Dominika Lewandowska
Państwowa Akademia Nauk Stosowanych
im. Ignacego Mościckiego w Ciechanowie
Wydział Inżynierii i Ekonomii

https://doi.org/10.64158/lc8sf8pk3z

Zróżnicowanie kosztów cyberbezpieczeństwa w małych, średnich i dużych przedsiębiorstwach – ujęcie porównawcze

Streszczenie: W artykule omówiono zagadnienie zróżnicowania kosztów cyberbezpieczeństwa w zależności od wielkości przedsiębiorstwa. Przedstawiono podział kosztów na bezpośrednie (np. zakup oprogramowania zabezpieczającego, koszty obsługi incydentów), pośrednie (np. szkolenia, ubezpieczenia, doradztwo) oraz ukryte (np. utrata reputacji, przerwy w działalności, odejście klientów). Na podstawie analizy wykazano, że małe firmy inwestują w cyberbezpieczeństwo najmniej, co czyni je bardziej podatnymi na ataki. Średnie przedsiębiorstwa korzystają z modelu hybrydowego (wewnętrzne zespoły i outsourcing), natomiast duże formy wdrażają zaawansowane rozwiązania oparte m.in. na sztucznej inteligencji i systemach monitoringu 24/7. Wywnioskować można, że choć cyberbezpieczeństwo generuje istotne koszty, jego brak może prowadzić do znacznie poważniejszych strat, dlatego traktowanie go jako inwestycji, a nie tylko wydatku jest kluczowe dla stabilności przedsiębiorstwa.

Słowa kluczowe: cyberbezpieczeństwo, koszty, koszty cyberbezpieczeństwa, koszty bezpośrednie, koszty pośrednie, koszty ukryte, małe przedsiębiorstwa, średnie przedsiębiorstwa, duże przedsiębiorstwa

Wprowadzenie

Przedsiębiorstwa coraz częściej muszą mierzyć się z wyzwaniami związanymi z ochroną zasobów cyfrowych. W dobie postępującej technologii i rosnącej liczby zagrożeń w cyberprzestrzeni, zapewnienie odpowiedniego poziomu bezpieczeństwa staje się nieodzownym elementem prowadzenia działalności gospodarczej. Koszty związane z cyberbezpieczeństwem są nieuniknione, jednak ich charakter oraz wpływ na działalność gospodarczą wymagają szerszego spojrzenia niż jedynie przez pryzmat wydatków operacyjnych.[1]

[1] A. Ferens, *Cyberbezpieczeństwo i cyberryzyko w raportach zintegrowanych i sprawozdaniach zarządu operatorów usług kluczowych*, Wydawnictwo Uniwersytetu Ekonomicznego

Celem niniejszego rozdziału jest przeprowadzenie analizy porównawczej kosztów związanych z wdrożeniem i utrzymaniem systemów cyberbezpieczeństwa w przedsiębiorstwach różnej wielkości – małych, średnich oraz dużych. Szczególny nacisk położono na zróżnicowanie struktury i poziomu tych wydatków w zależności od skali działalności gospodarczej.

Zakres przedstawionej pracy obejmuje analizę podstaw teoretycznych związanych z cyberbezpieczeństwem, identyfikację najczęściej występujących zagrożeń oraz ich wpływu na funkcjonowanie przedsiębiorstw. Uwzględniono w niej również przegląd obowiązujących regulacji prawnych, które określają odpowiedzialność firm w obszarze ochrony danych i systemów informatycznych. W pracy przedstawiono identyfikację kosztów związanych z wystąpieniem incydentów cybernetycznych, ich wdrożeniem, czy całkowitym brakiem. Podano możliwe korzyści reputacyjne i finansowe płynące z wdrożenia odpowiednich środków zabezpieczających oraz inwestycyjne działania państwa w cyberbezpieczeństwo.

1. Koszty związane z cyberbezpieczeństwem

Koszty cyberbezpieczeństwa można podzielić na bezpośrednie, pośrednie i ukryte.

