Politechnika Częstochowska

Wydział Zarządzania

Praca doktorska

ZARZĄDZANIE BEZPIECZEŃSTWEM PRZEDSIĘBIORSTWA W SEKTORZE TECHNOLOGII INFORMACYJNO-KOMUNIKACYJNYCH A SZPIEGOSTWO KORPORACYJNE

MANAGING ENTERPRISE SECURITY IN THE INFORMATION AND COMMUNICATION TECHNOLOGY SECTOR AND CORPORATE ESPIONAGE

Imię i nazwisko: mgr Kajetan Kozłowski
Promotor: dr hab. inż. Anna Brzozowska, prof. PCz

Częstochowa 2024

SPIS TREŚCI

WSTĘP

Globalizacja oraz dynamiczny rozwój technologii mają niewątpliwy wpływ na to, że współczesne przedsiębiorstwa stają w obliczu różnorodnych zagrożeń, które mogą znacząco wpłynąć na ich funkcjonowanie i konkurencyjność. Zjawiskiem, które nie jest powszechnie dostrzegane, a stanowi źródło poważnych zagrożeń dla przedsiębiorstwa, jest szpiegostwo korporacyjne, które ogólnie rzecz ujmując, polega na nielegalnym pozyskiwaniu poufnych informacji w celu uzyskania przewagi konkurencyjnej. Zjawisko to, mimo że znane od dawna, pod postacią szpiegostwa gospodarczego lub szpiegostwa przemysłowego, zyskało na znaczeniu w erze cyfrowej, gdzie informacje stanowią kluczowy zasób każdej organizacji. Szpiegostwo korporacyjne bywa często mylone z przytoczonym wcześniej szpiegostwem gospodarczym i przemysłowym, wobec czego w kwestii zdefiniowania, należy w głównej mierze podkreślić, iż obejmuje celowe zdobywanie poufnych informacji dotyczących strategii, technologii, procesów produkcyjnych czy finansów przedsiębiorstwa w celu uzyskania nieuczciwej przewagi nad konkurencją. Informacje te mogą być następnie wykorzystywane przez konkurentów do poprawy własnych wyników, często kosztem podmiotu będącego celem szpiegostwa. W wyniku takich działań, przedsiębiorstwa mogą ponieść znaczne straty finansowe, utracić przewagę konkurencyjną, a także doświadczyć poważnych problemów reputacyjnych.

Problematyka współczesnego zarządzania bezpieczeństwem przedsiębiorstwa sprawia, iż szpiegostwo korporacyjne stanowi wyzwanie nie tylko dla działów takich jak IT czy bezpieczeństwa, ale również dla działów innowacyjnych a w konsekwencji dla organów zarządzających[1]. Efektywne zarządzanie bezpieczeństwem wymaga inwestycji zarówno w zaawansowane technologie ochrony, jak i w rozwój świadomości oraz kompetencji pracowników. Edukacja i szkolenia w zakresie bezpieczeństwa informacyjnego stają się kluczowym elementem strategii ochrony danych, pozwalając pracownikom na rozpoznawanie i właściwe reagowanie na potencjalne zagrożenia.

Problem szpiegostwa korporacyjnego jest szczególnie istotny w sektorach o wysokiej dynamice innowacji, takich jak sektor technologii informacyjno-komunikacyjnych (ang. *Information and Communication Technologies*, ICT). Przedsiębiorstwa działające w tym obszarze często posiadając unikalne know-how oraz przygotowywane lub wdrażane innowacyjne technologie, stają się celem działań szpiegowskich ze strony konkurentów lub

[1] G. Gnych, *Znaczenie zarządzania bezpieczeństwem informacji*, EIIT, https://eitt.pl/baza-wiedzy/znaczenie-zarzadzania-bezpieczenstwem-informacji/ [dostęp 15.04.2024 r.].

grup przestępczych[2]. Konkludując, szpiegostwo korporacyjne jest zjawiskiem, które wymaga kompleksowego podejścia do zarządzania bezpieczeństwem. Integracja zaawansowanych technologii ochrony, edukacja i szkolenia pracowników, a także przestrzeganie międzynarodowych standardów i norm prawnych, stanowią fundamenty skutecznej ochrony przed tym zagrożeniem. Współczesne przedsiębiorstwa muszą być świadome istnienia zagrożeń wynikających ze szpiegostwa korporacyjnego i podejmować proaktywne działania, aby chronić swoje wrażliwe informacje i zapewnić stabilne funkcjonowanie w konkurencyjnym środowisku rynkowym.

Współczesne przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych w Polsce muszą stawić czoła rosnącym zagrożeniom związanym ze szpiegostwem korporacyjnym[3]. Istotnym elementem obrony przed tymi zagrożeniami są pracownicy, którzy niejednokrotnie posiadają nieadekwatne lub niepełne spojrzenie na kwestię ryzyka i niepełną wiedzę na temat metod przeciwdziałania, co osłabia skuteczność systemów bezpieczeństwa wewnętrznego.

Skuteczne zarządzanie stanowi fundament sprawnego funkcjonowania współczesnych organizacji, obejmując planowanie, organizowanie oraz kontrolę zasobów w celu osiągania strategicznych celów. W obliczu dynamicznego rozwoju technologii oraz złożonych zagrożeń współczesnego rynku[4], zarządzanie bezpieczeństwem staje się jednym z kluczowych obszarów działań zarządczych. Zarządzanie bezpieczeństwem odpowiada za identyfikację, ocenę oraz ograniczanie ryzyka, które mogłoby zaburzyć stabilność operacyjną oraz ochronę wartościowych zasobów organizacji[5]. Praca dostarcza sektorowi technologii informacyjno-komunikacyjnych podstaw do opracowania skutecznych strategii zarządzania bezpieczeństwem, które zwiększają odporność organizacji na szpiegostwo korporacyjne.

Głównym celem niniejszej pracy jest opracowanie modelu zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych, który uwzględnia zróżnicowane postrzeganie zagrożeń wynikających ze szpiegostwa korporacyjnego przez pracowników, w celu zwiększenia ochrony danych i tajemnicy

---

[2] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2024*, wrzesień 2024, https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf [dostęp 01.10.2024 r.], s. 15 i 17.

[3] ESET, DAGMA, *Cyberportret polskiego biznesu*, 2024, https://www.gov.pl/web/baza-wiedzy/cyberportret-polskiego-biznesu---raport-przygotowany-przez-eset-i-dagma-bezpieczenstwo-it? [dostęp 08.10.2024 r.], s. 12 i 22-23.

[4] J. Wojnar, *Zróżnicowanie wykorzystania technologii informacyjno-komunikacyjnych w krajach Unii Europejskiej*, Wiadomości Statystyczne. The Polish Statistician, 2020, vol. 65(8), DOI: 10.5604/01.3001.0014.3526, s. 40.

[5] P. Wiśniewski, *Systemy zarządzania bezpieczeństwem informacji w przedsiębiorstwie*, Acta Universitatis Nicolai Copernici. Zarządzanie, 45(2), https://doi.org/10.12775/AUNC_ZARZ.2018.026, s. 128-129.

przedsiębiorstwa. Osiągnięcie założonego celu, wymusiło określenie następujących celów szczegółowych:

C1: Identyfikacja roli i znaczenia bezpieczeństwa w zarządzaniu przedsiębiorstwem,

C2: Zidentyfikowanie przesłanek oraz wyzwań związanych z wdrażaniem zarządzania bezpieczeństwem informacji w organizacji,

C3: Ustalenie, jakie wyzwania dla zarządzania bezpieczeństwem przedsiębiorstw sektora technologii informacyjno-komunikacyjnych stwarza szpiegostwo korporacyjne,

C4: Diagnoza zależności między poziomem świadomości pracowników a skutecznością zarządzania bezpieczeństwem w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych.

W odniesieniu do założeń i celu pracy określono problem badawczy oraz sformułowano hipotezę główną. Główny problem badawczy sformułowano w formie pytania: **jakie wyzwania dla zarządzania bezpieczeństwem informacji w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych wynikają ze zróżnicowanego postrzegania przez pracowników zagrożeń ze strony szpiegostwa korporacyjnego?**

Tak zdefiniowany problem badawczy wymagał sformułowania hipotezy głównej, zgodnie z którą **zarządzanie bezpieczeństwem informacji przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych powinno uwzględniać rozbieżności w postrzeganiu przez pracowników zagrożeń wynikających ze szpiegostwa korporacyjnego**.

Aby osiągnąć cel rozprawy, dodatkowo zdefiniowano szczegółowe hipotezy i problemy badawcze oraz określono metody niezbędne do ich weryfikacji. Wśród szczegółowych problemów badawczych należy wymienić kilka zagadnień sformułowanych w formie pytań:

P1: Jaką rolę i znaczenie odgrywa bezpieczeństwo w zarządzaniu przedsiębiorstwem sektora technologii informacyjno-komunikacyjnych?

P2: Jakie przesłanki i wyzwania wpływają na implementację zarządzania bezpieczeństwem informacyjnym w organizacji?

P3: W jaki sposób zagrożenia wynikające ze szpiegostwa korporacyjnego wpływają na zarządzanie bezpieczeństwem przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych?

P4: W jaki sposób można ocenić poziom świadomości pracowników na temat zagrożeń wynikających ze szpiegostwa korporacyjnego oraz skuteczność zarządzania bezpieczeństwem?

P5: Jaka jest zależność pomiędzy poziomem świadomości pracowników a skutecznością zarządzania bezpieczeństwem w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych?

Odpowiednio do szczegółowych problemów badawczych, sformułowano następujące hipotezy szczegółowe:

H1: Racjonalne zarządzanie bezpieczeństwem, w tym wdrażanie odpowiednich procesów decyzyjnych oraz strategii identyfikacji i minimalizacji ryzyka, warunkuje ciągłość działania organizacji oraz zabezpieczenie jej kluczowych zasobów.

H2: Stosowanie odpowiednich standardów i norm w zarządzaniu bezpieczeństwem informacji, pozwala na skuteczne rozpoznawanie zagrożeń, kształtując poziom ochrony danych oraz tajemnicy przedsiębiorstwa.

H3: Szpiegostwo korporacyjne stawia przed zarządzaniem bezpieczeństwem przedsiębiorstwa konieczność przeciwdziałania środkom i metodom dostępu do danych oraz pozyskiwania informacji w celu zdobycia przewagi konkurencyjnej.

H4: Skuteczne zarządzanie bezpieczeństwem przedsiębiorstw sektora technologii informacyjno-komunikacyjnych wymaga uwzględnienia sposobu, w jaki pracownicy postrzegają szpiegostwo korporacyjne.

Główny cel pracy oraz wyznaczone hipotezy pozwoliły na dobranie odpowiedniej procedury badawczej, która umożliwiła realizację zamierzonego celu, rozwiązanie postawionych problemów badawczych oraz weryfikację przyjętych hipotez. Proces badawczy został podzielony na pięć etapów:

a) etap I, podczas realizacji którego przeprowadzono studia literaturowe z zakresu poruszanej problematyki. W ramach tej części dokonano również analizy krytycznej zgromadzonego materiału oraz zidentyfikowano kluczowe obszary, które poddano dalszej ewaluacji w kolejnym etapie,
b) etap II, poświęcony został przygotowaniu i przeprowadzeniu wywiadu eksperckiego ze specjalistami z zakresu bezpieczeństwa przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych. Etap ten obejmował uzyskanie odpowiedzi na trzynaście pytań, które stanowią załącznik nr 1 do niniejszej dysertacji,
c) etap III, podczas realizacji którego przygotowano i przeprowadzono własne badanie z wykorzystaniem kwestionariusza ankiety wśród szczegółowo określonych i wytypowanych przedsiębiorstw sektora technologii informacyjno-komunikacyjnych prowadzących swoją działalność na terytorium RP,

d) etap IV, poświęcony został przygotowaniu podstaw empirycznych i stworzenia modelu zarządzania bezpieczeństwem przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych,
e) etap V, podczas realizacji którego przeprowadzono symulację komputerową mającą na celu sprawdzenie stworzonego modelu zarządzania oraz przygotowanie proponowanych narzędzi do ewaluacji i monitorowania wdrożenia oraz optymalizacji modelu na podstawie wyników wdrożenia.

Celem każdego z wyszczególnionych powyżej etapów było uzyskanie wiedzy pozwalającej na weryfikację postawionych hipotez oraz wypracowanie i sformułowanie wniosków, które pozwoliłyby na osiągnięcie założonych celów pracy.

