Cybersecurity and Law

2026 Nr 1(15)

DOI: 10.35467/cal/215343

Cyberbezpieczeństwo – struktura kosztów a skala organizacji przedsiębiorstw

Cybersecurity – cost structure and scale of business organizations

Katarzyna SZYMAŃSKA
Państwowa Akademia Nauk Stosowanych w Ciechanowie
ORCID: 0000-0003-4131-2484
E-mail: katarzyna.szymanska@pansim.edu.pl

Streszczenie

W artykule dokonano analizy ekonomicznej roli cyberbezpieczeństwa w kontekście cyfryzacji współczesnej gospodarki. Celem artykułu jest próba przedstawienia wyników analizy i roli cyberbezpieczeństwa w gospodarce, ze szczególnym uwzględnieniem ekonomicznych determinant inwestycji w bezpieczeństwo informacji, struktury kosztów związanych z zabezpieczaniem systemów teleinformatycznych oraz ich zróżnicowania w zależności od wielkości przedsiębiorstw. W artykule przeprowadzono przegląd literatury z dziedzin ekonomii, finansów, zarządzania ryzykiem oraz bezpieczeństwa informacji, przedstawiono przyjęte ramy teoretyczne i metodologiczne; a także zaprezentowano wyniki analiz dotyczących wpływu nakładów cyberbezpieczeństwa na procesy decyzyjne w przedsiębiorstwach. Artykuł kończą wnioski rekomendujące wzmacnianie kompetencji z zakresu zarządzania cyberbezpieczeństwem, rozwijanie standaryzacji procesów ochronnych oraz tworzenie narzędzi finansowych wspierających.

Słowa kluczowe
cyberbezpieczeństwo, koszty pośrednie, koszty bezpośrednie, koszty ukryte

Abstract

In this article, an economic analysis of the role of cybersecurity is conducted in the context of the digitalization of the modern economy. The objective of this paper is to present the results of this analysis and to examine the role of cybersecurity in the economy, with particular emphasis on the economic determinants of investments in information security, the cost structure associated with protecting teleinformatic systems, and the variation of these costs depending on the size of the enterprise. The article includes a literature review in the fields of economics, finance, risk management, and information security, introduces the theoretical and methodological framework employed, and presents the results of analyses regarding the impact of cybersecurity expenditure

on decision-making in firms. The article concludes with recommendations to strengthen cybersecurity management competencies, develop standardization of protection processes, and create financial tools to support the smallest entities in particular in improving their cyber resilience.

Keywords

cybersecurity; indirect costs; direct costs; hidden costs

Wprowadzenie

Dynamiczna transformacja cyfrowa współczesnej gospodarki skutkuje rosnącą integracją technologii informacyjno-komunikacyjnych (ang. Information and Communications Technology - ICT) z procesami biznesowymi, co prowadzi do zwiększenia złożoności środowisk organizacyjnych oraz intensyfikacji zależności przedsiębiorstw od infrastruktury teleinformatycznej. Wzrost stopnia informatyzacji, automatyzacji i robotyzacji operacji generuje istotne korzyści w postaci wzrostu produktywności, innowacyjności i efektywności zasobowej, lecz równocześnie eskaluje ryzyko wystąpienia incydentów naruszenia bezpieczeństwa informacji. W tym kontekście cyberbezpieczeństwo należy postrzegać jako fundamentalny element ładu organizacyjnego, obejmujący zarówno aspekty techniczne, jak i ekonomiczne oraz instytucjonalne, a także determinujący zdolność przedsiębiorstw do utrzymania ciągłości działania i zachowania integralności krytycznych zasobów cyfrowych. Analiza roli cyberbezpieczeństwa w gospodarce nabiera zatem znaczenia systemowego, obejmującego interakcje między ryzykiem cybernetycznym a stabilnością funkcjonowania podmiotów gospodarczych.