Koszty bezpośrednie obejmują wydatki ponoszone przez przedsiębiorstwo w celu zapewnienia cyberbezpieczeństwa, które są z nim ściśle związane i wynikają bezpośrednio z działań podejmowanych w tym obszarze.[2] „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."[3]

W ramach tej kategorii można wyróżnić zarówno koszty prewencyjne, jak i reaktywne. Pierwsze obejmują inwestycje w technologie ochronne, takie jak

w Katowicach, Katowice 2021, s. 32-33, https://bibliotekanauki.pl/articles/1917418.pdf (dostęp: 05.06.2025r.).

[2] J. Dymek, *Badanie poziomu realizacji założeń cyberbezpieczeństwa firm i instytucji Unii Europejskiej*, Wydawnictwo Uniwersytetu Ekonomicznego, Wrocław 2024, s. 119, https://dbc.wroc.pl/Content/130415/Dymek_Badanie_poziomu_realizacji_zalozen_cyberbezpieczenstwa.pdf (dostęp: 07.02.2025r.).

[3] J. Dymek, *Badanie poziomu realizacji założeń cyberbezpieczeństwa firm i instytucji Unii Europejskiej*, Wydawnictwo Uniwersytetu Ekonomicznego, Wrocław 2024, s. 119, https://dbc.wroc.pl/Content/130415/Dymek_Badanie_poziomu_realizacji_zalozen_cyberbezpieczenstwa.pdf (dostęp: 07.02.2025r.).

zakup i utrzymanie systemów zabezpieczających, w tym oprogramowania antywirusowe, zapory sieciowe, czy systemy wykrywania i zapobiegania włamaniom.[4] Ponadto przedsiębiorstwa ponoszą wydatki na audyty bezpieczeństwa, testy penetracyjne oraz certyfikację zgodności z normami prawnymi.[5]

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.[6] W przypadku wycieku danych firma może ponosić koszty związane z ochroną konsumentów, w tym wydatki na monitoring tożsamości i rekompensaty finansowe.[7] 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.

Warto także wyszczególnić koszty technologiczne, obejmujące zakup i wdrożenie zabezpieczeń IT, które stanowią pierwszą linię obrony przed cyberatakami. Organizacje inwestują w serwery backupowe[8], urządzenia do przechowywania zaszyfrowanych kopii zapasowych oraz licencje i subskrypcje zaawansowanych narzędzi ochronnych, które pomagają w zapobieganiu i neutralizowaniu zagrożeń.[9] 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.[10] „Zaliczane są do nich między innymi: szkolenia

[4] A. Wygodny, *Metody prowadzenia audytu cyberbezpieczeństwa - ustawa o KSC*, Najwyższa Izba Kontroli, 2021, s. 85-86, https://www.nik.gov.pl/plik/id,23959.pdf (dostęp: 15.02.2025r.).

[5] P. Pelc, *Wybrane regulacje dotyczące cyberbezpieczeństwa instytucji finansowych*, Cybersecurity and Law, 2021, s. 135, https://bibliotekanauki.pl/articles/1987417.pdf (dostęp: 08.02.2025r.).

[6] 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, https://bibliotekanauki.pl/articles/40685472.pdf (dostęp: 15.02.2025r.).

[7] K. Południak-Gierz *Wpływ dyrektyw 2019/770 oraz 2019/771 na poziom ochrony konsumenta w ramach reżimu rękojmi w prawie polskim*, Instytut Wymiaru Sprawiedliwości, 2023, s. 174, https://bibliotekanauki.pl/articles/2234017.pdf (dostęp: 15.02.2025r.).

[8] kopia danych z pamięci jednego urządzenia zapisana na innym nośniku

[9] M. Chaikovska, *Trendy marketingowe i wyzwania technologiczne transformacji cyfrowych*, Wydawnictwo Narodowego Uniwersytetu Odeskiego, 2020, s. 293, https://bibliotekanauki.pl/chapters/34111996.pdf (14.02.2025r.).