Przeprowadzone badanie własne przy wykorzystaniu metody wywiadu eksperckiego objęło specjalistów z zakresu bezpieczeństwa przedsiębiorstwa bezpośrednio zatrudnionych w wytypowanych, na podstawie wskazanych powyżej kryteriów, przedsiębiorstwach z sektora technologii informacyjno-komunikacyjnych. Wykorzystana metoda badawcza miała na celu analizę stanu faktycznego oraz ocenę potencjalnych wariantów usprawnień[6]. Kontynuacją badań empirycznych było przeprowadzenie badania kwestionariuszowego. Ankietę zatytułowaną „*Problematyka Szpiegostwa Korporacyjnego w Przedsiębiorstwie Sektora Technologii Informacyjno-Komunikacyjnych*", zaadresowano do personelu na różnych poziomach hierarchicznych, od kierownictwa do pracowników biurowych. Główne aspekty, które poruszyła ankieta to przede wszystkim postrzeganie zjawiska szpiegostwa korporacyjnego, procedury reagowania na incydenty, szkolenia oraz zaangażowanie instytucji państwowych w uregulowanie i profilaktykę tej kwestii. Zastosowana metoda badawcza miała na celu zdiagnozowanie percepcji zjawiska szpiegostwa korporacyjnego przez pracowników oraz jej potencjalny wpływ na funkcjonowania organizacji z sektora technologii informacyjno-komunikacyjnych[7]. Kontynuacja badania empirycznego, oparta na metodach statystycznych i symulacji komputerowej, zaowocowały opracowaniem modelu zarządzania bezpieczeństwem przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych (ICT). Model ten uwzględniał kluczowe obszary wskazane zarówno przez ekspertów, jak i pracowników wybranych przedsiębiorstw sektora ICT. W dalszym etapie, przy wykorzystaniu symulacji komputerowej, przygotowano dziewięć wariantów wdrożenia modelu, wraz z propozycjami rozwiązań dotyczących monitorowania i ewaluacji skuteczności jego zastosowania. Dodatkowo, opracowano mechanizmy optymalizacji modelu w oparciu o wyniki uzyskane

[6] M. Lisiński, M. Szarucki, *Metody badawcze w naukach o zarządzaniu i jakości*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2020, s. 76.
[7] Ibidem, s. 77.

w procesie wdrażania, co pozwoliło na kompleksową weryfikację i doskonalenie zaproponowanych rozwiązań.

Zastosowana metodyka badań pozwoliła na zgromadzenie i analizę zebranych informacji, co w konsekwencji posłużyło jako podstawa do weryfikacji postawionych hipotez. Osiągnięcie zakładanych celów pracy jak również weryfikacja przygotowanych założeń hipotetycznych było możliwe dzięki przyjętej strukturze pracy, składającej się z sześciu rozdziałów, poruszających kwestię istoty zarządzania bezpieczeństwem przedsiębiorstwa, przesłanek implementacji zarządzania bezpieczeństwem informacyjnym organizacji, szpiegostwu korporacyjnemu i jego specyfice w aspekcie zarządzania bezpieczeństwem przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych, metodyce badań własnych, poziomowi świadomości pracowników jako determinancie efektywności zarządzania bezpieczeństwem w sektorze technologii informacyjno-komunikacyjnych oraz implementacji modelu zarządzania bezpieczeństwem.

Rozdział pierwszy dysertacji poświęcony został zagadnieniu zarządzania systemem bezpieczeństwa przedsiębiorstwa w sensie ogólnym. Punktem wyjścia do dalszego omawiania problematyki było zdefiniowania pojęcia bezpieczeństwa oraz elementów składających się na zakres bezpieczeństwa przedsiębiorstwa. Kolejnym elementem było omówienie istoty funkcjonowania systemu bezpieczeństwa w przedsiębiorstwie oraz przedstawienie różnych koncepcji i podejść do tego zagadnienia. Następnym krokiem było przedstawienie potencjalnych zagrożeń, które mogą negatywnie wpłynąć zarówno na samo funkcjonowanie przedsiębiorstwa, jak również na poszczególne jego podsystemy funkcjonalne. W dalszej części, autor przedstawił wybrane metody analizy i zarządzania ryzykiem według podziału na metody ilościowe oraz metody jakościowe. Ostatnim elementem przedstawionym przez autora było omówienie koncepcji zarządzania bezpieczeństwem przedsiębiorstwa. Charakterystyce poddane zostało środowisko bezpieczeństwa organizacji w kontekście jego składowych elementów funkcjonalnych. Następnie omówione zostały cztery podejścia do zarządzania bezpieczeństwem organizacji – zasobowe, zadaniowe, procesowe oraz systemowe (holistyczne) oraz przedstawiona została ewolucja rodzajów, percepcji oraz zapewniania bezpieczeństwa.

Rozdział drugi poświęcony został przedstawieniu problematyki związanej z kluczowymi aspektami zarządzania bezpieczeństwem informacyjnym – kluczowym z punktu widzenia przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych. Rozważania zawarte w niniejszym rozdziale poprzedzone zostały scharakteryzowaniem pojęć bezpieczeństwa informacyjnego oraz bezpieczeństwa informacji. Na podstawie przytoczonych definicji, autor przedstawił własne pojmowanie wskazanych pojęć oraz wskazał na istotną rolę

pierwszego z omawianych pojęć. Kolejny element stanowiło omówienie problematyki ochrony informacji i tajemnicy przedsiębiorstwa. W tej części autor skupił się na przedstawieniu i omówieniu międzynarodowych standardów ochrony informacji, przepisów regulujących ochronę informacji na poziomie państwowym, głównie w oparciu o funkcjonujące akty prawne w tym zakresie oraz scharakteryzowaniu i analizie pojęcia i elementów składowych polityki bezpieczeństwa. Następnie, autor przedstawił charakterystykę zagrożeń związanych z bezpieczeństwem informacyjnym, która poprzedzona została osadzeniem samego pojęcia w szerszym kontekście funkcjonowania obejmującym bezpieczeństwo: prawne, teleinformatyczne, osobowo-organizacyjne oraz bezpieczeństwo fizyczne organizacji. Autor wskazał również konkretne zagrożenia oraz miejsca w procesie informacyjnym narażone na potencjalny atak. Ostatnim elementem rozważań przeprowadzonych w niniejszym rozdziale było omówienie wybranych modeli zarządzania bezpieczeństwem informacyjnym w przedsiębiorstwie. Scharakteryzowane i omówione zostały cztery wybrane modele, których skuteczna implementacja możliwa jest zarówno w sektorze publicznym jak i prywatnym – model ISO/IEC 27001, model TISM, metoda TRA oraz metoda COBIT.

Trzeci rozdział porusza problematykę szpiegostwa korporacyjnego jako potencjalnego zagrożenia dla systemu bezpieczeństwa przedsiębiorstwa, szczególnie w kontekście bezpieczeństwa informacyjnego. Zasadniczym elementem tego rozdziału było omówienie różnic i podobieństw między pojęciami szpiegostwa przemysłowego i szpiegostwa gospodarczego. Wskazanie podobieństw i różnic było konieczne w celu prawidłowego zdefiniowana i omówienia pojęcia szpiegostwa korporacyjnego, które jest dużo obszerniejszym terminem i często łączy w sobie elementy szpiegostwa przemysłowego i gospodarczego. Kolejnym elementem rozważań dokonanych w tym rozdziale było szczegółowe omówienie wybranych sposobów pozyskiwania informacji o przedsiębiorstwie, gdzie autor skupił się na analizie operacyjnej, wywiadzie jawnoźródłowym, obserwacji, socjotechnice, szantażu i pozyskaniu pracownika oraz wybranych metodach pozyskiwania informacji o przedsiębiorstwie, gdzie autor omówił phishing, spoofing, spyware oraz sztuczną inteligencję.

Czwarty rozdział dysertacji koncentruje się na metodyce badań empirycznych, których celem była analiza zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych (ICT) w kontekście zagrożeń związanych ze szpiegostwem korporacyjnym. Przedstawiono zakres przedmiotowy, podmiotowy, przestrzenny i czasowy badań, obejmujący wybrane przedsiębiorstwa działające w polskim sektorze ICT, ze szczególnym uwzględnieniem ich specyfiki rynkowej i technologicznej. Proces badawczy został podzielony na trzy główne etapy: przegląd literatury naukowej, przeprowadzenie

wywiadów eksperckich oraz badanie ankietowe, które umożliwiły kompleksową analizę percepcji zagrożeń przez pracowników oraz praktyk zarządzania bezpieczeństwem. Wyniki badań zostały uzupełnione analizami statystycznymi i symulacjami komputerowymi, co pozwoliło na opracowanie modelu zarządzania bezpieczeństwem, uwzględniającego kluczowe wyzwania sektora ICT. Całość rozdziału podkreśla znaczenie zarządzania w interdyscyplinarnym podejściu do badania bezpieczeństwa w dynamicznie rozwijającym się sektorze technologicznym.

Piąty rozdział, o charakterze empirycznym, poświęcony został przedstawieniu wyników badań przeprowadzonych na próbie 12 ekspertów w ramach wywiadu eksperckiego oraz 466 osób w badaniu kwestionariuszowym. Wyniki potwierdzają rozważania teoretyczne i wskazują kluczowe działania sprzyjające poprawie bezpieczeństwa przedsiębiorstw, szczególnie w sektorze technologii informacyjno-komunikacyjnych. Badania wykazały, że regularne szkolenia, kampanie informacyjne, symulacje ataków, inwestycje w infrastrukturę bezpieczeństwa oraz wdrożenie zaawansowanych systemów zarządzania tożsamością i dostępem istotnie zwiększają zdolność przedsiębiorstw do przeciwdziałania zagrożeniom. Podkreślono także konieczność aktualizacji polityk bezpieczeństwa, zgodnie z regulacjami i zmianami technologicznymi, oraz prowadzenia regularnych audytów i testów penetracyjnych. Eksperci zwrócili uwagę na znaczenie współpracy z partnerami biznesowymi, dostawcami technologii i organami rządowymi, co ułatwia wymianę informacji o zagrożeniach oraz koordynację działań w przeciwdziałaniu szpiegostwu korporacyjnemu. Wyniki badań stały się podstawą opracowania modelu zarządzania bezpieczeństwem przedsiębiorstw sektora technologii informacyjno-komunikacyjnych, integrującego elementy szkoleniowe, techniczne, organizacyjne i strategiczne.

Szósty rozdział, o charakterze empirycznym, poświęcony został implementacji modelu zarządzania bezpieczeństwem w sektorze technologii informacyjno-komunikacyjnych. Struktura rozdziału koncentruje się na przygotowaniu organizacyjnym do wdrożenia modelu zarządzania bezpieczeństwem, symulacji procedury wdrożenia modelu w strukturze organizacyjnej, monitorowaniu i ewaluacji skuteczności wdrożenia oraz optymalizacji modelu w oparciu o wyniki wdrożenia. Rozdział akcentuje znaczenie systemowego podejścia, integrującego świadomość zagrożeń, kompetencje personelu oraz zaawansowane zabezpieczenia fizyczne i cyfrowe. Kluczowe wnioski wskazują na istotność monitorowania wskaźników KPI, takich jak poziom świadomości zagrożeń (TAL), retencja wiedzy po szkoleniach oraz czas reakcji na incydenty (IRT), które umożliwiają ocenę efektywności wdrożonych działań i identyfikację luk. Obserwacje zwracają uwagę na konieczność dynamicznego dostosowywania strategii bezpieczeństwa do zmieniającego się środowiska ICT,

w tym integracji narzędzi analitycznych oraz automatyzacji procesów weryfikacyjnych. Wyniki symulacji potwierdzają, że wdrożenie modelu w formie kompleksowej strategii, uwzględniającej aspekty edukacyjne, techniczne i proceduralne, znacząco zwiększa odporność organizacji na zagrożenia, co czyni ten model optymalnym rozwiązaniem dla sektorów o wysokim ryzyku operacyjnym.

Przeprowadzona metodyka badań pozwoliła na wyodrębnienie kierunków dalszego doskonalenia w obszarze zarządzania bezpieczeństwem przedsiębiorstwa w kontekście szpiegostwa korporacyjnego. Kluczowe kierunki to zwiększanie świadomości pracowników na temat zagrożeń związanych z tym zjawiskiem, intensyfikacja działań mających na celu ochronę, rozwój polityk i procedur, przygotowanie planów reagowania oraz wdrożenie szkoleń mających na celu edukację pracowników.

Analiza wyników przeprowadzonych badań empirycznych prowadzi do wniosków, zgodnie z którymi stwierdzić należy, iż kompleksowe podejście do zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych powinno obejmować aspekty technologiczne, proceduralne i ludzkie, które są niezbędne dla skutecznej ochrony przed szpiegostwem korporacyjnym. Inwestowanie w zaawansowane technologie, regularne szkolenia pracowników oraz dostosowywanie swoich polityk i procedur do zmieniających się zagrożeń, rozwiązań technologicznych oraz regulacji prawnych i budowanie kultury bezpieczeństwa w organizacji są kluczowe dla zapewnienia długoterminowej ochrony przed zagrożeniami cyfrowymi i szpiegostwem korporacyjnym przedsiębiorstw w sektorze technologii informacyjno-komunikacyjnych.

