe. Dlatego rozwój kompetencji cyfrowych należy postrzegać nie jako koszt, lecz jako inwestycję w stabilność i ciągłość działania organizacji.

Rozwój kompetencji cyfrowych

W obliczu gwałtownej transformacji cyfrowej rozwój kompetencji cyfrowych przestaje być kwestią fakultatywną – staje się imperatywem zarówno dla jednostek, jak i organizacji. W Polsce funkcjonuje kompleksowy Program Rozwoju Kompetencji Cyfrowych, którego celem jest zapewnienie każdemu obywatelowi możliwości podnoszenia umiejętności cyfrowych na różnych etapach życia, począwszy od edukacji wczesnoszkolnej, aż po wsparcie dorosłych pracowników i seniorów. Program ten ma również za zadanie wspierać rozwój rynku pracy oraz włączenie społeczne poprzez eliminowanie luk kompetencyjnych związanych z technologiami cyfrowymi

(Monitor Polski, 2023). Strategie rozwoju kompetencji cyfrowych w kontekście cyberbezpieczeństwa zakładają nie tylko zdobywanie wiedzy teoretycznej, ale przede wszystkim nabywanie praktycznych umiejętności adaptacyjnych, które umożliwiają użytkownikom świadomość zagrożeń oraz właściwe reagowanie w sytuacjach ryzykownych. Badania nad kompetencjami cyfrowymi podkreślają, że są one kluczowe dla funkcjonowania we współczesnym środowisku pracy, w którym technologie cyfrowe stały się narzędziem codziennych zadań zawodowych (European Training Foundation, 2018).

W skali europejskiej funkcjonują ramy takie jak Digital Competence Framework for Citizens (DigComp), które wskazują obszary kluczowe dla rozwoju kompetencji cyfrowych i są to:

1. Informacja i dane.

Ten segment obejmuje umiejętność wyszukiwania, gromadzenia, analizowania i oceniania informacji cyfrowej. Użytkownik powinien być zdolny do identyfikowania wartościowych źródeł informacji, rozróżniania ich wiarygodności oraz rozumienia znaczenia danych w określonym kontekście. Ta kompetencja jest fundamentalna, gdyż właściwe zarządzanie informacją jest podstawą podejmowania świadomych decyzji oraz unikania dezinformacji i manipulacji.

2. Komunikacja i współpraca.

Kompetencje w tym obszarze dotyczą efektywnego uczestnictwa w środowisku cyfrowym, w tym komunikowania się, współdzielenia zasobów, pracy w zespołach online oraz uczestnictwa w społecznościach cyfrowych. Istotna jest również umiejętność dostosowania komunikacji do różnych narzędzi i kulturowych kontekstów oraz rozumienie zasad netykiety. W kontekście bezpieczeństwa umiejętność ta zmniejsza ryzyko błędów wynikających z nieporozumień komunikacyjnych i pomaga w koordynacji działań związanych z reagowaniem na występujące incydenty.

3. Tworzenie treści cyfrowych.

Ten obszar odnosi się do tworzenia, przetwarzania i prezentowania treści cyfrowych – zarówno prostych, jak i bardziej złożonych. Obejmuje to edycję i integrację różnych formatów danych, programowanie, a także rozumienie zasad praw autorskich i licencjonowania. Umiejętność ta pozwala użytkownikom nie tylko „konsumować" treści, lecz aktywnie je kreować i modyfikować zgodnie z ich potrzebami.

4. Bezpieczeństwo.

Kompetencje bezpieczeństwa odnoszą się do świadomego i odpowiedzialnego korzystania z technologii z uwzględnieniem ochrony własnej i innych osób. Obejmują ochronę danych osobowych, prywatności, zarządzanie tożsamością cyfrową oraz rozumienie i stosowanie zasad bezpieczeństwa informatycznego. Kompetencje w tym obszarze są szczególnie ważne w kontekście cyberzagrożeń – przeciwdziałanie wyciekom, ochrona przed atakami socjotechnicznymi czy właściwe zabezpieczanie urządzeń są elementami codziennego cyberdziałania.