[10] J. Dymek, *Badanie poziomu realizacji założeń cyberbezpieczeństwa firm i instytucji Unii Europejskiej*, Wydawnictwo Uniwersytetu Ekonomicznego, Wrocław 2024, s. 119, https://dbc.wroc.pl/Content/130415/Dymek_Badanie_poziomu_realizacji_zalozen_cyberbezpieczenstwa.pdf (dostęp: 07.02.2025r.).

pracowników z zakresu cyberbezpieczeństwa, ubezpieczenie od ryzyka cybernetycznego, doradztwo specjalistyczne, wynagrodzenia pracowników dbających o cyberbezpieczeństwo, zakup licencji na programy antywirusowe oraz koszty związane z bezpieczeństwem danych."[11] 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.[12] 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.[13]

Koszty ukryte, choć trudne do zauważenia w bieżącym budżecie, mogą mieć znaczący pływ na działalność firmy. Wynikają zarówno z inwestycji w cyberbezpieczeństwo, jak i z konsekwencji cyberataków. „Wśród kosztów ukrytych wyróżnić można następujące: [14]

- 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."

[11] J. Dymek, Badanie poziomu realizacji…, op. cit., s. 119, (dostęp: 07.02.2025r.).

[12] R. Koszewski, B. Oręziak, M. Wielec, *Wdrożenie metod i instrumentów zapobiegania przestępczości w organizacjach*, Wydawnictwo Instytutu Wymiaru Sprawiedliwości, Warszawa 2021, s. 88.

[13] R. Koszewski, B. Oręziak, M. Wielec, Wdrożenie metod i instrumentów…, op. cit., s. 88.

[14] M. Fuksiewicz, *Rodzaje i natura cyberataków oraz zarys działań w obszarze cyberbezpieczeństwa infrastruktury informatycznej*, Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu 2023, s. 57, https://doi.org/10.58683/dnswsb.615 (dostęp: 08.02.2025r.).

Ukryte konsekwencje cyberataków mogą wpływać na przedsiębiorstwo w długim okresie i prowadzić do trudności w odbudowie pozycji na rynku.

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.

2. Analiza kosztów według rozmiarów przedsiębiorstw

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.

Koszty w małych przedsiębiorstwach

Małe firmy często mają ograniczone zasoby finansowe i kadrowe, co sprawia, że ich wydatki na cyberbezpieczeństwo są relatywnie niskie.[15] 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 małych przedsiębiorców."[16] Jeżeli tego typu instytucje zdecydują się na jakąkolwiek ochronę to skupią się na podstawowych zabezpieczeniach.[17] Jednak cyberataki mogą być dla nich szczególnie dotkliwe, ponie-

[15] P. Barczak, *Mała firma niszowa - próba zdefiniowania*, Szkoła Główna Handlowa w Warszawie, Warszawa 2018, s. 25, https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_5604_01_3001_0012_4726/c/1195-1060.pdf (dostęp: 13.02.2025r.).

[16] M. Rydzewska, I. Majchrzak, *Cyfryzacja podatków – korzyści i wyzwania dla małych przedsiębiorstw i księgowych*, Wydawnictwo Akademii Bialskiej, Biała Podlaska, 2023, s. 113, https://bibliotekanauki.pl/chapters/28408254.pdf (dostęp: 13.02.2025r.).

[17] L. Klapkiv, *Zakres ryzyka i szkód w cyberubezpieczeniu dla małych i średnich przedsiębiorstw*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2022, s. 33, http://dlibra.tu.koszalin.pl/Content/1749/2022_RwD.pdf#page=34 (dostęp: 13.02.2025r.).

waż 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.[18] 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.[19]

Koszty w średnich przedsiębiorstwach

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.[20] 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.[21] 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

[18] K. Czaplicki, A. Gryszczyńska, G. Szpor (red.), Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Wolters Kluwer Polska, Warszawa 2019, s. 29.

[19] G. Strupczewski, *Ryzyko cybernetyczne jako wyzwanie dla branży ubezpieczeń w Polsce i na świecie*, Komitet Nauk o Finansach PAN, Warszawa 2017, s. 259, https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.oai-journals-pan-pl-102470/c/oai-journals-pan-pl-102470_fulltext_Fin._201_10_-17_2015-G.Strupczewski.pdf (dostęp: 13.02.2025r.).

[20] 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, https://bibliotekanauki.pl/articles/56826708.pdf (dostęp: 14.02.2025r.).