Rozdział 1.ISTOTA ZARZĄDZANIA BEZPIECZEŃSTWEM PRZEDSIĘBIORSTWA

1.1 Rola bezpieczeństwa w zarządzaniu przedsiębiorstwem

Omówienie problematyki poruszanej w ramach niniejszej dysertacji poprzedzić należy zdefiniowaniem pojęć, które wykorzystywane będą w ramach dalszych rozważań, tak aby nie powstały żadne wątpliwości w pojmowaniu przedstawianych treści. Dlatego też, rozpocząć należy od charakterystyki samego pojęcia bezpieczeństwa, które w zależności od spojrzenia definiowane jest na wiele sposobów. Najprostszym określeniem bezpieczeństwa jest *stan niezagrożenia*[8], który odczuwalny jest podczas normalnego funkcjonowania człowieka w życiu codziennym i społecznym. Termin *bezpieczeństwo* wywodzi się z języka łacińskiego od *securitas*. Gdzie pierwszy człon pochodzi od *sine* – bez, drugi człon *cura* – zmartwienie, strach, obawa. W ujęciu lapidarnym to brak zmartwień i poczucia strachu. A. Dmowska w słowniku współczesnego języka polskiego termin bezpieczeństwo definiuje jako *stan psychiczny lub prawny, w którym jednostka ma poczucie pewności, oparcie w drugiej osobie lub sprawnie działającym systemie prawnym: przeciwieństwo zagrożenia*[9]. Kolejną definicją bezpieczeństwa jest zaproponowana przez pracowników naukowych Akademii Sztuki Wojennej i rozumiana jako *naczelna potrzeba, wartość i cel każdego realnego bytu, mające zapewnić jego przetrwanie, funkcjonowanie i rozwój, a także realizację interesów*[10]. Tematyka bezpieczeństwa jest istotnym elementem funkcjonowania państwa, gdyż głównymi jego wyznacznikami są społeczeństwo i władza państwowa. Wobec powyższego, można wyróżnić cztery podstawowe stany bezpieczeństwa:

a) **stan braku bezpieczeństwa** – występuje w obliczu poważnego, rzeczywistego zagrożenia, a postrzeganie tegoż zagrożenia jest prawidłowe,
b) **stan obsesji** – występuje w obliczu nieznacznego zagrożenia, które postrzegane jest jako poważne,
c) **stan fałszywego bezpieczeństwa** – występuje w obliczu poważnego zagrożenia, które postrzegane jest jako nieznaczące,
d) **stan bezpieczeństwa** – występuje w obliczu niewielkiego zagrożenia, którego postrzeganie jest prawidłowe[11].

[8] *Uniwersalny słownik języka polskiego*, http://sjp.pwn.pl/sjp/bezpieczenstwo;2443939.html [dostęp: 19.07.2022].
[9] A. Dmowska, *Słownik współczesnego języka polskiego*, Warszawa 1996, s. 56.
[10] *Słownik terminów z zakresu bezpieczeństwa*, J. Pawłowski, B. Zdrodowski, M. Kuliczkowski red. nauk., Wydawnictwo Adam Marszałek, Toruń 2020, s. 20-21.
[11] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Wyd. ISP, Warszawa 1996, s. 17.

Istotę bezpieczeństwa w funkcjonowaniu człowieka uwzględnił Abraham H. Maslow w piramidzie potrzeb, w której niezbędność bezpieczeństwa zajmuje drugie miejsce w hierarchii wymogów ludzkich i bez jej osiągnięcia niemożliwe staje się osiągnięcie pozostałych, równie istotnych w procesie samorealizacji człowieka potrzeb[12].

Początkowo pojęcie bezpieczeństwa interpretowane było w ramach działań prowadzonych przez siły zbrojne i politycznych podejmowanych przez państwo. Taka ograniczona perspektywa skupiona była na przeciwdziałaniu niebezpieczeństwom, które zagrażały istnieniu i suwerenności narodu, co oznaczało ciągłe dostosowywanie się do nowych lub przewidywalnych zagrożeń. W tym kontekście, projektowanie systemów bezpieczeństwa opierało się na opracowywaniu scenariuszy potencjalnych zagrożeń[13].

Bezpieczeństwo może być postrzegane jako definiowanie i zarządzanie współczesnymi i przyszłymi wyzwaniami cywilizacyjnymi, w taki sposób, aby zamiast pozwolić im stać się zagrożeniem, przekształcać je w szanse. Współczesne pojmowanie bezpieczeństwa obejmuje szerszy zakres niż dotychczas uważano – dotyczy nie tylko przetrwania, ale również zapewnienia rozwoju[14]. Bezpieczeństwo postrzegane jest jako stan, proces, odczucie, percepcja, sytuacja, zdolność, potrzeba oraz cel działań. Jednakże, pomimo swojej rozpiętości, takie ujęcie krytykowane jest ze względu na swoje ograniczenia znaczeniowe – przywiązanie do konkretnego sektora lub jednowymiarowość[15]. Bezpieczeństwo dotyczy konkretnego zjawiska. Dlatego co do kwestii przedmiotu bezpieczeństwa, wśród badaczy panuje zgoda, natomiast w kwestii podmiotu następuje pewna rozbieżność. Szerokie ujęcie podmiotu bezpieczeństwa wiąże się z istotą, której to bezpieczeństwo dotyczy, co oznacza, że jego istnienie jest warunkiem koniecznym dla bezpieczeństwa. Koncepcja ta zakłada, że bezpieczeństwo stanowi integralną część tego podmiotu, zwaną bezpieczeństwem podmiotu (bezpieczeństwo państwa, narodu, rodziny itd.). Węższe ujęcie podmiotu bezpieczeństwa odnosi się do konkretnej, odpowiedzialnej i zapewniającej bezpieczeństwo jednostki o charakterze sprawczym (państwo, system prawny, służby, policja itd.).

Bezpieczeństwo stanowi kluczowy aspekt definiujący struktury organizacyjne i ich funkcjonowanie w szerokim kontekście rynkowym i rozumiane może być na wiele sposobów. Na kompleksowość i różnorodność znaczeniową tego terminu wskazują badacze tacy jak Piotr

[12] Por. A. H. Maslow, *Motivation and Personality*, Longman, Nowy Jork 1987.
[13] *Słownik terminów z zakresu bezpieczeństwa…*, op. cit.
[14] K. Kozłowski, *System Bezpieczeństwa Wewnętrznego RP. Wybrane aspekty zarządzania bezpieczeństwem w XXI w.*, Management and Quality – Zarządzanie I Jakość, Vol 4 No 3 (2022), s. 60-61.
[15] Ibidem.

Majer[16], Andrzej Czupryński[17], Marek Fałdowski[18], Edward Kołodziński[19] oraz Jarosław Gryz[20].

Różnorodność definicji pozwala na wyróżnienie statycznej oraz dynamicznej perspektywy bezpieczeństwa[21]. Pierwsza z nich, charakteryzuje bezpieczeństwo jako obecny stan organizacji w danym punkcie jej rozwoju, skupiając się na obecnie wykorzystywanych zasobach i potencjale. Druga zaś, podkreśla fakt zdolności organizacji do adaptacji i ewolucji w czasie poprzez różne etapy rozwoju[22]. Ważnym jest, aby zwrócić uwagę, iż obie te perspektywy są istotne dla menedżerów i właścicieli koncertujących się na tworzeniu systemu bezpieczeństwa organizacji. Jest to bowiem spowodowane faktem, że odzwierciedlają one krótko i długoterminowe podejście do organizacji w szerokim spektrum działania. Bezpieczeństwo organizacji obejmuje bowiem zarówno aspekt operacyjny, jak i strategiczny[23]. Przykładowe ujęcia bezpieczeństwa, które posłużą jako odniesienie do interpretacji bezpieczeństwa w nowoczesnych organizacjach, zaprezentowano w tabeli nr 1.

Tabela 1 Przykładowe definicje terminu bezpieczeństwo

Lp.	Autor	Definicja
Ujęcie statystyczne		
1.	OECD	sytuacja, w której nie występuje ryzyko niemożliwe do przyjęcia w organizacji.
2.	K. Ficoń	stan pewności i stabilności organizacji w otoczeniu, odznaczający się brakiem występowania ryzyka związanego z utratą określonych wartości, które są szczególnie cenione przez organizację oraz jej interesariuszy, kryterium systemowe, ponieważ koncentruje się zarówno na zbiorze elementów danego systemu działania (tj. organizacji), jak i uwzględnia zbiór relacji łączący te elementy.
3.	T. Szopa	pojęcie przeciwstawne pojęciom strat i ryzyka,

[16] P. Majer, *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*, „Przegląd bezpieczeństwa wewnętrznego" 2012, nr 7(4), s. 11-18.
[17] A. Czupryński, *Bezpieczeństwo w ujęciu teoretycznym*, W: *Bezpieczeństwo. Teoria-Badania-Praktyka*. (red.) A. Czupryński, B. Wiśniewski, J. Zboina, Wydawnictwo CNBOP-PIB, Józefów 2015, s. 9-24.
[18] M. Fałdowski, *Współczesny wymiar bezpieczeństwa*, „Zeszyty Naukowe SGSP" 2018, nr 66(2), s. 111-114.
[19]E. Kołodziński, *Wprowadzenie do zarządzania bezpieczeństwem*, 2021, http://www.uwm.edu.pl/mkzk/download/wprowadzenie.pdf [dostęp: 15 grudnia 2023].
[20] J. Gryz, *Zarys podstaw teorii bezpieczeństwa*, Akademia Obrony Narodowej, Warszawa 2010, s. 9-11
[21] J. Woźniak, *Percepcja i kształtowanie bezpieczeństwa organizacji w warunkach gospodarki cyfrowej*, W: *Bezpieczeństwo organizacji w warunkach gospodarki cyfrowej*. (red.) W. Gonciarski, J. Woźniak, Difin, Warszawa 2021, s. 42.
[22]A. Mrożek, *Zarządzanie bezpieczeństwem organizacji o strukturze heterarchicznej*, https://sg-cdn.uek.krakow.pl/file/root/stanowisko-ds.-obronnych/sdo-zarzadzanie-bezpieczenstwem-organizacji-o-strukturze-heterarchicznej-artykul.pdf [dostęp: 15.12.2023 r.].
[23]M. Płecka, *Bezpieczeństwo ekonomiczne małych i średnich przedsiębiorstw*, https://revue.vsdanubius.sk/sites/default/files/Plecka%20-%20BEZPIECZE%C5%83STWO%20EKONOMICZNE%20MA%C5%81YCH%20I%20%C5%9AREDNIC%20PRZEDSI%C4%98BIORSTW.pdf [dostęp: 15.12.2023 r.].

Lp.	Autor	Definicja
		bezpieczeństwo należy traktować jako wypadkową różnych czynników, tj. zjawisk i obiektów, które mogą wystąpić zarówno w danej jednostce organizacyjnej, jak i w otoczeniu.
4.	Słownik języka polskiego PWN	jest to stan niezagrożenia
5.	K. Raczkowski	postrzeganie i ocena bezpieczeństwa powinny odnosić się do warstwy samooceny jednostki i wyznawanego przez nią światopoglądu, bezpieczeństwo ma charakter subiektywny, ale jest jednocześnie wypadkową tzw. czynników zbiorowych, które stanowią swoiste odzwierciedlenie charakteru relacji jednostki z otoczeniem (lokalnym, krajowym lub międzynarodowym).
6.	L. F. Korzeniowski	zdolność do kreatywnej aktywności podmiotu – oznacza holistyczną i dynamiczną sytuację obiektywną, polegającą na braku zagrożenia, odczuwaną subiektywnie przez jednostki lub grupy społeczne.
7.	J. Stańczyk	stan, charakteryzujący się spokojem, stabilizacją i pewnością, że zagrożenie nie wystąpi, a jednocześnie, gdyby się pojawiło, to człowiek/organizacja będzie przed nim chroniony/a, wartość różnorodnie pojmowana.
8.	D. Frei	stan, który występuje jedynie wówczas, kiedy brak jest rzeczywistego zagrożenia (tj. czynnika obiektywnego) i poczucia zagrożenia (tj. czynnika subiektywnego).
9.	P. D. Williams	stan, który trudno jest jednoznacznie określić – dla każdego oznacza coś innego.
Ujęcie dynamiczne		
10.	J. Świniarski, P. Kawalerski	proces potęgowania lub stabilizacji negentropii, porządku i jego doskonalenia. (…) przechodzenie od entropii (chaosu) ku negentropii (porządkowi) i racjonalizacji istnienia).
11.	E. Kołodziński, T. Lachowicz	stan niestabilny, który może ulegać zmianom w czasie, bezpieczeństwo nie ma charakteru stałego i jego wartość nie jest przypisana organizacji raz na zawsze.
12.	S. Koziej	dziedzina aktywności danego podmiotu, której treścią jest zapewnianie możliwości przetrwania (egzystencji) i swobody realizacji własnych interesów w niebezpiecznym środowisku – m.in. poprzez wykorzystywanie szans, redukowanie ryzyka i przeciwdziałanie zagrożeniom.
13.	A. Maslow	ludzka potrzeba, której niezaspokojenie uniemożliwia poprawny rozwój człowieka i funkcjonowanie w społeczeństwie.
14.	R. Zięba	potrzeba składająca się ze zdywersyfikowanych elementów, będąca wypadkową różnych czynników związanych z działaniem poszczególnych grup interesariuszy organizacji w określonym przedziale czasu, ciągłość istnienia podmiotu w sposób trwały.