5. Rozwiązywanie problemów.

Ostatni obszar dotyczy identyfikowania potrzeb i zasobów cyfrowych oraz podejmowania świadomych decyzji co do wyboru narzędzi i sposobów ich zastosowania. Umiejętność rozwiązywania problemów cyfrowych polega na stosowaniu logicznego myślenia, analizie błędów i optymalizacji procesów, a także adaptacji do nowych technologii. Kompetencje te umożliwiają użytkownikom radzenie sobie z nowymi wyzwaniami oraz efektywne wykorzystywanie technologii w różnych kontekstach życia zawodowego i prywatnego.

Ramy te stanowią punkt odniesienia dla tworzenia programów szkoleniowych i polityk edukacyjnych w państwach członkowskich, w tym również w Polsce.

W praktyce przyjęty jest „model 4K", który wyróżnia cztery główne kompetencje:

- krytyczne myślenie – zdolność do analizy informacji, oceny ich wiarygodności oraz dostrzegania potencjalnych zagrożeń w środowisku cyfrowym. Użytkownik potrafiący myśleć krytycznie nie reaguje automatycznie na otrzymane komunikaty, lecz weryfikuje ich źródło i kontekst. Ma to szczególne znaczenie w przypadku phishingu czy dezinformacji, gdzie emocjonalny przekaz ma skłonić do pochopnych działań,
- kreatywność – to umiejętność poszukiwania nowych rozwiązań problemów oraz elastycznego wykorzystywania dostępnych narzędzi. Nie chodzi wyłącznie o tworzenie treści, lecz o twórcze podejście do bezpieczeństwa i organizacji pracy,

- komunikacja – zdolność jasnego przekazywania informacji w kanałach cyfrowych oraz właściwe rozumienie otrzymywanych treści. W kontekście cyberbezpieczeństwa ważne jest precyzyjne zgłaszanie incydentów i ostrzeganie współpracowników przed zagrożeniami. Użytkownik kompetentny komunikacyjnie potrafi opisać problem techniczny w sposób jasny i zrozumiały,
- kooperacja – umiejętność współpracy z innymi przy wykorzystaniu narzędzi cyfrowych oraz wspólnego rozwiązywania problemów bezpieczeństwa. Cyberzagrożenia rzadko dotyczą pojedynczej osoby, dlatego kluczowe jest działanie zespołowe (Nowa Era, 2024).

Rozwój kompetencji cyfrowych nie jest procesem jednorazowym ani jednowymiarowym. W praktyce obejmuje różne formy edukacji, od formalnego kształcenia w szkołach i na uczelniach aż po działania samokształceniowe i inicjatywy organizacyjne. Jak zauważają autorzy raportu UNESCO (2021), edukacja cyfrowa powinna być integralną częścią nauczania na wszystkich poziomach, aby przygotować obywateli do aktywnego i bezpiecznego uczestnictwa we współczesnym społeczeństwie informacyjnym.

Edukacji formalnej, która obejmuje system szkolnictwa podstawowego, średniego i wyższego, warto podkreślić, że elementy kompetencji cyfrowych są coraz częściej wpisane w program nauczania. W Polsce zgodnie z podstawą programową elementy komunikacyjne i informatyki uwzględniają zagadnienia związane z bezpieczeństwem w sieci (Dziennik Ustaw RP, 2018). Marlena Plebańska podkreśla, że system edukacji formalnej – od etapu szkoły podstawowej po studia – stanowi pierwszą i najważniejszą ścieżkę nabywania kompetencji cyfrowych, integrując wiedzę teoretyczną z praktycznymi działaniami edukacyjnymi (Plebańska, 2023).