Cyberbezpieczeństwo[1] jest elementem utrzymania stabilności i bezpieczeństwa w cyberprzestrzeni przedsiębiorstwa. Dąży do zapewnienia osiągnięcia i utrzymania właściwości bezpieczeństwa organizacji i aktywów użytkownika przed odpowiednimi cyberzagrożeniami.[2] Wspiera innowacyjność, umożliwia firmom korzystanie z nowoczesnych technologii, takich jak sztuczna inteligencja, *blockchain* czy rozwiązania chmurowe.[3] Odgrywa także kluczową rolę w działalności gospodarczej pod względem różnych obszarów oddziaływania. Szczególnie istotne jest zabezpieczenie systemów łączących funkcje informacyjne i operacyjne, ponieważ ich zainfekowanie może mieć skutki również w kontekście bezpieczeństwa użytkowników. Stąd też firmy muszą inwestować w rozwiązania ochrony danych, takie jak szyfrowanie, zabezpieczenia sieciowe, czy systemy wielopoziomowego uwierzytelniania.[4] Nakłady na odpowiednie rozwiązania zabezpieczające nie tylko pomagają ograniczyć te ryzyka, lecz również przynoszą znaczące korzyści, takie jak zaufanie klientów, spełnianie norm prawnych czy podnoszenie wydajności operacyjnej.

Celem artykułu jest próba przedstawienia wyników analizy i roli cyberbezpieczeństwa w gospodarce, ze szczególnym uwzględnieniem

[1] Cyberbezpieczeństwo to zbiór narzędzi, zasad, koncepcji bezpieczeństwa, zabezpieczeń, wytycznych, metod zarządzania ryzykiem, działań, szkoleń, najlepszych praktyk, gwarancji i rozwiązań technologicznych, które można wykorzystać do ochrony cyberśrodowiska organizacji oraz aktywów użytkownika.

[2] R.A. Janczewski, Cyberwalka. Militarny wymiar działań, Warszawa 2023, s. 57.

[3] M. Włodarczyk, Ewolucja gospodarki cyfrowej w świetle hipotezy twórczej destrukcji J.A. Schumpetera, Kraków 2024, s. 44.

[4] D. Kacprowicz, Ocena bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne, Szczecin 2024, s. 99.

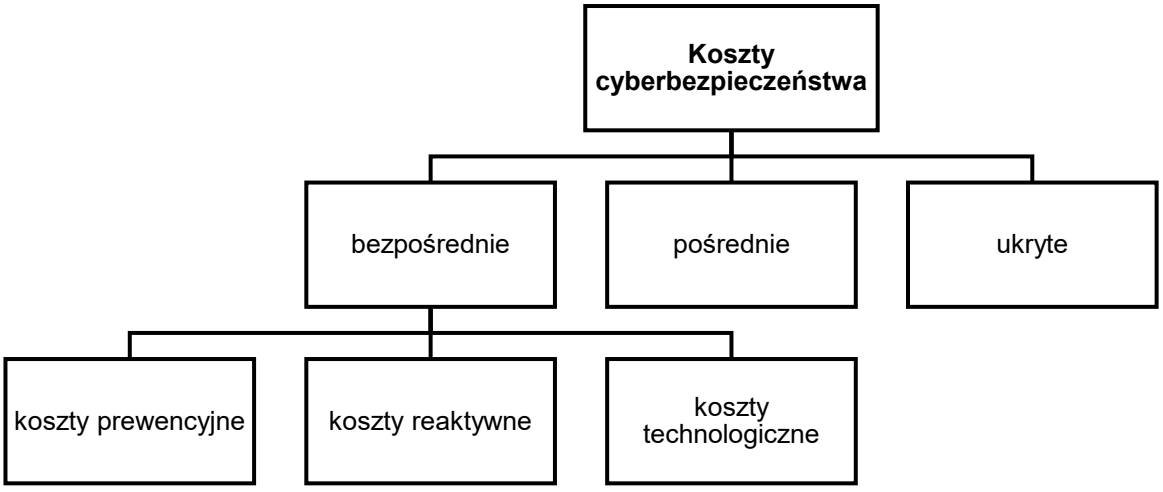
ekonomicznych determinant inwestycji w bezpieczeństwo informacji, struktury kosztów związanych z zabezpieczaniem systemów teleinformatycznych oraz ich zróżnicowania w zależności od wielkości przedsiębiorstw.