[21] J. Antczak, *Zarządzanie bezpieczeństwem informacji w jednostce gospodarczej*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2023, s. 99, https://bibliotekanauki.pl/chapters/27310195.pdf (dostęp: 14.02.2025r).

po ewentualnym ataku. Średniego rozmiaru firmy często inwestują w rozwiązania do monitorowania i analizy ruchu sieciowego, które umożliwiają szybsze wykrywanie anomalii i potencjalnych zagrożeń.[22] 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.

Koszty w dużych przedsiębiorstwach

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.[23] Dodatkowo, wymogi regulacyjne oraz złożona struktura operacyjna wymagają od nich kompleksowego i strategicznego podejścia do ochrony danych i systemów informatycznych.[24]

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.[25] 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.[26]

---

[22] A. Pawłowska, M. Pawłowski, *Zarządzanie kryzysem w małym i średnim przedsiębiorstwie - perspektywa przerwy w działalności gospodarczej*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2022, s. 12, http://dlibra.tu.koszalin.pl/Content/1749/2022_RwD.pdf#page=34 (dostęp: 13.02.2025r.).

[23] L. Klapkiv, *Zakres ryzyka i szkód w cyberubezpieczeniu dla małych i średnich przedsiębiorstw*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2022, s. 33, http://dlibra.tu.koszalin.pl/Content/1749/2022_RwD.pdf#page=34 (dostęp: 13.02.2025r.).

[24] E. Makoś, *ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI I ZACHOWANIE BEZPIECZEŃSTWA W SYSTEMIE INFORMATYCZNYM*, Studenckie Zeszyty Naukowe, 2022, s. 138, https://phavi.umcs.pl/at/attachments/2022/1223/105739-consensus-23.pdf#page=135 (dostęp: 14.02.2025r.).

[25] N. Malec, *Sztuczna inteligencja a bezpieczeństwo państwa*, Prawo i Bezpieczeństwo – Law & Security, 2024, s. 27, https://bibliotekanauki.pl/articles/56029077.pdf (dostęp: 14.02.2025r.).

[26] Komitet Kontaktowy, *Cyberbezpieczeństwo w UE i państwach członkowskich UE*, Europejski Trybunał Obrachunkowy, 2020, s. 15, https://www.eca.europa.eu/sites/cc/Lists/

3. Przykłady kosztów

Bezpieczeństwo w świecie cyfrowym stanowi kluczowy element strategii ochrony danych i systemów informatycznych w przedsiębiorstwach. W zależności od wielkości działalności różni się zarówno poziom zagrożeń, jak i środki przeznaczone na zabezpieczenia.[27]

Podstawowe rozwiązania zabezpieczające są fundamentem ochrony każdej firmy. Niezależnie od rozmiaru korporacji, pewne środki muszą być wdrożone, aby zapewnić podstawowy poziom ochrony. „Bezpieczeństwo IT rozumiane jest jako bezpieczeństwo, w którym dane są najważniejszym aktywem, których bezpieczeństwo powinno być brane pod uwagę w pierwszej kolejności. Dla wielu firm jednakże zakłócenie działalności operacyjnej może przynieść wielkie szkody."[28]

Tabela 1. Przykładowe koszty cyberbezpieczeństwa w różnych rodzajach przedsiębiorstw

	Wielkość przedsiębiorstwa		
Przykładowe koszty	**Małe**	**Średnie**	**Duże**
Oprogramowanie antywirusowe i firewall	X	X	X
Zarządzanie tożsamością i dostępem (IAM, MFA)	X	X	X
Ochrona poczty e-mail (Anti-Phishing)	X	X	X
Ochrona przed atakami ransomware	X	X	X
Systemy wykrywania i zapobiegania włamaniom (IDS/IPS)		X	X
Monitoring bezpieczeństwa 24/7		X	X
Rozwiązania SIEM (monitorowanie i analiza zagrożeń)		X	X
Zaawansowana analiza zagrożeń (AI/ML)			X
Zespół reagowania na incydenty (SOC)			X
Wdrożenie polityki zero-trust			X

CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_PL.pdf.com (dostęp: 14.02.2025r.).

[27] K. Kurkiewicz, *Wielowymiarowy aspekt gospodarki elektronicznej z uwzględnieniem kwestii bezpieczeństwa*, Wydawnictwo Akademii Bialskiej, Biała Podlaska, 2024, s. 7-8, https://bibliotekanauki.pl/chapters/55795572.pdf (dostęp: 14.02.2025r.).