W literaturze zwraca się uwagę, że edukacja w obszarze mediów i technologii musi nadążać za zmianami rzeczywistości cyfrowej. Grzegorz Ptaszek (2019) podkreśla: „edukacja medialna musi rozwijać się równolegle do zmian rzeczywistości". Tę zasadę można bezpośrednio odnieść do kompetencji cyfrowych w organizacjach: jeżeli szkolenie i praktyki nie są aktualizowane, użytkownicy działają według nieadekwatnych schematów, co zwiększa podatność na błędy i manipulacje.

Z perspektywy szkolnictwa wyższego interesujące są również polskie opracowania wskazujące, że problematyka bezpieczeństwa i zagrożeń

w społeczeństwie informacyjnym bywa w programach kształcenia ujmowana niewystarczająco – co uzasadnia potrzebę bardziej systemowego włączania elementów bezpieczeństwa cyfrowego do edukacji formalnej (Stachowiak, 2012). W konsekwencji, sensowne projektowanie ścieżek edukacyjnych powinno łączyć treści kompetencyjne (informacja, komunikacja, tworzenie treści, bezpieczeństwo, rozwiązywanie problemów) z praktyką i odpowiedzialnością użytkownika, ponieważ dopiero taki model buduje trwałe zachowania w środowisku cyfrowym.

Edukacja pozaformalna stanowi obecnie jeden z najważniejszych filarów rozwoju kompetencji cyfrowych, zwłaszcza wśród osób dorosłych, które zakończyły już etap kształcenia szkolnego. W odróżnieniu od edukacji formalnej ma ona charakter elastyczny, krótkookresowy i silnie powiązany z praktycznymi potrzebami użytkowników oraz rynku pracy. Forma edukacji pozaformalnej jest bardzo zróżnicowana. Obejmuje kursy i warsztaty organizowane przez instytucje społeczne, uczelnie trzeciego wieku (UTW), organizacje pozarządowe oraz działania realizowane w ramach programów publicznych i unijnych, które adresują potrzeby rozwojowe osób dorosłych. W kontekście kompetencji cyfrowych szczególnie ważne są programy skoncentrowane na praktycznych umiejętnościach, tj. bezpieczne korzystanie z narzędzi cyfrowych, zarządzanie informacją czy reagowanie na zagrożenia w sieci – to one uzupełniają formalne treści edukacyjne i pozwalają użytkownikom na bieżąco aktualizować swoją wiedzę. Edukacja pozaformalna jest ściśle powiązana z pojęciem *uczenia się przez całe życie* (lifelong learning) – koncepcji uznanej za kluczową w politykach edukacyjnych Unii Europejskiej i szeroko opisaną w kontekście kompetencji cyfrowych.

Z kolei samokształcenie to proces indywidualnego rozwijania umiejętności i wiedzy poza formalnymi i instytucjonalnymi strukturami edukacyjnymi. W praktyce oznacza to korzystanie z zasobów cyfrowych - platformy np. NAVOICA, tutoriale wideo, webinaria, materiały open access, a także aktywne uczestnictwo w społecznościach praktyków i forach dyskusyjnych. W polskich realiach samokształcenie w obszarze cyfrowym zyskuje szczególne znaczenie wśród osób dorosłych, które muszą reagować na zmiany w miejscu pracy lub w życiu codziennym – od korzystania z e-administracji po świadome zabezpieczanie swoich danych (Ćwiek, Maj-Serwatka, 2024).

W świecie, w którym technologie zmieniają się szybciej niż procedury i regulaminy, to właśnie zdolność do uczenia się, aktualizowania wiedzy

decyduje o rzeczywistej dojrzałości cyfrowej. Edukacja formalna wyznacza kierunek, pozaformalna nadaje mu praktyczny wymiar, a samokształcenie pozwala reagować na to, czego nie przewidziały żadne programy nauczania. Dopiero ich połączenie sprawia, że kompetencje cyfrowe przestają być teorią, a stają się codziennym nawykiem działania. W tym sensie rozwój użytkownika staje się najtrwalszym mechanizmem cyberbezpieczeństwa – cichym, lecz skuteczniejszym niż najbardziej zaawansowane technologie.