Lp.	Autor	Definicja
15.	P. Majer	stan gwarantujący pewność istnienia i przetrwania, a także swobodę rozwoju danego podmiotu.
16.	P. Zaskórski, J. Woźniak, K. Szwarc, Ł. Tomaszewski	funkcja wielu zmiennych – w zależności od zmian jednego czynnika, funkcja ta może przyjmować różne wartości.

Źródło: J. Woźniak, Percepcja i kształtowanie bezpieczeństwa w organizacji…, op. cit., s. 43-45.

Mając na uwadze przytoczone powyżej definicje, warto podkreślić, że rozumienie, badanie i zagwarantowanie bezpieczeństwa w organizacji powinno odbywać się na dwóch wzajemnie powiązanych poziomach:

a) bezpieczeństwa wewnętrznego – ta płaszczyzna, w swojej najprostszej formie, odzwierciedla podejście mikroekonomiczne, skupiając się na obecnym lub przyszłym (przewidywalnym) stanie organizacji oraz na stopniu osiągania celów, które są rezultatem działań wykonywanych przez pracowników na różnych poziomach w strukturze organizacji,
b) bezpieczeństwa zewnętrznego – w uproszczeniu, ta płaszczyzna koresponduje z połączonymi perspektywami mezoekonomiczną, makroekonomiczną i megaekonomiczną, ponieważ dotyczy mechanizmów, na podstawie których organizacja funkcjonuje w swoim otoczeniu. Obejmuje to m.in. wpływ wywierany przez podmioty zewnętrzne na potencjał organizacji (i odwrotnie) oraz współdziałanie organizacji w realizacji wspólnych celów, często w ramach sieciowych struktur[24].

W omawianym podrozdziale, za punkt wyjścia do przygotowania autorskiej definicji bezpieczeństwa organizacji przyjęto podejście, iż kształtowanie tej kategorii *odnosi się do minimalizacji zagrożeń w prowadzeniu działalności gospodarczej, gdzie wielkość przychodu netto ze sprzedaży dóbr i usług w rachunku zysków i strat umożliwi wypracowanie takiego zysku netto w danym roku obrotowym, który pozwoli na niezakłócone prowadzenie działalności gospodarczej w perspektywie krótko i średniookresowej*[25]. Tak przedstawiony fundament definicyjny nabiera szczególnego znaczenia, gdyż integruje dwa kluczowe filary bezpieczeństwa organizacji: środki finansowe oraz inne zasoby dostępne w organizacji, których efektywne wykorzystanie jest możliwie dzięki specyficznej stabilności finansowej[26]. Autor

[24] J. Woźniak, *Kryterium bezpieczeństwa organizacji*, W: *Projektowanie i doskonalenie organizacji*. (red.) J. Woźniak, Wojskowa Akademia Techniczna, Warszawa 2015, s. 89.
[25] K. Raczkowski, *Współczesny model tetrarchii zarządzania a bezpieczeństwo ekonomiczne obrotu gospodarczego,* W: *Bezpieczeństwo ekonomiczne obrotu gospodarczego. Ekonomia. Prawo. Zarządzanie*. (red.) K. Raczkowski, Wolters Kluwer, Warszawa 2014, s. 38.
[26] J. Woźniak, *Percepcja i kształtowanie bezpieczeństwa organizacji…*, op. cit., s. 45.

proponuje definiować bezpieczeństwo przedsiębiorstwa jako stan oraz proces zarządzania zagrożeniami, w którym organizacja zapewnia stabilność i ciągłość funkcjonowania, minimalizuje ryzyko oraz maksymalizuje zdolność do reagowania na zmieniające się warunki otoczenia.

Aktualnie bezpieczeństwo finansowe nie pozostaje jedyną sferą, którą zajmują się menedżerów i właścicieli organizacji. Zakres ten poszerzony został o dodatkowe aspekty, takie jak relacje z interesariuszami, struktura organizacyjna, kompetencje pracowników, aspekty instytucjonalno-regulacyjne, wykorzystanie technologii informacyjno-komunikacyjnych, innowacje, rozwój rynkowy oraz zarządzanie traktowane jako środek do świadomego zapewnienia bezpieczeństwa[27]. Bezpieczeństwo finansowe organizacji, charakteryzujące się wąskim zakresem tematycznym, można określić jako proces lub zbiór warunków związanych z pozyskiwaniem, gromadzeniem i wykorzystaniem środków finansowych[28]. W obecnych warunkach społecznych, ekonomicznych, kulturowych, technologicznych i innych (zarówno na poziomie globalnym, jak i w poszczególnych gospodarkach narodowych), ograniczanie pojęcia bezpieczeństwa organizacji wyłącznie do aspektu finansowego byłoby nadmiernym uproszczeniem. Dlatego należy bezpieczeństwo organizacji rozpatrywać w kontekście holistycznym[29], obejmującym obszary kluczowe dla niezakłóconego funkcjonowania[30]. Wspomniane obszary zostały przedstawione na rysunku nr 1.

[27] A. Gembalska-Kwiecień, Z. Żurakowski, *Zarządzanie bezpieczeństwem a problem partycypacji pracowników w przedsiębiorstwie*, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie", nr 159, 2015, DOI: 10.29119/1641-3466.2022.159, s. 94 i 97.
[28] A. N. Duraj, *Rezerwy a strategie finansowe publicznych spółek akcyjnych*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2008, s. 85-88.
[29] Rybicki J., *Holizm w controllingowym zarządzaniu organizacjami*, „Przegląd Organizacji", Nr 1(984), 2022, DOI: 10.33141/po.2022.01.02, s. 13.
[30] D. Janus, *Holizm w controllingowym zarządzaniu organizacjami*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu", 2022, t. 66, nr 2, DOI: 10.15611/pn.2022.2.05, s. 63 i 66.

Rysunek 1 Podstawowe wymiary kształtowania bezpieczeństwa organizacji - ujęcie przedmiotowe

Źródło: opracowanie własne na podstawie J. Woźniak, Percepcja i kształtowanie bezpieczeństwa…, op. cit., s. 46.

Jako potwierdzeniem dotychczasowych rozważań, autor wskazuje na stanowisko prezentowane przez Małgorzatę Płecką, która zauważa, że z perspektywy przedmiotowej w kontekście bezpieczeństwa organizacji można wyszczególnić aspekty takie jak bezpieczeństwo finansowe, technologiczne, kompetencyjne i inne[31]. Co więcej, bezpieczeństwo organizacji odnosi się do warunków sprzyjających jej harmonijnemu rozwojowi i stabilnej działalności[32], jak również do kreowania zrównoważonego dobrobytu pracowników oraz utrzymania wypłacalności organizacji[33]. Renata Włoch podkreśla również aspekt kadrowy bezpieczeństwa, wskazując, że jest to taki stan, w którym tworzone są niezbędne warunku dla przetrwania i rozwoju pracowników[34]. Zenon Stachowiak, Stanisław Kurek oraz Sylwester Kurek rozwijają wymiar menedżerski i relacyjny bezpieczeństwa. Uważają oni, że bezpieczeństwo obejmuje sferę decyzyjną w kontekście gospodarczym, mającą na celu zapewnienie swobody w kształtowaniu procesów zgodnie z celami organizacji i jej

[31] M. Płecka, *Bezpieczeństwo ekonomiczne małych…,* op. cit.
[32] K. M. Księżopolski, *Bezpieczeństwo ekonomiczne*, Dom Wydawniczy ELIPSA, Warszawa 2011, s. 32-33.
[33] K. Żukrowska, *Ekonomia jako sfera bezpieczeństwa państwa*, W: *Interdyscyplinarność nauk o bezpieczeństwie*. (red.) K. Raczkowski, K. Żukrowska, M. Żuber, Difin, Warszawa 2013.
[34] R. Włoch, *Bezpieczeństwo ekonomiczne państwa*, W: *Bezpieczeństwo państwa. Wybrane zagadnienia.* (red.) K. A. Wojtaszczyk, A. Materska-Sosnowska, Oficyna Wydawnicza Aspra-JR, Warszawa 2009.

interesariuszy[35]. Innymi słowy, bezpieczeństwo to taki stan organizacji, w którym dzięki efektywnemu wykorzystaniu wewnętrznych czynników rozwojowych oraz zewnętrznych czynników wpływu, gwarantowana jest wysoka efektywność działania oraz zdolność do efektywnego reagowania na zewnętrzne wyzwania, które mogą zakłócić rozwój organizacji[36].

Bezpieczeństwo fizyczne definiować można jako *rodzaj (kategorię) bezpieczeństwa, dotyczący osoby lub obiektu oraz ich otoczenia, danych i informacji o nich, realizowane poprzez ochronę przed szkodliwym oddziaływaniem, inwigilacją, sabotażem, destrukcją, a także nieuprawnionym władaniem*[37]. Bezpieczeństwo fizyczne najczęściej kojarzy się z ochroną indywidualną oraz stosowaniem różnorakich środków, takich jak: systemy alarmowe oraz systemy informujące o podsłuchu, włamaniu czy napadzie, monitoring przemysłowy, systemy kontroli dostępu, komunikacja, obsługa wartownicza i dyżurna, oświetlenie budynków, punkty obserwacyjne, zabezpieczenia inżynieryjne oraz mechaniczne zabezpieczenia budynków.

Informacje zgromadzone w bazach danych powinny być chronione, a zwłaszcza te o strategicznym znaczeniu dla działalności organizacji. Stosunkowo istotnym obszarem w procesie projektowania systemów informacyjnych wspierających zarządzanie przedsiębiorstwem jest rola bezpieczeństwa informacji, obejmująca określanie kompleksowego zestawu zasad, metod i narzędzi służących ochronie oraz monitorowaniu danych[38]. Definiowanie bezpieczeństwa informacji stanowi wyzwanie, głównie ze względu na dynamiczny postęp w dziedzinie technologii informacyjnych i ciągłe pojawianie się nowych metod naruszania zabezpieczeń. Dlatego, dokładna definicja tego pojęcia musi być ściśle związana z identyfikacją kluczowych atrybutów bezpieczeństwa, które obejmują:

a) poufność – informacja jest niedostępna dla nieautoryzowanych osób, podmiotów lub procesów;
b) autentyczność – tożsamość podmiotu lub zespołu jest potwierdzona stosownym certyfikatem dostępu,
c) dostępność – możliwość wykorzystania informacji w danym czasie przez osobę, która ma do tego prawo,
d) integralność danych – dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

[35] Z. Stachowiak, S. Kurek, S. Kurek, *Bezpieczeństwo ekonomiczne Rzeczypospolitej Polskiej*, Akademia Obrony Narodowej, Warszawa 2004, s. 18-19.
[36] E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego,* Difin, Warszawa 2011, s. 89-100.
[37] *Słownik terminów z zakresu bezpieczeństwa…*, op. cit., s. 23.
[38] K. Woźniak, M. Tatka, *Bezpieczeństwo informacji – hasło,* Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Bezpiecze%C5%84stwo_informacji [dostęp 15.12.2023 r.].

e) integralność systemowa – właściwość umożliwiająca systemowi realizację zamierzonej funkcji w nienaruszony przez nieautoryzowane manipulacje (celowe lub przypadkowe) sposób;
f) integralność – integralność danych oraz systemu,
g) rozliczalność – oznacza, że działania podmiotu np. użytkownika mogą być mu przypisane,
h) niezawodność – spójne, zamierzone zachowanie i skutki[39].

Krzysztof Liderman bezpieczeństwo informacji definiuje jako *uzasadnione (np. analizą ryzyka i przyjętymi metodami postępowania z ryzykiem) zaufanie, że nie zostaną poniesione straty wynikające z niepożądanej zmiany, na skutek realizacji zagrożenia, wymagających istotnych kryteriów jakości informacji*[40].