[28] 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, https://bibliotekanauki.pl/articles/56826708.pdf (dostęp: 14.02.2025r.).

cd. tabeli 1

	Wielkość przedsiębiorstwa		
Przykładowe koszty	**Małe**	**Średnie**	**Duże**
Ubezpieczenie od cyberataków		X	X
Dedykowany dział cyberbezpieczeństwa			X
Fizyczne zabezpieczenia serwerowni			X

Źródło: opracowanie własne.

Koszty te różnią się w zależności od wielkości przedsiębiorstwa, zakresu zabezpieczeń oraz poziomu ryzyka, z którym się mierzą. Wnioskiem z analizy jest fakt, że cyberbezpieczeństwo stanowi istotny koszt dla przedsiębiorstw, jednak jego brak może prowadzić do jeszcze większych strat finansowych. Dlatego organizacje powinny inwestować w odpowiednie zabezpieczenia adekwatne do swojej skali działalności i poziomu zagrożeń.

Podsumowanie

Cyberbezpieczeństwo stanowi istotny element funkcjonowania współczesnych organizacji. Ochrona danych i infrastruktury IT wiąże się z różnorodnymi kosztami, które można podzielić na trzy główne kategorie: koszty bezpośrednie, pośrednie i ukryte. Koszty bezpośrednie obejmują wydatki na technologie ochronne, takie jak zapory sieciowe, oprogramowanie antywirusowe, systemy wykrywania intruzów, testy penetracyjne oraz usługi prawne związane z obsługą incydentów. Koszty pośrednie to wydatki na szkolenia, doradztwo, ubezpieczenia cybernetyczne oraz zgodność z regulacjami prawnymi.[29] Koszty ukryte obejmują m.in. utratę reputacji, zakłócenia operacyjne, utratę klientów i dewaluację wartości firmy.

Brak właściwego zabezpieczenia może skutkować poważnymi stratami finansowymi wynikającymi z konieczności odbudowy infrastruktury, przestojów operacyjnych czy płatności okupu w przypadku ataków ransomware. Naruszenie danych może prowadzić do wysokich kar prawnych, kryzysu wizerunkowego oraz utraty klientów i inwestorów, co w konsekwencji wpływa na pozycję rynkową przedsiębiorstwa.[30] Koszty cyberbezpieczeństwa rosną wraz z wielkością

[29] Inlogica, *Koszty bezpośrednie i pośrednie – definicja, przykłady, różnice*, https://inlogica.com/artykuly/koszty-bezposrednie-i-posrednie-definicja-przyklady-roznice/ (dostęp: 05.06.2025r.).

[30] Magazynit.pl, *Ile naprawdę kosztuje ransomware? Straty, o których firmy nie chcą mówić*, https://www.magazynit.pl/bezpieczenstwo-it/32055-ile-naprawde-kosztuje-ransomware-straty-o-ktorych-firmy-nie-chca-mowic.html (dostęp: 05.06.2025r.).

organizacji. Małe firmy ponoszą minimalne wydatki, co czyni je bardziej podatnymi na ataki. Średnie przedsiębiorstwa inwestują w bardziej zaawansowane rozwiązania, łącząc wewnętrzne zespoły IT z outsourcingiem. Duże firmy stosują kompleksowe strategie ochrony, w tym wielowarstwowe zabezpieczenia, sztuczną inteligencję i audyty bezpieczeństwa.

Przykładowe wydatki obejmują zakup oprogramowania antywirusowego, firewalli, zarządzanie tożsamością i dostępem (IAM, MFA), ochronę przed *phishingiem* i *ransomware*, monitoring bezpieczeństwa 24/7, systemy wykrywania zagrożeń (IDS/IPS, SIEM), analizę zagrożeń opartą na AI/ML oraz ubezpieczenia cybernetyczne. Koszty te różnią się w zależności od wielkości przedsiębiorstwa, zakresu zabezpieczeń oraz poziomu ryzyka, z którym się mierzą.

Bibliografia

Koszewski R., Oręziak B., Wielec M., *Wdrożenie metod i instrumentów zapobiegania przestępczości w organizacjach*, Wydawnictwo Instytutu Wymiaru Sprawiedliwości, Warszawa 2021.