W artykule przeprowadzono przegląd literatury z dziedzin ekonomii, finansów, zarządzania ryzykiem oraz bezpieczeństwa informacji, przedstawiono przyjęte ramy teoretyczne i metodologiczne; a także zaprezentowano wyniki analiz dotyczących wpływu nakładów cyberbezpieczeństwa na procesy decyzyjne w przedsiębiorstwach. Metodologia obejmuje podejście empiryczne, polegające na analizie kosztów cyberbezpieczeństwa w przedsiębiorstwach o zróżnicowanej skali działalności i strukturze organizacyjnej. Wyniki analizy wskazują, że mikro- i małe przedsiębiorstwa napotykają większe bariery finansowe przy wdrażaniu mechanizmów ochronnych, podczas gdy średnie i duże organizacje skłaniają się ku strategicznemu i systemowemu zarządzaniu cyberryzykiem. Rosnące inwestycje w zabezpieczenia okazują się ekonomicznie uzasadnione, ponieważ przyczyniają się do zredukowania ryzyka poważnych incydentów oraz zwiększenia odporności (ang. *resilience*) organizacji. Artykuł kończą wnioski rekomendujące wzmacnianie kompetencji z zakresu zarządzania cyberbezpieczeństwem, rozwijanie standaryzacji procesów ochronnych oraz tworzenie narzędzi finansowych wspierających szczególnie najmniejsze podmioty w podnoszeniu odporności cybernetycznej.

Podział kosztów uwzględniających wydatki na cyberbezpieczeństwo

Ochrona danych, systemów czy infrastruktury IT wymaga określonych czynności zabezpieczających, które wiążą się z różnorodnymi kosztami. Koszty cyberbezpieczeństwa można podzielić na bezpośrednie, pośrednie i ukryte (Rysunek 1).

Rys.1. *Podział kosztów cyberbezpieczeństwa w przedsiębiorstwie*



Źródło: *oprac. na podstawie: J. Dymek, Badanie poziomu realizacji założeń cyberbezpieczeństwa firm i instytucji Unii Europejskiej, Wrocław 2024, s. 119*[5].

[5] R. Koszewski, B. Oręziak, M. Wielec, Wdrożenie metod i instrumentów zapobiegania przestępczości w organizacjach, Warszawa 2021, s. 88; M. Fuksiewicz, Rodzaje i natura cyberataków oraz zarys działań w obszarze cyberbezpieczeństwa infrastruktury informatycznej, Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu 2023, s. 57; A. Wygodny, Metody

Koszty bezpośrednie obejmują wydatki ponoszone przez przedsiębiorstwo w celu zapewnienia cyberbezpieczeństwa, które wynikają bezpośrednio z działań podejmowanych w tym obszarze. „Koszty bezpośrednie wiążą się z naprawą szkód wywołanych cyberprzestępczością. Do tej kategorii kosztów należą: koszty związane z ochroną konsumenta w momencie wycieku danych osobowych, opłata za usługi prawne, koszt odzyskania utraconych danych, naruszenie wizerunku, utrata środków pieniężnych w wyniku włamania na konto bankowe firmy oraz utrata własności intelektualnej”[6].

W ramach tej kategorii można wyróżnić zarówno koszty prewencyjne, jak i reaktywne. Pierwsze obejmują inwestycje w technologie ochronne, takie jak zakup i utrzymanie systemów zabezpieczających, w tym oprogramowania antywirusowe, zapory sieciowe, czy systemy wykrywania i zapobiegania włamaniom.[7] Ponadto przedsiębiorstwa ponoszą wydatki na audyty bezpieczeństwa, testy penetracyjne oraz certyfikację zgodności z normami prawnymi.[8] Koszty reaktywne wynikają z konieczności usuwania skutków ataków cybernetycznych i obejmują wydatki na specjalistyczne usługi związane z analizą incydentów oraz przywracaniem systemów do pełniej sprawności.[9] W przypadku wycieku danych firma może ponosić koszty związane z ochroną konsumentów, w tym wydatki na monitoring tożsamości i rekompensaty finansowe.[10] Istotnym obciążeniem są także opłaty za usługi prawne, wynikające z konieczności obrony przed roszczeniami klientów lub spełnienia wymogów regulacyjnych. Do kosztów bezpośrednich zalicza się również wydatki na odzyskanie utraconych danych oraz przeciwdziałanie naruszeniom wizerunku firmy.[11]

Do kosztów bezpośrednich zalicza się również koszty technologiczne, obejmujące zakup i wdrożenie zabezpieczeń IT, które stanowią pierwszą linię obrony przed cyberatakami. Organizacje inwestują w serwery backupowe[12], urządzenia do przechowywania zaszyfrowanych kopii zapasowych oraz licencje i subskrypcje zaawansowanych narzędzi ochronnych, które pomagają w zapobieganiu i neutralizowaniu zagrożeń.[13] Wydatki te obejmują również ochronę punktów końcowych, takich jak komputery, laptopy czy smartfony.