Bezpieczeństwo informacji stanowi jeden z kluczowych czynników zapewniający bezpieczeństwo organizacji w kontekście aktualnych wyzwań i zagrożeń bezpieczeństwa związanych ze wzrostem popularności i dostępu do nowych technologii. Problematyka powyższego zagadnienia zostanie w szerszy sposób omówiona w kolejnym rozdziale niniejszej dysertacji.

Pomimo, iż kryteria określające pojęcie bezpieczeństwa są zróżnicowane, trudne do zmierzenia i mogą być interpretowane w sposób różny przez każdą jednostkę, w tym również menedżerów, właścicieli czy pracowników liniowych organizacji, powinno być jednocześnie traktowane jako kluczowy element w kreowaniu tzw. zrównoważonego rozwoju organizacji, zarówno w krótkim, jak i długim okresie[41]. Przykładem tego może być zapewnienie ciągłości procesów biznesowych, utrzymywanie trwałych relacji ze wszystkimi interesariuszami oraz podnoszenie wartości, jaką organizacja dostarcza swoim pracownikom i środowisku zewnętrznemu[42].

Nie wszyscy menedżerowie czy przedsiębiorcy podchodzą do kwestii bezpieczeństwa swojej organizacji w sposób jednolity i świadomy. Mimo, iż niektórzy otwarcie podkreślają jego znaczenie, drudzy mogą nie dostrzegać pełnego spektrum zagrożeń lub nie przykładają należytej wagi do zabezpieczenia niezakłóconego funkcjonowania organizacji. Ważne jest jednak, aby bezpieczeństwo przedsiębiorstwa nie sprowadzało się do pustych słów czy

[39] J. Czekaj, *Podstawy zarządzania informacją*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2012, s. 128.
[40] K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydawnictwo PWN, Warszawa 2017, s. 13.
[41] J. Zawiła-Niedźwiedzki, *Zarządzanie ryzykiem operacyjnym w zapewnieniu ciągłości działania organizacji*, Wydawnictwo edu-Libri, Kraków-Warszawa 2013, s. 83.
[42] A. Chodyński, *Interesariusze w kształtowaniu bezpieczeństwa organizacji wobec kryzysu pozaekonomicznego*, „Bezpieczeństwo. Teoria i Praktyka" 2016, nr 10(4), s. 44-53.

sloganów, które są często używane przez kadry kierownicze i właścicieli. Jest dużo bardziej kompleksowa kwestia, która wymaga realnego zaangażowania i skutecznych działań.

Zapewnianie bezpieczeństwa w organizacji to nie tylko kwestia ochrony fizycznej i technologicznej, ale także aspekt psychologiczny, społeczny i ekonomiczny. Wiąże się to zarówno z ochroną danych i własności intelektualnej, jak i zapewnianiem stabilnego środowiska pracy pracownikom, a to z kolei przekłada się na ich dobrostan i produktywność. Nie można zapominać, że bezpieczeństwo jest też związane z reputacją organizacji – naruszenia bezpieczeństwa mogą mieć długotrwałe skutki związane z utratą zaufania klientów i partnerów biznesowych[43].

Zapewnianie bezpieczeństwa wymaga nie tylko wdrożenia odpowiednich technologii i procedur, ale także budowania kultury organizacyjnej, w której bezpieczeństwo jest wartością nadrzędną. To oznacza regularne szkolenia pracowników oraz podnoszenie ich kompetencji rozumianych jako wiedza, umiejętności i postawy, które są kluczowe dla realizacji strategii organizacyjnej[44]. Ponadto, istotnym jest utrzymywanie aktualnych i skutecznych planów awaryjnych, a także stałe monitorowanie i adaptowanie się do zmieniającego się środowiska zewnętrznego.

Dzisiejszy, szybko zmieniający się świat, w którym nowe technologie i metody działania stwarzają nowe zagrożenia w sposób szczególny wymusza na organizacjach zapewnienie i utrzymanie bezpieczeństwa. Przedsiębiorstwa muszą nieustannie monitorować najnowsze trendy w zakresie cyberbezpieczeństwa, ochrony danych osobowych oraz zgodności wewnętrznych procedur z przepisami prawa[45]. To wymaga nie tylko inwestycji finansowych, ale również zrozumienia, że bezpieczeństwo jest procesem ciągłym, a nie jednorazowym działaniem.

Ponadto, menedżerowie i właściciele powinni rozumieć, że bezpieczeństwo to nie tylko obowiązek, ale i inwestycja, która może przynieść długoterminowe korzyści, takie jak zwiększenie zaufania klientów, lepsza pozycja rynkowa oraz redukcja ryzyka finansowego i operacyjnego.

Podsumowując, autor rozpoczął omawianie problematyki od przedstawienia podstawowej definicji bezpieczeństwa, wskazując na jego percepcję jako stanu niezagrożenia i psychicznego komfortu. Następnie rozszerza tę definicję, uwzględniając różnorodne

[43] A. Woody, *Enterprise security: A data-centric approach to securing the enterprise*, Packt Publishing, Birmingham 2013, s. 37-41.
[44] P. Lula , R. Oczkowska, S. Wiśniewska, K. Wójcik K, *An attempt to estimate the competency gap in the IT sector*, „International Entrepreneurship Review", 2019, vol. 5, nr 3, DOI: 10.15678/IER.2019.0503.07. s. 96-98.
[45] I. Sprycha, M. Kurek, J. Wysocka-Golec, *Nowy wymiar compliance*, KPMG, https://kpmg.com/pl/pl/home/insights/2024/03/nowy-wymiar-compliance.html? [dostęp 03.10.2024 r.].

perspektywy i wymiary bezpieczeństwa – od fizycznego po informacyjne, a następnie przytoczył wybrane definicje bezpieczeństwa w ujęciu funkcjonowania przedsiębiorstwa. Kluczowym wnioskiem jest, że bezpieczeństwo jest nie tylko fundamentalną potrzebą ludzką, ale również kluczowym elementem funkcjonowania organizacji. Wymaga ono holistycznego podejścia, które obejmuje zarówno zabezpieczenia technologiczne, jak i kulturowe, podkreślając potrzebę ciągłego dostosowywania się do zmieniających się zagrożeń. Ponadto, bezpieczeństwo jest przedstawione jako proces ciągły, wymagający zarówno zrozumienia obecnych wyzwań, jak i przewidywania przyszłych.

Niniejszy podrozdział dotyczy przedstawienia roli bezpieczeństwa w zarządzaniu przedsiębiorstwem i stanowi podstawę do zrozumienia kluczowych pojęć, jakie będą analizowane w dalszych rozważaniach. Autor jako punkt wyjścia, obrał zdefiniowanie pojęcia bezpieczeństwa. Następnie przedstawione zostały różne ujęcia bezpieczeństwa – zarówno w kontekście jednostki (psychiczny i prawny spokój), jak i organizacji (przetrwanie, rozwój oraz realizacja interesów). Autor omówił cztery podstawowe stany bezpieczeństwa, jak również sklasyfikował bezpieczeństwo jako potrzebę fundamentalną dla funkcjonowania ludzi i organizacji, odnosząc się do piramidy potrzeb Maslowa.

Dalsza część wywodu, poświęcona została na przedstawienie zmiennych perspektyw interpretacji bezpieczeństwa. Tradycyjnie skupione na zagrożeniach państwowych, współczesne ujęcie kładzie nacisk na zarządzanie szerokimi wyzwaniami cywilizacyjnymi oraz na adaptację organizacji do przyszłych zmian. Bezpieczeństwo w organizacji należy rozważać z dwóch perspektyw: statycznej, związanej z obecnym stanem i zasobami organizacji, oraz dynamicznej, koncentrującej się na zdolności adaptacyjnej organizacji w zmieniającym się środowisku. Zwraca się również uwagę na różnorodność wymiarów bezpieczeństwa organizacji: fizyczne, informacyjne, finansowe, technologiczne, instytucjonalno-regulacyjne, kadrowe, a także na znaczenie współpracy z interesariuszami.

Odnosząc powyższe do hipotezy szczegółowej: *racjonalne zarządzanie bezpieczeństwem, w tym wdrażanie odpowiednich procesów decyzyjnych oraz strategii identyfikacji i minimalizacji ryzyka, warunkuje ciągłość działania organizacji oraz zabezpieczenie jej kluczowych zasobów* niniejszy podrozdział potwierdza kilka jej elementów:

a) strategie identyfikacji i minimalizacji ryzyka – bezpieczeństwo organizacji wymaga aktywnego dostosowywania do zagrożeń poprzez opracowywanie scenariuszy oraz stosowanie ochrony fizycznej i informacyjnej. Opisane są szczegółowe zabezpieczenia i metody ochrony informacji, co potwierdza praktyki identyfikacji i minimalizacji ryzyka,

b) zabezpieczenie kluczowych zasobów organizacji – wymieniając m.in. bezpieczeństwo finansowe, kadrowe i technologiczne, autor potwierdza, że organizacja zabezpiecza swoje zasoby, co stanowi podstawę stabilnego funkcjonowania,
c) ciągłość działania organizacji – dyskusja o bezpieczeństwie jako dynamicznym procesie, wymagającym regularnego dostosowania i inwestycji, wskazuje na istotność zarządzania bezpieczeństwem w celu zapewnienia ciągłości operacyjnej.

Autor zatem potwierdza potrzebę wdrożenia systematycznego zarządzania bezpieczeństwem organizacji, co wpisuje się w częściowe potwierdzenie hipotezy szczegółowej, iż racjonalne procesy decyzyjne i strategie minimalizowania ryzyka są kluczowe dla ciągłości działania i ochrony zasobów.

1.2 Optymalizacja zarządzania bezpieczeństwem w kontekście działalności przedsiębiorstwa

Funkcjonowanie przedsiębiorstwa w erze cyfrowej powinno zostać oparte na solidnym fundamencie w postaci dobrze funkcjonującego systemu bezpieczeństwa. W obliczu stale rosnących zagrożeń atakami cybernetycznymi, naruszeniami danych oraz nieautoryzowanym dostępem do zasobów, niezbędnym jest, aby organizacje priorytetowo traktowały wdrożenie kompleksowych mechanizmów bezpieczeństwa. Taki sposób podejścia do zagadnienie, nie tylko ochroni wrażliwe informacje, ale również zapewni niezawodność i wiarygodność usług oraz produktów przedsiębiorstwa. Aby zapewnić określony poziom bezpieczeństwa, należy wdrożyć różnorodne środki obejmujące stosowanie zabezpieczeń fizycznych, osobowych oraz elektronicznych. Natomiast odpowiednie zarządzanie systemem bezpieczeństwa powinno odbywać się w oparciu o trzy filary: zarządzanie ryzkiem, zarządzanie wiedzą oraz dobre praktyki bezpieczeństwa. Wyszczególnione elementy odgrywają kluczową rolę w zapewnieniu ochrony zasobów przedsiębiorstwa.

Poziom bezpieczeństwa zależy również od rzetelnie i kompleksowo przekazanej wiedzy na temat standardów bezpieczeństwa oraz dobrych praktykach w przedsiębiorstwie pracownikom organizacji. Programy szkoleniowe i dokumentacja mogą stanowić istotny wkład w edukację personelu oraz pomoc w uzyskaniu umiejętności niezbędnych do rozpoznawania i reagowania na potencjalne zagrożenia związane z funkcjonowaniem przedsiębiorstwa. W ostatecznym rozrachunku, silny system bezpieczeństwa chroni nie tylko organizację i jej użytkowników, ale także buduje zaufanie i pewność co do jej działalności.

Przystępując do omówienia problematyki funkcjonowania systemu bezpieczeństwa w przedsiębiorstwie teleinformatycznym należałoby rozpocząć od rzetelnego zdefiniowania

samego pojęcia systemu bezpieczeństwa. Zgodnie z koncepcją wypracowaną przez badaczy Akademii Sztuki Wojennej, system bezpieczeństwa stanowią *wszystkie elementy wraz z wszelkimi powiązaniami, zapewniające przetrwanie, funkcjonowanie i rozwój podmiotu bezpieczeństwa, a także realizację jego interesów*[46]. Przedstawiona definicja prezentuje holistyczne ujęcie elementów tworzących system odpowiadający za bezpieczeństwo, jednak stanowi solidny fundament na potrzeby dalszych rozważań na temat systemy bezpieczeństwa w przedsiębiorstwie teleinformatycznym ze względu na dwa istotne elementy definicji – przetrwanie, funkcjonowanie i rozwój podmiotu oraz realizację jego interesów. Nieco węższe i ukierunkowane podejście prezentowane jest przez badaczy Politechniki Kijowskiej, którzy zwracają uwagę, iż *efektywny system bezpieczeństwa przedsiębiorstwa polega na integracji dwóch składników: zapewnieniu efektywności zestawu działań mających na celu osiągnięcie bezpieczeństwa oraz zdolności do odpowiedniego reagowania w odpowiednim czasie na zagrożenia pochodzące ze środowiska zewnętrznego i wewnętrznego*[47]. Definicja ta podkreśla rolę reagowania, w odpowiednim czasie, na zagrożenia pochodzące z zewnętrznego i wewnętrznego otoczenia organizacji. Ponadto, problematyka zapewnienia bezpieczeństwa przedsiębiorstwa w kontekście wyzwań otoczenia wewnętrznego i zewnętrznego jest kluczowa dla osiągnięcia zrównoważonego rozwoju oraz zwiększenia konkurencyjności.