Bariery w podnoszeniu kompetencji cyfrowych

Podnoszenie kompetencji cyfrowych we współczesnych organizacjach – i szerzej w społeczeństwie – napotyka na wiele przeszkód, które wynikają zarówno z ograniczeń strukturalnych, jak i indywidualnych oraz organizacyjnych. W podnoszeniu kompetencji cyfrowych zwykle nie przeszkadza jeden czynnik, tylko zestaw barier nakładających się na siebie – od „twardych" (sprzęt, łącze, środowisko pracy) po „miękkie" (postawy, motywacja, kultura organizacyjna).

Najnowsze badania i analizy wskazują, że rozwój tych kompetencji nie jest automatyczną konsekwencją dostępu do narzędzi cyfrowych, lecz procesem zależnym od szeregu uwarunkowań, których pokonywanie wymaga świadomego planowania i wsparcia (Urząd Marszałkowski Województwa Śląskiego, 2025). W analizach dotyczących polskich przedsiębiorstw jako najczęściej występujące przeszkody wskazuje się przede wszystkim: brak czasu na rozwój, niedostateczne wsparcie ze strony organizacji, niską świadomość znaczenia kompetencji cyfrowych oraz trudności w identyfikowaniu realnych potrzeb szkoleniowych (Dernowska-Żaczyk, Smarzewska, 2024). Autorzy badań podkreślają, że nawet dobrze zaprojektowane programy edukacyjne nie przynoszą oczekiwanych rezultatów, jeśli nie towarzyszy im odpowiednia motywacja pracowników oraz spójna polityka organizacyjna.

Istotną rolę odgrywają również bariery o charakterze kulturowym i psychologicznym. Opór wobec zmian technologicznych, obawa przed popełnieniem błędu czy przekonanie o niskiej przydatności nowych umiejętności prowadzą do powierzchownego uczestnictwa w szkoleniach i braku trwałej zmiany zachowań (Dernowska-Żaczyk, Smarzewska, 2024). W efekcie kompetencje cyfrowe pozostają na poziomie deklaratywnym, nie przekładając się na realne praktyki bezpieczeństwa w środowisku pracy.

Urząd Marszałkowski Województwa Śląskiego (2025) w raporcie wymienia kilka barier rozwoju kompetencji cyfrowych:

- ograniczenia o charakterze finansowym, organizacyjnym oraz społecznym. Środki przeznaczane na projekty cyfryzacyjne często pozostają niewystarczające, co znacząco ogranicza zarówno skalę podejmowanych działań, jak i ich długofalową efektywność. Niedobory te utrudniają tworzenie stabilnych programów edukacyjnych oraz zapewnienie odpowiedniego zaplecza technicznego,
- nierównomierny dostęp do oferty edukacyjnej wynikający z asymetrycznego rozmieszczenia. Ośrodki szkoleniowe i instytucje wspierające rozwój kompetencji cyfrowych koncentrują się głównie w dużych miastach, co powoduje, że mieszkańcy mniejszych miejscowości oraz obszarów peryferyjnych mają znacznie ograniczone możliwości uczestnictwa w tego typu inicjatywach,
- nierównej dystrybucji zasobów, które obejmują zarówno deficyty materialne – tj. brak odpowiedniego sprzętu, dostępu do szybkiego Internetu czy czasu na korzystanie z nowych technologii – jak i ograniczenia w zasobach ludzkich, związane z niewystarczającą wiedzą techniczną i motywacją kadry. Istotne znaczenie mają także zasoby społeczne i kulturowe, w tym brak sieci wsparcia, utrudniony dostęp do wiedzy eksperckiej oraz niskie kompetencje w zakresie świadomego korzystania z usług cyfrowych (Batorski, Płoszej, Jasiewicz, Czerniawska, Peszat, 2012),
- bariery „twarde" (ograniczenia infrastrukturalne i finansowe) i „miękkie" (deficyty wiedzy i umiejętności, obawy psychologiczne, niską motywację do uczenia się, a także zjawisko autowykluczenia cyfrowego),
- możliwości instytucjonalne samorządów, które często nie dysponują wystarczającymi środkami ani narzędziami do inicjowania i koordynowania szeroko zakrojonych projektów cyfryzacyjnych. Ogranicza to ich rolę jako kluczowych aktorów w procesie podnoszenia kompetencji cyfrowych na poziomie regionalnym,
- niskie zainteresowanie części potencjalnych uczestników, zwłaszcza osób powyżej 50 roku życia, dla których udział w szkoleniach