Koszty pośrednie, choć nie są bezpośrednio związane z konkretnym incydentem, mają istotny wpływ na funkcjonowanie przedsiębiorstwa i wiążą się z zapobieganiem cyberatakom. Ich wartość zazwyczaj można przewidzieć, a ich celem jest minimalizacja ryzyka. „Zaliczane są do nich między innymi: szkolenia pracowników z zakresu cyberbezpieczeństwa, ubezpieczenie od ryzyka

---

prowadzenia audytu cyberbezpieczeństwa - ustawa o KSC, Warszawa 2021, s. 85-86; P. Pelc, Wybrane regulacje dotyczące cyberbezpieczeństwa instytucji finansowych, Cybersecurity and Law 2021, nr 2, s. 135; A. Rychły-Lipińska, W. Kamiński, Bezpieczeństwo informacji w erze pracy zdalnej a rola modelu ISO 27001: 2017, Zeszyty Naukowe Politechniki Częstochowskiej, Częstochowa 2024, s. 114; K. Południak-Gierz, Wpływ dyrektyw 2019/770 oraz 2019/771 na poziom ochrony konsumenta w ramach reżimu rękojmi w prawie polskim, Warszawa 2023, s. 174; J. Antczak, Zarządzanie nakładami na cyberbezpieczeństwo w jednostce gospodarczej [w:] L. Kiełtyka, K. Smoląg (red.), Wybrane uwarunkowania i determinanty rozwoju współczesnych przedsiębiorstw, Toruń 2021, s. 89.

[6] J. Dymek, op.cit., s. 119.

[7] A. Wygodny, op.cit., s. 85-86.

[8] P. Pelc, op.cit., s. 135.

[9] A. Rychły-Lipińska, W. Kamiński, op.cit., s. 114.

[10] K. Południak-Gierz, op.cit., s. 174.

[11] J. Antczak, op.ccit., s. 89.

[12] Kopia danych z pamięci jednego urządzenia zapisana na innym nośniku.

[13] M. Chaikovska, Trendy marketingowe i wyzwania technologiczne transformacji cyfrowych, Odessa 2020, s. 293.

cybernetycznego, doradztwo specjalistyczne, wynagrodzenia pracowników dbających o cyberbezpieczeństwo, zakup licencji na programy antywirusowe oraz koszty związane z bezpieczeństwem danych."[14] W skład tej kategorii wchodzą także wydatki na wdrażanie strategii zabezpieczeń, rozwój systemów kontroli dostępu, przeprowadzanie testów penetracyjnych oraz utrzymanie zaawansowanych narzędzi monitorujących sieć i infrastrukturę IT. Wiele firm ponosi również koszty związane z dokumentowaniem procedur bezpieczeństwa oraz z dostosowaniem systemów do aktualnych przepisów prawnych. Istotnym elementem jest zapobieganie potencjalnym zagrożeniom poprzez utrzymanie centrów operacji bezpieczeństwa, analizę incydentów cybernetycznych oraz wdrażanie systemów automatycznego wykrywania i neutralizowania zagrożeń w czasie rzeczywistym.[15]

Koszty ukryte, choć trudne do zauważenia w bieżącym budżecie, mogą mieć znaczący wpływ na działalność firmy. Wynikają zarówno z inwestycji w cyberbezpieczeństwo, jak i z konsekwencji cyberataków. „Wśród kosztów ukrytych wyróżnić można następujące: wzrost składki ubezpieczeniowej, zwiększenie kosztów finansowania zewnętrznego, zakłócenie działalności operacyjnej, wartość utraconych przychodów z umów, koszty komunikacji z dostawcami i klientami, utratę reputacji, skutki zmian regulacji prawnych, skutki wprowadzonych działań naprawczych w zakresie IT, skutki działań naprawczych w obszarze bezpieczeństwa prawnego, koszty konsultacji w zakresie analizy po włamaniu, utratę zaufania do usług, utratę klientów, utracone relacje z klientami, dewaluację nazwy handlowej czy marki, utratę wartości intelektualnej, koszty usług prawnych."[16]