Bezpieczeństwo jest nieodłączną cechą procesu zarządzania przedsiębiorstwem i stanowi wszechstronny rodzaj działalności ekonomicznej, który przenika wszystkie procesy zarządzania, w tym elementy strategii i planów operacyjnych. Skuteczne funkcjonowanie systemu bezpieczeństwa przedsiębiorstwa możliwe jest dzięki zastosowaniu zintegrowanego podejścia z wykorzystaniem specjalistycznych technologii, metod i narzędzi. Synergiczny efekt ich użycia ma na celu osiągnięcie pozytywnego rezultatu końcowego, którym jest stabilna i bezpieczna działalność przedsiębiorstwa jako systemu ekonomicznego. Różnorodne podejścia do funkcjonowania systemu bezpieczeństwa przedsiębiorstwa zostały przedstawione w tabeli nr 2.

Tabela 2 Podejścia do funkcjonowania systemu bezpieczeństwa przedsiębiorstwa

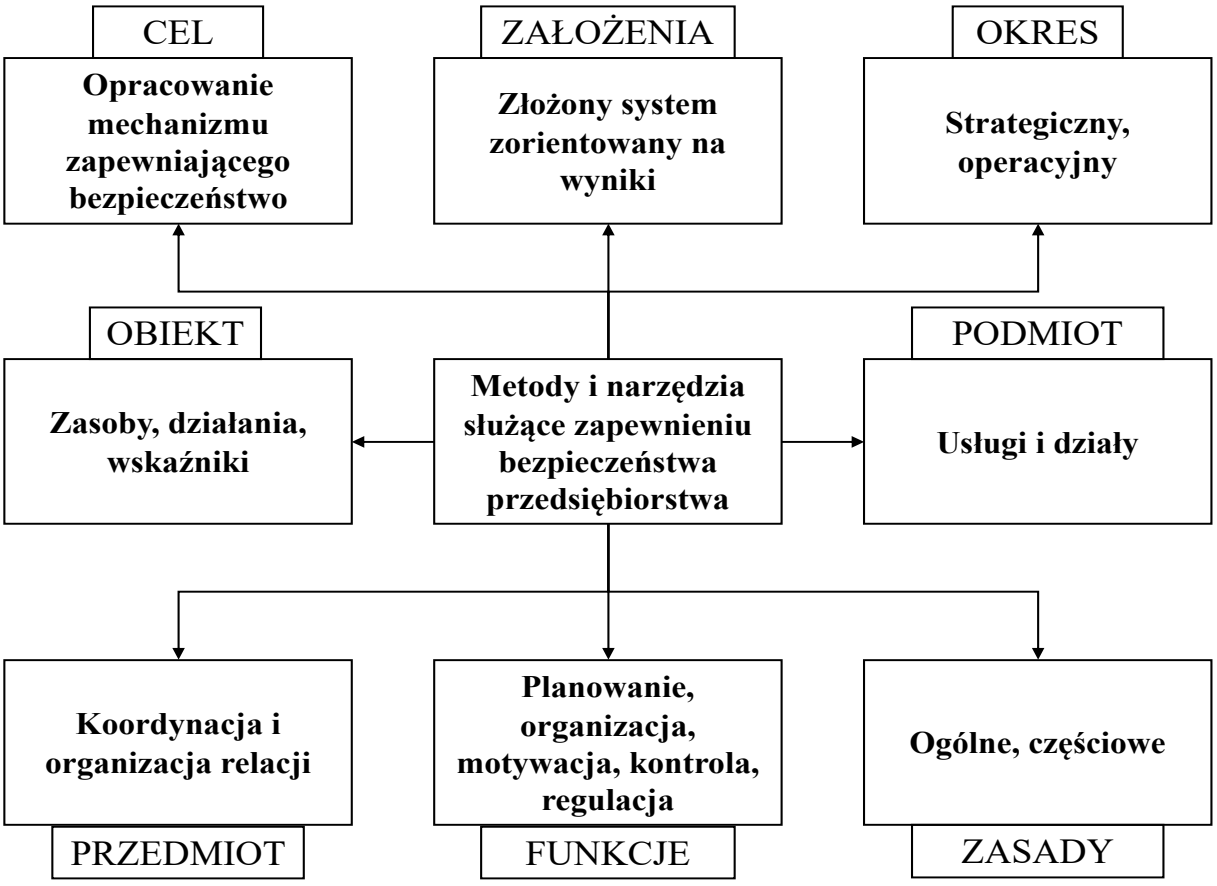
Lp.	Podejście	Istota
1.	W odniesieniu do procesów zarządzania	rozróżnienie procesów opracowywania, wdrażania i zarządzania bezpieczeństwem przedsiębiorstwa.

[46] *Słownik terminów z zakresu bezpieczeństwa…*, op. cit., s. 220.
[47] N. Iershova, V. Garkusha, *Functioning of the system of ensuring the economic security of the industrial enterprise: conceptual provisions*, „Economics & Education", 2021 nr 06(02), s. 38.

Lp.	Podejście	Istota
2.	W odniesieniu do obiektów zarządzania	system bezpieczeństwa przedsiębiorstwa wygodnie jest podzielić na oddzielne podsystemy dla różnych obiektów (zasobów, działań), taki podział zapewni lepsze i terminowe zarządzanie.
3.	W odniesieniu do elementów	cel, założenia, zasady, funkcje, przedmiot i podmiot, narzędzia, metody, regulacje.

Źródło: N. Iershova, V. Garkusha, Functioning of the system…, op. cit., s. 39.

Rozwój koncepcji funkcjonowania systemu bezpieczeństwa przedsiębiorstwa, jego organizacja, jak również praktyczne wdrożenie, powinno opierać się na racjonalnym zestawie zasad teoretycznych, praktycznych oraz przewidywalności pewnych zjawisk. Zasady te odnoszą się do struktury, funkcji, zasad, kwestii organizacyjnych oraz metod dla konkretnego przedsiębiorstwa. Wskazane elementy zostały przedstawione na rysunku nr 2.



Rysunek 2 Koncepcyjne podstawy funkcjonowania systemu bezpieczeństwa przedsiębiorstwa

Źródło: N. Iershova, V. Garkusha, Functioning of the system…, op. cit., s. 40.

Zapewnienie efektywnego funkcjonowania systemu bezpieczeństwa przedsiębiorstwa wymaga przeprowadzenie następujących kroków:

a) doboru składników i opracowania technologii organizacji funkcjonowania systemu bezpieczeństwa,
b) zarządzania składnikami systemu bezpieczeństwa, które zapewniają optymalizację kosztów,
c) opracowania i wdrożenia odpowiednich metod bezpieczeństwa,
d) organizacji odpowiedniej pracy serwisowej, rozwoju informacyjnego i metodycznego wsparcia dla mechanizmu bezpieczeństwa ekonomicznego,
e) ustalenia terminów wprowadzenia informacyjnego i metodycznego wsparcia dla mechanizmu bezpieczeństwa ekonomicznego,
f) stworzenia efektywnego systemu kontroli nad przestrzeganiem wymagań dotyczących organizacji bezpieczeństwa ekonomicznego[48].

Funkcjonowanie systemu bezpieczeństwa przedsiębiorstwa jest uzależnione od działania czynników takich jak: zdolności, możliwości, pragnienia, zainteresowania i aspiracje[49].

Podejście prezentowane przez badaczy i praktyków anglosaskich, zwłaszcza amerykańskich w istotnej mierze odbiega od tego prezentowanego przez badaczy ukraińskich. Zgodnie z dotychczasowymi rozważaniami, organizacje o charakterze biznesowym, swoje systemy bezpieczeństwa budują w oparciu o architekturę bezpieczeństwa przedsiębiorstwa (ang. *enterprise security architecture*). Pojęcie to definiowane jest jako metodyka i proces używane do opracowania ram bezpieczeństwa nastawionych na ryzyko oraz kontroli biznesowych. Głównym zadaniem architekta przedsiębiorstwa powinno być dostosowanie kontroli i procesów bezpieczeństwa informacji do strategii, celów i założeń biznesowych[50].

Pierwszym korkiem uproszczonego podejścia zwinnego do budowy programu architektury bezpieczeństwa jest:

a) identyfikacja celów biznesowych, strategii i założeń przedsiębiorstwa,
b) określenie atrybutów biznesowych, które są wymagane do osiągnięcia tych celów,
c) identyfikacja wszystkich ryzyk związanych z atrybutami, które mogą przeszkodzić przedsiębiorstwu w osiągnięciu jego celów,
d) identyfikacja wymaganych kontroli do zarządzania ryzykiem,
e) określenie programu do projektowania i wdrażania tych kontroli, w tym:
    a. zdefiniowanie koncepcyjnej architektury dla ryzyka biznesowego,
    b. określenie sposobu zarządzania, polityki oraz architektury domenowej,

[48] N. Iershova, V. Garkusha, *Functioning of the system…*, op. cit., s. 39-40.
[49] Ibidem.
[50] R. Ghaznavi-Zadeh, *Enterprise Security Architecture— A Top-down Approach*, „ISACA JOURNAL", 2017 nr 4, s. 3-4.

c. wskazanie sposobu zarządzania ryzykiem operacyjnym,
d. określenie architektury informacji,
e. wskazanie sposobu zarządzania certyfikatami,
f. określenie architektury kontroli dostępu,
g. wskazanie sposobu reagowania na incydenty,
h. zapewnienie bezpieczeństwa aplikacji,
i. określenie architektury usług internetowych,
j. zapewnienie bezpieczeństwa komunikacji,

f) określenie fizycznej architektury bezpieczeństwa i jej powiązania z koncepcją bezpieczeństwa, w tym bezpieczeństwa:
   a. platformy,
   b. sprzętu,
   c. sieci
   d. systemu operacyjnego,
   e. katalogów,
   f. plików,
   g. baz danych wraz z praktykami i procedurami,
g) określenie architektury komponentów i ich powiązanie z architekturą fizyczną, w tym:
   a. standardy bezpieczeństwa (np. National Institute of Standards and Technology [NIST] w USA, ISO),
   b. produkty i narzędzia zabezpieczające (np. antywirus [AV], wirtualna sieć prywatna [VPN], firewall, bezpieczeństwo sieci bezprzewodowych, skaner podatności),
   c. Zabezpieczenie usług internetowych (np. protokół HTTP/HTTPS, interfejs programowania aplikacji [API], firewall aplikacji internetowych [WAF]),
h) określenie architektury operacyjnej, w tym:
   a. przewodniki implementacji,
   b. administracja,
   c. zarządzanie konfiguracją i uaktualnieniami,
   d. monitorowanie,
   e. logowanie,
   f. testy penetracyjne,
   g. zarządzanie dostępem,
   h. zarządzanie zmianami,

i. analizy kryminalistyczne itp.[51]

Po zidentyfikowaniu i ocenie ryzyka, przedsiębiorstwo może rozpocząć projektowanie komponentów architektury, takich jak polityki, świadomość użytkowników, sieć, aplikacje i serwery. Proces ten jest szczególnie istotny dla procesu zapewniania bezpieczeństwa i efektywności operacji organizacji. Wobec powyższego, badacze i praktycy amerykańscy opracowali trzy modele odpowiadające za wdrożenie i funkcjonowanie w przedsiębiorstwie architektury bezpieczeństwa[52]. Przedmiotowe modele przedstawiono w tabeli nr 3.

Tabela 3 Modele systemu bezpieczeństwa przedsiębiorstwa

Lp.	Nazwa modelu	Autor	Opis	Założenia
1.	Model Bell-LaPadula[53]	D. E. Bell, L. J. LaPadula	Najczęściej kojarzony z polityką klasyfikacji stosowaną przez wojsko, która skupia się na poufności danych na wyższych poziomach wrażliwości niż na zdolności użytkowników do modyfikacji tych danych, zarówno celowej jak i przypadkowej.	Model składa się z czterech komponentów: - podmiotów (użytkowników i procesów wykonawczych systemu), - obiektów (elementów danych), - trybów dostępu (odczyt, zapis, wykonanie i ich kombinacje), - poziomów bezpieczeństwa (klasyfikacja bezpieczeństwa). Wskazane elementy odpowiadają za ustalenie trzech zasad bezpieczeństwa - poziom podmiotu musi być co najmniej równy poziomowi obiektu, jeśli tryb dostępu pozwala na odczyt, - poziom obiektu musi być co najmniej równy poziomowi podmiotu, jeśli tryb dostępu pozwala na zapis, - operacja nie może zmienić poziomu klasyfikacji obiektu.