Szpor G., Gryszczyńska A., Świtała K., Prusak-Górniak K., Czaplicki K., Drobek P., Wilbrandt-Gotowicz M., Silicki K., Szafrański B., *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Wolters Kluwer Polska, Warszawa 2019.

Czasopisma naukowe

Antczak J., *Zarządzanie bezpieczeństwem informacji w jednostce gospodarczej*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2023.

Barczak P., *Mała firma niszowa - próba zdefiniowania*, Szkoła Główna Handlowa w Warszawie, Warszawa 2018.

Chaikovska M., *Trendy marketingowe i wyzwania technologiczne transformacji cyfrowych*, Wydawnictwo Narodowego Uniwersytetu Odeskiego, Odessa 2020.

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

Ferens A., Cyberbezpieczeństwo i cyberryzyko w raportach zintegrowanych i sprawozdaniach zarządu operatorów usług kluczowych, Wydawnictwo Uniwersytetu Ekonomicznego, Katowice 2021.

Fuksiewicz M., *Rodzaje i natura cyberataków oraz zarys działań w obszarze cyberbezpieczeństwa infrastruktury informatycznej*, Zeszyty Naukowe Wyższej Szkoły Bankowej, Poznań 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, Kraków 2024.

Klapkiv L., *Zakres ryzyka i szkód w cyberubezpieczeniu dla małych i średnich przedsiębiorstw*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2022.

Komitet Kontaktowy, *Cyberbezpieczeństwo w UE i państwach członkowskich UE*, Europejski Trybunał Obrachunkowy, Luksemburg 2020.
Kurkiewicz K., *Wielowymiarowy aspekt gospodarki elektronicznej z uwzględnieniem kwestii bezpieczeństwa*, Wydawnictwo Akademii Bialskiej, Biała Podlaska 2024.
Makoś E., *Zarządzanie bezpieczeństwem informacji i zachowanie bezpieczeństwa w systemie informatycznym*, Studenckie Zeszyty Naukowe, Wrocław 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*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2022.
Pelc P., *Wybrane regulacje dotyczące cyberbezpieczeństwa instytucji finansowych*, Cybersecurity and Law, Warszawa 2021.
Południak-Gierz K., *Wpływ dyrektyw 2019/770 oraz 2019/771 na poziom ochrony konsumenta w ramach reżimu rękojmi w prawie polskim*, Instytut Wymiaru Sprawiedliwości, 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*, Wydawnictwo Akademii Bialskiej, Biała Podlaska 2023.
Strupczewski G., *Ryzyko cybernetyczne jako wyzwanie dla branży ubezpieczeń w Polsce i na świecie*, Komitet Nauk o Finansach PAN, Warszawa 2017.
Wygodny A., *Metody prowadzenia audytu cyberbezpieczeństwa - ustawa o KSC*, Najwyższa Izba Kontroli, Warszawa 2021.

Źródła internetowe

https://inlogica.com/artykuly/koszty-bezposrednie-i-posrednie-definicja-przyklady-roznice/.
https://www.magazynit.pl/bezpieczenstwo-it/32055-ile-naprawde-kosztuje-ransomware-straty-o-ktorych-firmy-nie-chca-mowic.html.

Differentiation of cyber security costs in small, medium and large enterprises - a comparative approach

Abstract: The article discusses the issue of how cyber security costs vary depending on the size of the company. A breakdown of costs into direct (e.g., purchase of security software, incident handling costs), indirect (e.g., training, insurance, consulting) and hidden (e.g., loss of reputation,

business interruption, customer churn) was presented. Based on the analysis, it was shown that small companies invest the least in cyber security, making them more vulnerable to attacks. Medium-sized companies use a hybrid model (in-house teams and outsourcing), while large forms deploy advanced solutions based on, among other things, artificial intelligence and 24/7 monitoring systems. The conclusion is that while cyber-security generates significant costs, its absence can lead to much more serious losses, so treating it as an investment, not just an expense, is crucial to a company's stability.

Keywords: cyber security, costs, cyber security costs, direct costs, indirect costs, hidden costs, small businesses, medium-sized businesses, large businesses