Koszty związane z cyberbezpieczeństwem obejmują szeroki zakres wydatków, począwszy od inwestycji w technologie ochronne i szkolenia, aż po koszty związane z usuwaniem skutków ataków i utratą reputacji. Przedsiębiorstwa muszą uwzględnić zarówno koszty bezpośrednie, które wynikają z konieczności wdrażania zabezpieczeń, jak i te pośrednie oraz ukryte, które mogą długofalowo wpływać na ich działalność i pozycję na rynku.

Podział kosztów wg klasyfikacji wielkości przedsiębiorstw

Rzeczywistość gospodarcza wymusza na przedsiębiorcach funkcjonowanie w sieci, która staje się konieczna do załatwiania spraw formalnych, ułatwia prowadzenie podmiotu, pozwala na poszerzenie wiedzy, a także może stanowić nowe źródło dochodu. Cyberzagrożenia są jednym z kluczowych rodzajów ryzyka, z którym musi zmierzyć się każda firma, zarówno nowo powstała, jak i długo funkcjonująca na rynku.

Małe firmy często mają ograniczone zasoby finansowe i kadrowe, co sprawia, że ich wydatki na cyberbezpieczeństwo są relatywnie niskie.[17] Czyni je to bardziej podatnymi na incydenty. „Małe przedsiębiorstwa zgłaszają również szereg obaw związanych z wdrażaniem i stosowaniem technologii cyfrowych. Wśród nich znajdują się wielość obowiązków, z których wynika konieczność cyfryzacji, wysokie koszty wdrożenia technologii cyfrowych oraz niedostateczne kompetencje cyfrowe

[14] J. Dymek, op.cit., s. 119.
[15] R. Koszewski, B. Oręziak, M. Wielec, op.cit., s.88.
[16] M. Fuksiewicz, op.cit., s. 57.
[17] P. Barczak, Mała firma niszowa - próba zdefiniowania, Warszawa 2018, s. 25.

małych przedsiębiorców."[18] Jeżeli tego typu instytucje zdecydują się na jakąkolwiek ochronę to skupią się na podstawowych zabezpieczeniach,[19] jednak cyberataki mogą być dla nich szczególnie dotkliwe, ponieważ skutki naruszenia danych mogą prowadzić do poważnych strat finansowych i utraty klientów. Dodatkowym wyzwaniem dla małych przedsiębiorstw jest brak specjalistycznej wiedzy w zakresie cyberbezpieczeństwa, co powoduje, że często nie są one świadome skali zagrożeń i potencjalnych konsekwencji ataków.[20] Wiele z nich nie wdraża polityk bezpieczeństwa ani regularnych aktualizacji oprogramowania, co czyni ich systemy szczególnie podatnymi na ataki *ransomware* i *phishing*. Z tego powodu, nawet niewielkie incydenty mogą skutkować długimi przestojami operacyjnymi, co w przypadku małych firm może oznaczać poważne trudności finansowe, a nawet konieczność zamknięcia działalności.[21] Główne koszty obejmują: podstawowe oprogramowanie zabezpieczające, usługi chmurowe z wbudowanym bezpieczeństwem, szkolenia dla pracowników oraz opłaty związane z wystąpieniem incydentów.