zdalnych bywa mało atrakcyjny lub zbyt wymagający. Skutkuje to częstymi rezygnacjami i osłabieniem efektów programów edukacyjnych,
- niedobór odpowiednio przygotowanej kadry szkoleniowej oraz brak usystematyzowanej wiedzy o realnych potrzebach pracodawców. Informacje dotyczące zapotrzebowania na konkretne umiejętności cyfrowe są rozproszone, co utrudnia projektowanie adekwatnej oferty szkoleniowej.

Analiza barier rozwoju kompetencji cyfrowych pokazuje, że trudności te mają charakter wielowymiarowy i nie ograniczają się wyłącznie do kwestii technicznych. Ostatecznie to nie sama technologia, lecz człowiek decyduje o realnym poziomie bezpieczeństwa cyfrowego organizacji. Dopóki bariery w rozwoju kompetencji będą ograniczać wiedzę, nawyki i gotowość użytkowników do bezpiecznego działania, każda organizacja pozostanie podatna na zagrożenia. Przełamanie tych barier staje się więc nie dodatkiem do strategii cyberbezpieczeństwa, lecz jej warunkiem podstawowym.

Podsumowanie

Przeprowadzone w rozdziale rozważania potwierdzają, że cyberbezpieczeństwo organizacji nie jest wyłącznie funkcją zastosowanych technologii, lecz w dużej mierze zależy od kompetencji cyfrowych użytkowników. Współczesne środowisko pracy, oparte na komunikacji elektronicznej, usługach chmurowych i zdalnym dostępie do danych, powoduje, że użytkownik staje się integralnym elementem systemu bezpieczeństwa informacji, a jego działania mogą zarówno wzmacniać, jak i osłabiać poziom ochrony. Jak wskazuje Plebańska, kompetencje cyfrowe należy rozumieć jako połączenie wiedzy, umiejętności i postaw, które umożliwiają odpowiedzialne funkcjonowanie w społeczeństwie cyfrowym i bezpośrednio wpływają na sposób korzystania z technologii w organizacji (Plebańska, 2023).

Problem główny rozdziału został sformułowany następująco: w jakim stopniu kompetencje cyfrowe warunkują odporność organizacji na cyberataki? Przeprowadzone analizy pozwalają stwierdzić, że kompetencje cyfrowe w znacznym stopniu determinują odporność organizacji, ponieważ wpływają na zdolność użytkowników do rozpoznawania zagrożeń, stosowania procedur bezpieczeństwa oraz reagowania na incydenty. Człowiek jako

użytkownik systemów informatycznych, stanowi bowiem zarówno potencjalne źródło podatności, jak i element pierwszej linii obrony. Celem głównym rozdziału było określenie roli kompetencji cyfrowych użytkowników w budowaniu odporności organizacji na cyberataki. Cel ten został zrealizowany poprzez omówienie znaczenia kompetencji cyfrowych, mechanizmów ich rozwoju oraz barier utrudniających ich podnoszenie. Wykazano, że kompetencje cyfrowe obejmują nie tylko umiejętności techniczne, lecz także wiedzę, postawy oraz nawyki związane z bezpiecznym korzystaniem z technologii. Ich rozwój wymaga podejścia wieloetapowego, obejmującego edukację formalną, pozaformalną oraz samokształcenie.