[51] Ibidem.
[52] M. J. Decker, *Enterprise Security Capability: Common Models* W: *Encyclopedia of Information Assurance* (red.) R. Herold, M. K. Rogers, CRC Press, Londyn 2010, s. 1019.
[53] D. E. Bell, L. J. LaPadula, *Secure computer system: Unified exposition and Multics Interpretation*, Mitre Corporation, Bedford 1976, s. 19-23.

Lp.	Nazwa modelu	Autor	Opis	Założenia
2.	Model integralności Biby[54]	K. J. Biba	Model opiera się na hierarchii poziomów integralności. Poziomy te (hierarchia klasyfikacji bezpieczeństwa) przypisywane są podmiotom (użytkownikom, programom) oraz obiektom (elementom danych) i opierają się na zasadach, które definiują politykę integralności do naśladowania.	Model wspiera pięć różnych polityk integralności, w tym: - polityka niskiego poziomu wody – umożliwia zmianę poziomu integralności obiektu lub podmiotu, ustawiając nowy poziom na niższy z poziomów integralności obiektu lub podmiotu, który ostatnio wykonał operację na obiekcie, - polityka niskiego poziomu wody dla obiektu – dodaje zezwolenie na zmianę poziomu integralności obiektu, - audytowa polityka integralności niskiego poziomu wody – dodaje zasady do mierzenia potencjalnego uszkodzenia danych, - polityka pierścienia – egzekwuje stały poziom integralności przez cały cykl życia podmiotów i obiektów. Podmioty nie mogą pisać do obiektów o wyższym poziomie integralności ani czytać obiektów o niższym poziomie integralności, - ścisła polityka integralności - dodaje do polityki pierścienia zasadę, że podmiot nie może czytać obiektów o wyższym poziomie integralności.
3.	Model Clark'a-Wilson'a[55]	D. D. Clark, D. R. Wilson	Model jest najczęściej stosowany w środowisku komercyjnym, ponieważ chroni integralność danych finansowych i księgowych	Model Clark'a-Wilson'a definiuje trzy cele integralności: - nieupoważnione podmioty nie mogą dokonywać żadnych zmian,

[54] K. J. Biba, *Integrity considerations for secure computer systems*, Mitre Corporation, Bedford 1977, s. 19-28.
[55] D. D. Clark, D. R. Wilson, *A comparison of commercial and military computer security policies*, IEEE Symposium on Security and Privacy, Oakland 1987, https://groups.csail.mit.edu/ana/Publications/PubPDFs/A%20Comparison%20of%20Commercial%20and%20Military%20Computer%20Security%20Policies.pdf [dostęp 02.01.2024 r.], s. 189-191.

Lp.	Nazwa modelu	Autor	Opis	Założenia
			oraz zmniejsza prawdopodobieństwo wystąpienia oszustw. Model skupia się na zapewnieniu, że działania w systemach informatycznych są dokładne i autoryzowane, co jest kluczowe dla utrzymania zaufania do procesów finansowych i księgowych w przedsiębiorstwie.	- upoważnione podmioty nie mogą dokonywać nieautoryzowanych zmian, - utrzymana jest spójność wewnętrzna i zewnętrzna. Ponadto, model wprowadza dwa mechanizmy do realizacji wyznaczonych celów: - dobrze sformowane transakcje, które wprowadzają koncepcję dualności dla każdej transakcji, - separacja obowiązków, która zakazuje jednej osobie dostępu do obu stron dobrze sformowanej transakcji oraz do wszystkich etapów kompletnego procesu transakcyjnego.

Źródło: opracowanie własne.

Model Bell-LaPadula jest skuteczny w środowisku wojskowym, ale nie nadaje się dla podmiotów komercyjnych ze względu na brak zaadresowania problematyki integralności danych. Model Biby rozwiązuje problem związany z brakiem integralności danych, jednak dalej jest niewystarczający w środowisku komercyjnym ze względu na niski poziom zapobieżenia incydentom manipulacji danych przez pojedynczego użytkownika o wysokim poziomie uprawnień. Natomiast model Clark'a-Wilson'a nie przypisuje poziomów klasyfikacji do danych ani użytkowników. Zamiast tego, wprowadza ścisłe kontrole dotyczące programów mających uprawnienia do manipulowania określonymi danymi i użytkowników mających dostęp do tych programów[56].

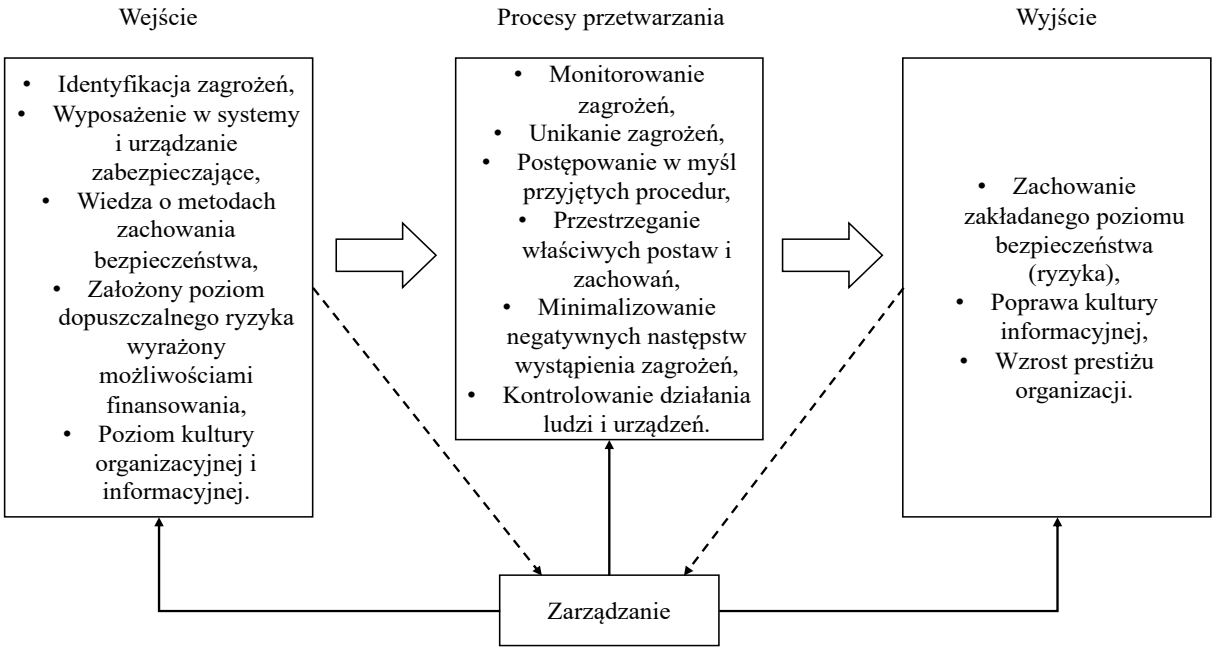
Mirosław Kwieciński zauważa, że system bezpieczeństwa organizacji *jest to celowo zaprojektowany i zorganizowany układ materialny, zespołów ludzkich i informacyjny (ideowy) eksploatowany przez człowieka, służący zachowaniu założonego poziomu oddziaływania zróżnicowanych zagrożeń (ryzyka) w celu zachowania bytu organizacji w postaci zapewnienia niezbędnych zasileń i samodzielnego kształtowania możliwości rozwoju w danych warunkach*

[56] M. J. Decker, *Enterprise Security Capability: Common…,* op. cit., s. 1020-1021.

otoczenia[57]. System bezpieczeństwa organizacji obejmuje układ wektorów i wycinkowe podsystemy zarządzania. W skład wektorów wchodzą:

a) wektor wejścia – dostarczanie niezbędnych aktywów,
b) wektor procesów przetwarza
c) nia – obejmujący szeroko rozumiane procesy bezpieczeństwa,
d) wektor wyjścia – obejmujący produkty będące efektem tych procesów)[58].

Wycinkowe podsystemy zarządzania bezpieczeństwem odnoszą się do specyficznych segmentów zarządzania wewnątrz organizacji, które są odpowiedzialne za różne aspekty bezpieczeństwa. Układ przedstawionych wektorów został zaprezentowany w sposób graficzny w ramach rysunku nr 3.



Rysunek 3 System bezpieczeństwa organizacji
Źródło: opracowanie własne na podstawie M. Kwieciński, Zarządzanie bezpieczeństwem działalności…, op. cit.

Głównymi elementami tworzącymi wektor wejścia systemu bezpieczeństwa organizacji są przede wszystkim:

a) kapitał rzeczowy – obejmuje infrastrukturę taką jak budynki, maszyny, urządzania, transport oraz finanse,
b) zasoby ludzkie – obejmują różnorodne grupy pracowników, ich umiejętności, motywację oraz inne aspekty,

[57] M. Kwieciński, *Zarządzanie bezpieczeństwem działalności przedsiębiorstwa – zarys problematyki*, PWSZ Krosno, http://archiwum.pwsz.krosno.pl/gfx/pwszkrosno/pl/defaultopisy/1155/4/1/9_miroslaw_kwiecinski_zarzadzanie_bezpieczenstwem_dzialalnosci_przedsiebiorstwa__zarys_problematyki.pdf [dostęp 16.12.2023 r.], s. 154.
[58] Ibidem, s. 155.

c) informacje – obejmują procesy pozyskiwania, gromadzenia i przetwarzania danych, a także dyfuzję wiedzy,
d) myśl ludzka – obejmuje zarówno aktualną jak i potencjalną wiedzę, włączając w to wiedzę specjalistyczną pracowników,
e) zasoby relacyjne – obejmują zewnętrzne kontakty wspierające integrację działań bezpieczeństwa,
f) zasoby naturalne – obejmują czas i przestrzeń, jako fundamentalne elementy działania[59].

Procesy przetwarzania (procesy bezpieczeństwa) to zorganizowane działania, które odpowiadają za transformację elementów wektora wejścia w rezultaty stanowiące wektor wyjściowy. Zatem wynikiem tych procesów, są następujące elementy składowe:

a) zaspokojenie potrzeb głównych beneficjentów (klientów, inwestorów, interesariuszy, mieszkańców, obywateli, itd.), które wynika z kompleksowego produktu bezpieczeństwa. Efekt ten wpływa na celowość organizacji procesu zarządzania bezpieczeństwem,
b) wzbogacenie wiedzą i kompetencjami zespołów ludzkich przez udział w dynamicznych procesach bezpieczeństwa,
c) rozwój zasobów informacji i kapitału relacyjnego, zmiany w otoczeniu i w procesach bezpieczeństwa,
d) doświadczenia negatywne (np. wypadki, kolizje, błędy) jako źródło inspiracji do doskonalenia i profesjonalizacji procesów bezpieczeństwa[60].

Wycinkowe podsystemy zarządzania bezpieczeństwem składają się z następujących elementów:

a) profilaktyka bezpieczeństwa, poświęcona monitorowaniu i analizie zagrożeń, planowaniu, szkoleniach, kontrolowaniu przestrzegania wytycznych i wyznaczaniu stref bezpieczeństwa,
b) podsystem zarządzania operacyjnego bezpieczeństwem, obejmujący aktywne reagowanie na występujące incydenty i zagrożenia, działania ratownicze oraz zabezpieczenia dowodów,
c) zarządzanie procesami logistyki bezpieczeństwa, skupione na kontrolowaniu zapasów i utrzymaniu infrastruktury transportowej,

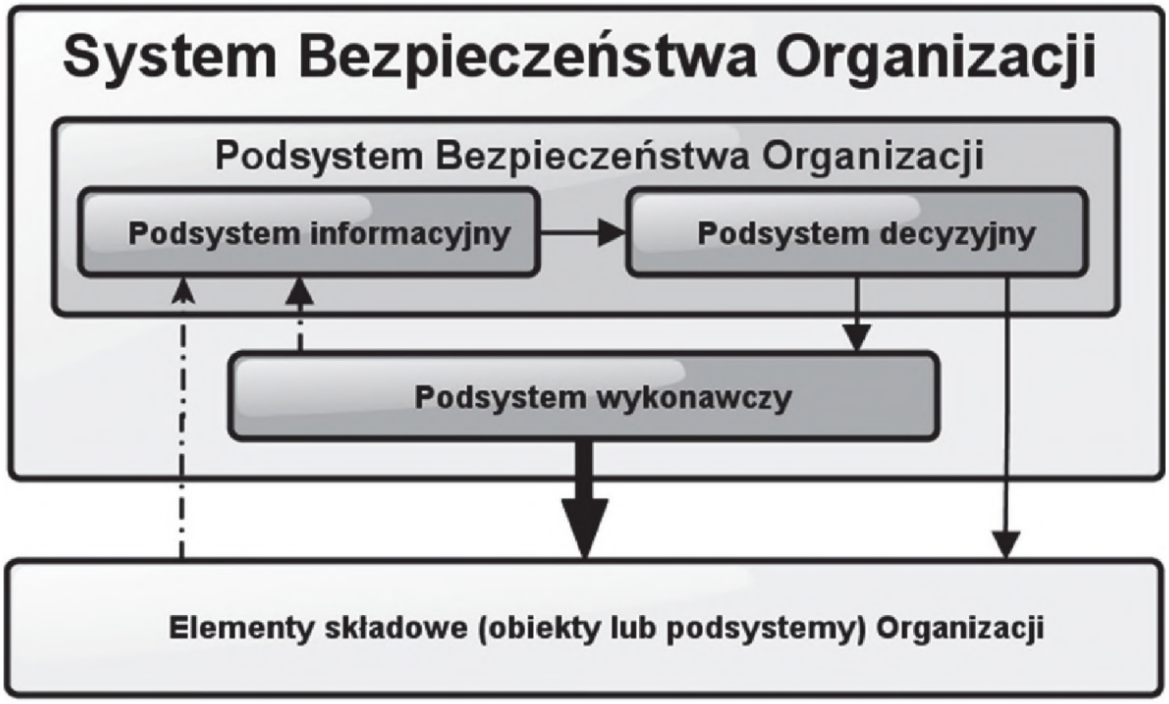
[59] M. Kwieciński, *Zarządzanie bezpieczeństwem działalności…*, op. cit.
[60] Ibidem.

d) zarządzanie likwidacją skutków zagrożeń, obejmujące pomoc poszkodowanym, ewakuację oraz działania odbudowujące[61].