Średnie organizacje, ze względu na większą skalę działalności i liczbę pracowników, są zobowiązane do inwestowania w bardziej zaawansowane systemy zabezpieczeń. Zwykle wybierają model hybrydowy, w którym część ochrony zapewniają wewnętrzne zespoły IT, a pozostałe działania powierzają zewnętrznym specjalistom.[22] Takie podejście pozwala im optymalizować koszty i jednocześnie korzystać z najnowszych technologii oraz ekspertyzy specjalistów ds. cyberbezpieczeństwa. Dodatkowo, średnie przedsiębiorstwa często wdrażają polityki zarządzania tożsamością i dostępem, aby ograniczyć ryzyko nieautoryzowanego dostępu do krytycznych zasobów.[23] Coraz częściej decydują się również na regularne testy penetracyjne i symulacje ataków, które pozwalają wykrywać i eliminować potencjalne luki zabezpieczeniach, zanim zostaną wykorzystane przez cyberprzestępców. Wdrażanie skutecznych mechanizmów ochrony wymaga również odpowiedniej polityki zarządzania incydentami, co oznacza konieczność stworzenia planów reakcji na cyberzagrożenia oraz procedur przywracania ciągłości działania po ewentualnym ataku. Średniego rozmiaru firmy często inwestują w rozwiązania do monitorowania i analizy ruchu sieciowego, które umożliwiają szybsze wykrywanie anomalii i potencjalnych zagrożeń.[24] Ważnym aspektem jest także zabezpieczenie pracy zdalnej oraz integracja różnych systemów IT, co generuje dodatkowe koszty związane z ochroną urządzeń końcowych i kontrolą dostępu do firmowych zasobów. Do głównych kosztów zaliczają się: zaawansowane systemy zabezpieczeń IT, outsourcing usług cyberbezpieczeństwa, regularne audyty bezpieczeństwa, rozbudowane szkolenia dla personelu oraz opłaty związane z ubezpieczeniem cybernetycznym.

---

[18] M. Rydzewska, I. Majchrzak, Cyfryzacja podatków – korzyści i wyzwania dla małych przedsiębiorstw i księgowych, Biała Podlaska 2023, s. 113.
[19] L. Klapkiv, Zakres ryzyka i szkód w cyberubezpieczeniu dla małych i średnich przedsiębiorstw, Lublin 2022, s. 33.
[20] K. Czaplicki, A. Gryszczyńska, G. Szpor (red.), Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Warszawa 2019, s. 29.
[21] G. Strupczewski, Ryzyko cybernetyczne jako wyzwanie dla branży ubezpieczeń w Polsce i na świecie, Warszawa 2017, s. 257.
[22] Z. Handzel, K. Tyl, W. Urbanczyk, Studia w zakresie cyberbezpieczeństwa, a zapewnienie potrzeb bezpieczeństwa IT/OT w przedsiębiorstwach, Zeszyty Naukowe Wyższej Szkoły Ekonomii i Informatyki 2024, s. 135.
[23] J. Antczak, op.cit., s. 99.
[24] A. Pawłowska, M. Pawłowski, Zarządzanie kryzysem w małym i średnim przedsiębiorstwie - perspektywa przerwy w działalności gospodarczej, Lublin 2022, s. 12.

Duże przedsiębiorstwa są szczególnie narażone na ryzyko cyberataków ze względu na skalę działalności oraz ogromne ilość przetwarzanych danych, co czyni je atrakcyjnym celem dla cyberprzestępców. W związku z tym są zobowiązane do wdrażania najbardziej zaawansowanych rozwiązań oraz utrzymania wyspecjalizowanych zespołów ds. cyberbezpieczeństwa.[25] Dodatkowo, wymogi regulacyjne oraz złożona struktura operacyjna wymagają od nich kompleksowego i strategicznego podejścia do ochrony danych i systemów informatycznych.[26] Wysoki poziom ryzyka cybernetycznego wymusza na dużych firmach stosowanie wielowarstwowych zabezpieczeń oraz stałe monitorowanie zagrożeń. Aby skutecznie chronić swoje zasoby, przedsiębiorstwa wdrażają systemy detekcji i reagowania na incydenty, sztuczną inteligencję do analizy podejrzanych aktywności, a także technologie automatyzujące zarządzanie bezpieczeństwem.[27] Ochrona przed cyberatakami wymaga również koordynacji działań pomiędzy różnymi działami organizacji, co wiąże się z koniecznością tworzenia spójnych polityk bezpieczeństwa i regularnych audytów wewnętrznych oraz zewnętrznych. Firmy muszą także uwzględniać ryzyka związane z pracą zdalną i integracją z systemami partnerów biznesowych, co dodatkowo zwiększa koszty i stopień skomplikowania wdrażanych rozwiązań. Do głównych kosztów należą: zaawansowane infrastruktura IT, działy ds. cyberbezpieczeństwa, zarządzanie ryzykiem i zgodność z regulacjami, testy penetracyjne i symulacje cyberataków, wysokie ubezpieczenie cybernetyczne oraz zabezpieczenie łańcucha dostaw. Poziom inwestycji dopasowany do wielkości przedsiębiorstwa zestawiono w tabeli 1.