W świetle przeprowadzonych rozważań można stwierdzić, że kompetencje cyfrowe użytkowników pełnią funkcję strategicznego zasobu organizacji, wpływając bezpośrednio na jej zdolność do zapobiegania, wykrywania oraz reagowania na incydenty cyberbezpieczeństwa. Organizacje, które inwestują w systematyczny rozwój kompetencji cyfrowych swoich pracowników, zwiększają swoją odporność na ataki, natomiast zaniedbania w tym obszarze prowadzą do wzrostu ryzyka operacyjnego i reputacyjnego.

Ostatecznie cyberbezpieczeństwo organizacji nie jest wyłącznie problemem technologicznym, lecz przede wszystkim problemem kompetencyjnym i organizacyjnym. To użytkownik, wyposażony w odpowiednią wiedzę, umiejętności i postawy, decyduje, czy technologia stanie się skutecznym narzędziem ochrony, czy jedynie pozorną barierą wobec zagrożeń. W tym sensie rozwój kompetencji cyfrowych należy uznać za jeden z kluczowych filarów budowania odporności organizacji w erze cyfrowej.

Literatura

1. Batorski, D., Płoszej, A., Jasiewicz, J., Czerniawska, D., Peszat, K. (2012). *Diagnoza i rekomendacje w obszarze kompetencji cyfrowych społeczeństwa i przeciwdziałania wykluczeniu cyfrowemu w kontekście zaprogramowania wsparcia w latach 2014-2020.* Warszawa: Ministerstwo Rozwoju Regionalnego.
2. Ćwiek, M., Maj-Serwatka, K. (2024). *Digital Competence of Young Adults in Poland*. Studia z Polityki Publicznej, 3(368), 46-68. https://doi.org/10.18778/0208-6018.368.03

3. Dernowska-Żaczyk, N., Smarzewska, D. (2024). *The Significance and Advancement of Digital Competencies in Human Capital Management*. Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, 69(2), 38-49. https://doi.org/10.15611/pn.2025.2.04
4. Digital Skills and Jobs Platform. (2020). *Poland Digital Competence Development Programme (2020–2030).* Pobrano z: https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/poland-digital-competence-development-programme-2020-2030 (dostęp: 01.02.2026).
5. DigComp. (b.d.) *Europejskie ramy kompetencji cyfrowych – DigComp.* Pobrano z: https://www.digcomp.pl (dostęp: 01.02.2026).
6. European Training Foundation. (2018). *Digital Skills and Competence, and Digital and Online Learning.* Bruksela: European Training Foundation. Pobrano z: https://www.etf.europa.eu/sites/default/files/2018-10/DSC%20and%20DOL_0.pdf (dostęp: 01.02.2026).
7. European Union Agency for Cybersecurity (ENISA). (2020). *Cybersecurity Skills Development in the EU.* Athens: European Union Agency for Cybersecurity (ENISA). Pobrano z: https://www.enisa.europa.eu/publications/cybersecurity-skills-development-in-the-eu (dostęp: 01.02.2026).
8. IBM Security, Ponemon Institute. (2024). *Cost of a Data Breach Report 2024.* Pobrano z: https://www.ibm.com/reports/data-breach (dostęp: 01.02.2026).
9. Kancelaria Prezesa Rady Ministrów. (2025). *Analiza bezpieczeństwa polskiego Internetu w 2024 roku.* Pobrano z: https://www.gov.pl/web/baza-wiedzy/analiza-bezpieczenstwa-polskiego-internetu-w-2024-roku (dostęp: 01.02.2026).
10. Khadka K. Barkat Ullah A. (2025) *Human factors in cybersecurity: an interdisciplinary review and framework proposal,* https://doi.org/10.1007/s10207-025-01032-0 (dostęp: 01.02.2026).
11. Komisja Europejska. (2025). Termin: *Umiejętności cyfrowe*. Pobrano z: https://digital-strategy.ec.europa.eu/pl/policies/digital-skills (dostęp: 01.02.2026).
12. Ministerstwo Cyfryzacji. (2022). Termin: *Czym jest cyfrowa higiena?* Pobrano z: https://www.gov.pl/web/cyfryzacja/czym-jest-cyfrowa-higiena (dostęp: 01.02.2026).