Tabela 1. *Koszty małych, średnich i dużych przedsiębiorstw*

	Wielkość przedsiębiorstwa		
	Małe	**Średnie**	**Duże**
Poziom inwestycji	Niski	Średni	Wysoki
Rodzaj zabezpieczeń	Podstawowe oprogramowanie	Zaawansowane systemy IT	Wielowarstwowe rozwiązania
Wsparcie zewnętrzne	Sporadyczne	Częściowy outsourcing	Stała współpraca z ekspertami
Polityki bezpieczeństwa	Rzadko wdrażane	Standardowe regulacje	Pełna strategia bezpieczeństwa
Szkolenia pracowników	Minimalne lub brak	Regularne szkolenia	Zaawansowane programy edukacyjne
Testy penetracyjne i audyty	Sporadyczne lub brak	Regularne	Ciągłe oraz stymulacje ataków
Zarządzanie incydentami	Działania reaktywne	Opracowany plan reagowania	Pełna strategia
Koszty incydentów	Wysokie w stosunku do zasobów	Znaczące, ale zarządzalne	Wysokie, ale uwzględnione w budżecie
Ubezpieczenie cybernetyczne	Brak lub podstawowe	Standardowe	Pełne

Źródło: *opracowanie własne.*

[25] L. Klapkiv, Zakres ryzyka i szkód w cyberubezpieczeniu dla małych i średnich przedsiębiorstw, Lublin 2022, s. 33.
[26] E. Makoś, Zarządzanie bezpieczeństwem informacji i zachowanie bezpieczeństwa w systemie informatycznym, Studenckie Zeszyty Naukowe 2022, s. 138.
[27] N. Malec, Sztuczna inteligencja a bezpieczeństwo państwa, Prawo i Bezpieczeństwo – Law & Security 2024, s. 27.

Koszty cyberbezpieczeństwa rosną wraz z wielkością przedsiębiorstwa, zależnie od dostępnych zasobów i poziomu zagrożeń. Małe firmy ograniczają wydatki do podstawowych zabezpieczeń, co zwiększa ich podatność na ataki. Średnie przedsiębiorstwa stosują bardziej zaawansowane rozwiązania, łącząc wewnętrzne zespoły IT z outsourcingiem, co pozwala im skuteczniej zarządzać ryzykiem. Duże firmy inwestują w kompleksowe systemy ochrony, sztuczną inteligencję i audyty, co wiąże się z najwyższymi kosztami, ale zapewnia lepszą odporność na cyberzagrożenia.

Podsumowanie

Wzrost stopnia informatyzacji i złożoności środowiska teleinformatycznego bezpośrednio wpływa na skalę ekspozycji na cyberzagrożenie, co wymusza systematyczne podnoszenie poziomu cyberodporności przedsiębiorstw. Cyberbezpieczeństwo należy zatem postrzegać nie tylko jako obszar działań technicznych, lecz jako komponent strategiczny, determinujący zdolność organizacji do zachowania ciągłości działania, ochrony zasobów informacyjnych i utrzymania przewagi konkurencyjnej.

Analiza struktury kosztów związanych z bezpieczeństwem informacji wykazała, że stanowią one zróżnicowaną kategorię obejmującą zarówno nakłady kapitałowe, jak i koszty operacyjne, które w sposób systemowy wpływają na funkcjonowanie przedsiębiorstwa. Uwzględnienie podziału przedsiębiorstw według ich wielkości potwierdziło istnienie istotnych różnic w strukturze kosztów, poziomie dojrzałości technologicznej oraz zdolności implementacji zaawansowanych rozwiązań ochronnych.

Podsumowując, cyberbezpieczeństwo w coraz większym stopniu staje się kategorią ekonomiczną, której znaczenie wykracza poza obszar technologii informacyjnych i obejmuje strategiczne zarządzanie ryzykiem, finanse przedsiębiorstw oraz polityki organizacyjne. Wyniki badań wskazują na konieczność dalszej integracji podejścia technicznego, ekonomicznego i instytucjonalnego, a także na potrzebę rozwijania modeli analitycznych pozwalających na precyzyjną ocenę opłacalności inwestycji w bezpieczeństwo informacji. W praktyce gospodarczej rekomenduje się wzmacnianie kompetencji z zakresu zarządzania cyberbezpieczeństwem, rozwijanie standaryzacji procesów ochronnych oraz tworzenie narzędzi finansowych wspierających szczególnie najmniejsze podmioty w podnoszeniu odporności cybernetycznej.

Bibliografia

Antczak J., Zarządzanie nakładami na cyberbezpieczeństwo w jednostce gospodarczej, [w:] L. Kiełtyka, K. Smoląg (red.), Wybrane uwarunkowania i determinanty rozwoju współczesnych przedsiębiorstw, Toruń 2021.

Barczak P., Mała firma niszowa - próba zdefiniowania, Warszawa 2018.

Chaikovska M., Trendy marketingowe i wyzwania technologiczne transformacji cyfrowych, Odessa 2020,

Czaplicki K., Gryszczyńska A., Szpor G. (red.), Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Warszawa 2019.

Dymek J., Badanie poziomu realizacji założeń cyberbezpieczeństwa firm i instytucji Unii Europejskiej, Wrocław 2024.

Fuksiewicz M., Rodzaje i natura cyberataków oraz zarys działań w obszarze cyberbezpieczeństwa infrastruktury informatycznej, Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu 2023.
Handzel Z., Tyl K., Urbanczyk W., Studia w zakresie cyberbezpieczeństwa, a zapewnienie potrzeb bezpieczeństwa IT/OT w przedsiębiorstwach, Zeszyty Naukowe Wyższej Szkoły Ekonomii i Informatyki 2024.
Janczewski R.A., Cyberwalka. Militarny wymiar działań, Warszawa 2023.
Kacprowicz D., Ocena bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne, Szczecin 2024.
Klapkiv L., Zakres ryzyka i szkód w cyberubezpieczeniu dla małych i średnich przedsiębiorstw, Lublin 2022.
Koszewski R., Oręziak B., Wielec M., Wdrożenie metod i instrumentów zapobiegania przestępczości w organizacjach, Warszawa 2021.
Makoś E., Zarządzanie bezpieczeństwem informacji i zachowanie bezpieczeństwa w systemie informatycznym, Studenckie Zeszyty Naukowe 2022.
Malec N., Sztuczna inteligencja a bezpieczeństwo państwa, Prawo i Bezpieczeństwo – Law & Security 2024.
Pawłowska A., Pawłowski M., Zarządzanie kryzysem w małym i średnim przedsiębiorstwie - perspektywa przerwy w działalności gospodarczej, Lublin 2022.
Pelc P., Wybrane regulacje dotyczące cyberbezpieczeństwa instytucji finansowych, Cybersecurity and Law 2021, nr 2.
Południak-Gierz K., Wpływ dyrektyw 2019/770 oraz 2019/771 na poziom ochrony konsumenta w ramach reżimu rękojmi w prawie polskim, Warszawa 2023.
Rychły-Lipińska A., Kamiński W., Bezpieczeństwo informacji w erze pracy zdalnej a rola modelu ISO 27001: 2017, Zeszyty Naukowe Politechniki Częstochowskiej, Częstochowa 2024.
Rydzewska M., Majchrzak I., Cyfryzacja podatków – korzyści i wyzwania dla małych przedsiębiorstw i księgowych, Biała Podlaska 2023.
Strupczewski G., Ryzyko cybernetyczne jako wyzwanie dla branży ubezpieczeń w Polsce i na świecie, Warszawa 2017.
Włodarczyk M., Ewolucja gospodarki cyfrowej w świetle hipotezy twórczej destrukcji J.A. Schumpetera, Kraków 2024.
Wygodny A., Metody prowadzenia audytu cyberbezpieczeństwa - ustawa o KSC, Warszawa 2021.