13. Ministerstwo Cyfryzacji. (2020). Termin: *Kompetencje cyfrowe.* Pobrano z: https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe (dostęp: 01.02.2026).
14. Monitor Polski. (2023). *Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie ustanowienia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych" (M.P. 2023 poz. 318).* Pobrano z: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20230000318/O/M20230318.pdf (dostęp: 01.02.2026).
15. Nowa Era. (2024). *4K, czyli cztery najważniejsze kompetencje XXI wieku*. Pobrano z: https://www.nowaera.pl/4k-czyli-cztery-najwazniejsze-kompetencje-xxi-wieku (dostęp: 01.02.2026).
16. Pawłowska-Cyprysiak, K., Hildt-Ciupińska, K. (2024). *Kompetencje cyfrowe wymagane na współczesnym rynku pracy – perspektywa pracodawcy.* Media i Społeczeństwo, *20*(1), 257-273. https://doi.org/10.5604/01.3001.0054.6527
17. Plebańska, M. (2023). *Kompetencje cyfrowe i ich cyfrowy rozwój*. Warszawa: Wydawnictwo Difin.
18. Polska Agencja Rozwoju Przedsiębiorczości. (2024). *Rynek pracy, edukacja, kompetencje. Aktualne trendy i wyniki badań.* Pobrano z: https://serwis-uslugirozwojowe.parp.gov.pl/component/content/article/8663-3-raport-rynek-pracy-edukacja-kompetencje-aktualne-trendy-i-wyniki-badan (dostęp: 01.02.2026).
19. Ptaszek, G. (2019). *Edukacja medialna 3.0. Krytyczne rozumienie mediów cyfrowych w dobie Big Data i algorytmizacji*. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.
20. Rogacka, M. (2022). *Kompetencje cyfrowe w miejscu pracy – perspektywa pracowników i pracodawców*. e-mentor, *5*(97), 53-64. https://doi.org/10.15219/em97.1591
21. Siemieniecki, B. (red.). (2012). *Edukacja medialna w świecie ponowoczesnym*. Toruń: Wydaw. Naukowe UMK.
22. Stachowiak, B. (2012). *Problematyka bezpieczeństwa i zagrożenia jednostki w społeczeństwie informacyjnym – podstawy programowe i standardy kształcenia a wymagania rzeczywistości.* W: B. Siemieniecki (red.), Edukacja medialna w świecie ponowoczesnym, Toruń: Wydawnictwo Naukowe UMK.

23. UNESCO. (2021). *Reimagining Our Futures Together: A New Social Contract for Education.* Pobrano z: https://unesdoc.unesco.org/ark:/48223/pf0000379707 (dostęp: 01.02.2026).
24. Urząd Marszałkowski Województwa Śląskiego. (2025). *Badanie identyfikacji barier utrudniających rozwój kompetencji cyfrowych wraz z analizą wpływu wykorzystania technologii informacyjno-komunikacyjnych na rozwój tych kompetencji*. Katowice: Urząd Marszałkowski Województwa Śląskiego.
25. Vademecum Bezpieczeństwa Informacyjnego. (2020). Termin: *Kompetencje cyfrowe*, Pobrano z: https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/10/kompetencje-cyfrowe/ (dostęp: 01.02.2026).
26. Verizon. (2024). 2024 *Data Breach Investigations Report.* Pobrano z: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf (dostęp: 01.02.2026).
27. Włodarczyk, J. (2020). Termin: *Human Firewall*. Pobrano z: https://cyberwiedza.pl/zs/human-firewall (dostęp: 01.02.2026).