Ponadto, M. Kwieciński zauważa, iż w systemie bezpieczeństwa organizacji kluczowe elementy wektora wejścia obejmują kapitał rzeczowy (infrastruktura, finanse), zasoby ludzkie (umiejętności, motywacja pracowników), informacje (procesy danych), myśl ludzką (aktualna i potencjalna wiedza), zasoby relacyjne (zewnętrzne kontakty) oraz zasoby naturalne (czas, przestrzeń). Procesy przetwarzania odpowiedzialne są za transformację tych elementów w zadowolenie beneficjentów, wzbogacenie wiedzy i kompetencji pracowników, rozwój zasobów informacyjnych i doświadczenia negatywne jako inspirację do doskonalenia funkcjonujących procesów. Podsystemy zarządzania bezpieczeństwem obejmują profilaktykę, zarządzanie operacyjne, logistykę i likwidację skutków zagrożeń.

Systemowe podejście do zapewnienia bezpieczeństwa organizacji zaprezentowane zostało również przez badaczy związanych z Wojskową Akademią Techniczną. Zgodnie przedstawionym przez nich opracowaniem, przedsiębiorstwo posiada możliwość kształtowania poziomu bezpieczeństwa dziedzinowego oraz kompleksowego. W tym kontekście, wielkościami, które można kontrolować są parametry definiujące elementy wpływające na poziom bezpieczeństwa organizacji. Obejmują one działania profilaktyczne przeciwko potencjalnym zagrożeniom dla organizacji, przygotowanie infrastruktury na możliwość wystąpienia tych zagrożeń, systemy bezpieczeństwa skonstruowane do zapobiegania tym zagrożeniom oraz procedury eliminujące skutki takich zdarzeń[62]. Każda organizacja powinna dążyć do zapewnienia sobie stabilności poziomu bezpieczeństwa. W tym celu tworzony jest system bezpieczeństwa organizacji, który został przedstawiony na rysunku nr 4.

[61] Ibidem.
[62] J. Stanik, R. Hoffman, J. Napiórkowski, *Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji,* Ekonomiczne Problemy Usług nr 123 (2016), DOI:10.18276/epu.2016.123-30, s. 325.



Rysunek 4 Struktura funkcjonalna systemu bezpieczeństwa organizacji
Źródło: J. Stanik, R. Hoffman, J. Napiórkowski, Zarządzanie ryzykiem…, op. cit., s. 326.

Podejście modelowe do Systemu Bezpieczeństwa Organizacji (SBO) wyróżnia dwa główne podsystemy: operacyjny, na który składają się zasoby i środki służące do wykonywania procesów operacyjnych oraz podsystem zarządzania bezpieczeństwem, odpowiadający za procesy informacyjno-decyzyjne determinujące sposób ochrony poszczególnych obiektów przez podsystem operacyjny.

Celem funkcjonowania Podsystemu Zarządzania Bezpieczeństwem Organizacji (PZBO) jest zachowanie pożądanego poziomu ogólnego bezpieczeństwa oraz ochrona wrażliwych zasobów. Ten cel jest realizowany poprzez ciągłą kontrolę nad podsystemem operacyjnym odpowiedzialnym za zabezpieczenia. W skład PZBO wchodzą dwa kluczowe elementy: podsystem informacyjny, który odpowiada za uzyskiwanie informacji o możliwości wystąpienia lub wystąpieniu zagrożeń oraz podsystem decyzyjny, który odpowiada za stawianie zadań związanych z przeciwdziałaniem lub neutralizacją zagrożeń.

Głównym zadaniem Systemu Bezpieczeństwa Organizacji jest przygotowanie dedykowanego podmiotu – służb bezpieczeństwa – na ewentualność wystąpienia zagrożeń, efektywnego zarządzania tymi zagrożeniami oraz odbudowa warunków sprzed ich wystąpienia.

Niniejszy podrozdział poświęcony został przedstawieniu optymalizacji zarządzania bezpieczeństwem w funkcjonowaniu przedsiębiorstw, szczególnie w kontekście zagrożeń cyfrowych i szeroko pojętego cyberbezpieczeństwa. Autor podkreślił znaczenie zintegrowanego podejścia do zarządzania bezpieczeństwem, opartego na mechanizmach

fizycznych, personalnych oraz elektronicznych, które razem zapewniają skuteczną ochronę zasobów. W celu minimalizacji zagrożeń kluczowe są trzy filary zarządzania bezpieczeństwem przedsiębiorstwa: zarządzanie ryzykiem, zarządzanie wiedzą oraz stosowanie dobrych praktyk bezpieczeństwa. Autor zwraca również uwagę na istotną rolę szkolenia pracowników, którzy powinni znać standardy bezpieczeństwa i umieć rozpoznawać potencjalne zagrożenia.

Dalsza część rozważań poświęcona została na podkreślenie, iż zarządzanie bezpieczeństwem przedsiębiorstwa powinien opierać się na stabilnych podstawach teoretycznych, praktycznych oraz na przewidywaniu zagrożeń. Zdefiniowano różne modele systemów bezpieczeństwa stosowane w przedsiębiorstwach, w tym modele anglosaskie, takie jak architektura bezpieczeństwa przedsiębiorstwa (Enterprise Security Architecture), które są dostosowane do charakteru działalności oraz strategii organizacyjnych.

W odniesieniu do hipotezy szczegółowej: *racjonalne zarządzanie bezpieczeństwem, w tym wdrażanie odpowiednich procesów decyzyjnych oraz strategii identyfikacji i minimalizacji ryzyka, warunkuje ciągłość działania organizacji oraz zabezpieczenie jej kluczowych zasobów*, podrozdział potwierdza kilka jej kluczowych aspektów:

a) strategie identyfikacji i minimalizacji ryzyka – omawiany tekst potwierdza znaczenie systematycznego podejścia do zarządzania bezpieczeństwem. Definicje systemu bezpieczeństwa przedsiębiorstwa wskazują na konieczność szybkiego i skutecznego reagowania na zagrożenia zewnętrzne i wewnętrzne, co bezpośrednio nawiązuje do identyfikacji i minimalizacji ryzyka,
b) wdrażanie odpowiednich procesów decyzyjnych – podkreślenie roli podsystemu decyzyjnego w systemie zarządzania bezpieczeństwem potwierdza znaczenie procesów decyzyjnych w organizacji. Proces ten umożliwia szybkie podejmowanie decyzji związanych z ochroną zasobów oraz przeciwdziałaniem zagrożeniom,
c) zabezpieczenie kluczowych zasobów – informacje, finanse, infrastruktura czy zasoby ludzkie, które są kluczowe dla stabilności organizacji,
d) ciągłość działania organizacji – skupienie się na integralności i stabilności operacyjnej przedsiębiorstwa jako efektu wdrożenia systemu bezpieczeństwa wyraźnie wspiera hipotezę, że efektywne zarządzanie bezpieczeństwem zapewnia ciągłość działania organizacji.

Rozważanie przedstawione w niniejszym podrozdziale częściowo potwierdzają założenia hipotezy szczegółowej, wykazując, że racjonalne zarządzanie bezpieczeństwem, łącznie z odpowiednimi strategiami oraz procesami decyzyjnymi, wpływa na zabezpieczenie zasobów i utrzymanie stabilności działania przedsiębiorstwa.

1.3 Identyfikacja i zarządzanie zagrożeniami bezpieczeństwa organizacji

Era globalizacji i cyfryzacji sprawiła, iż bezpieczeństwo staje się kluczowym wyzwaniem dla każdej organizacji. W obliczu rosnącej zależności od technologii informacyjnej i komunikacyjnej, zagrożenia dla bezpieczeństwa przedsiębiorstwa nabierają nowego wymiaru, wpływając na ich stabilność i efektywność działania.

Współczesny krajobraz bezpieczeństwa organizacji jest złożony i dynamiczny, sprawiając, że tradycyjne metody ochrony są nieustannie poddawane próbie przez nowe, bardziej wyrafinowane strategie ataków. Skutkiem rozwoju technologicznego dla organizacji jest to, iż muszą chronić nie tylko swoje cyfrowe zasoby, ale również świadomie zarządzać informacjami i wiedzą, co stanowi kluczowy element w procesie utrzymania konkurencyjności i innowacyjności[63].

Zagrożenia dla funkcjonowania organizacji nie ograniczają się jednak wyłącznie do sfery cyfrowej. W miarę zacierania się granicy pomiędzy światem fizycznym a cyfrowym, zagrożenia rozmywają się, a organizacji musi działać odpowiednio w celu zabezpieczenia całego spektrum prowadzonych operacji. Jako przykład można wskazać naruszenie (w postaci wycieku) danych medycznych gromadzonych przez firmę ALAB[64], które doprowadziło nie tylko do bezpośrednich strat finansowych, ale również do uszczerbku na reputacji, skutkującego długoterminowymi konsekwencjami dla relacji z klientami i partnerami biznesowymi.

Ponadto, w kontekście globalizacji, organizacje muszą również radzić sobie z zagrożeniami o charakterze międzynarodowym i transgranicznym. Ataki bowiem mogą pochodzić z dowolnego miejsca na świecie, co implikuje wykorzystanie współpracy międzynarodowej oraz potrzebę analizy i zrozumienia zróżnicowanych ram prawnych i regulacyjnych funkcjonujących w danym państwie. Dodatkowo. Rosnące napięcia geopolityczne i wojny informacyjne dodają kolejny poziom złożoności współczesnych zagrożeń, gdzie bezpieczeństwo organizacji może stać się elementem w szerszym kontekście międzynarodowej rywalizacji i dyplomacji[65].

---

[63] A. Brzozowska, *Information Management in a Dynamic Business Environment – A Case Study of Fractal Organisations*, Acta Universitatis Lodziensis. Folia Oeconomica 2 (367) 2024, DOI: https://doi.org/10.18778/0208-6018.367.01, s. 16.

[64] M. Dobrołowicz, K. Żak, *Wyciek danych medycznych. Spółka ALAB wydała komunikat*, RMF FM, 2023, https://www.rmf24.pl/fakty/polska/news-wyciek-danych-medycznych-spolka-alab-wydala-komunikat,nId,7175272#crp_state=1 [dostęp 15.01.2024 r.].

[65] E. Farage, *UN releases report on Ukraine telecoms damage by Russia*, Reusters 2023, https://www.reuters.com/world/europe/un-releases-report-ukraine-telecoms-damage-by-russia-2023-01-06/ [dostęp 15.01.2024 r.[oraz T. Balmforth, *Russian Hackers Were Inside Ukraine Telecoms Giant for Months*, Reuters 2024, https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/ [dostęp 15.01.2024 r.]

Dlatego też, pojawia się kluczowa kwestia sposobu klasyfikacji współczesnych zagrożeń bezpieczeństwa przedsiębiorstwa. Zgodnie z najogólniejszą klasyfikacją, zagrożenia można podzielić na następujące grupy:

a) zagrożenia strategiczne – które niosą za sobą konsekwencje dla długotrwałych planów i celów organizacji,
b) zagrożenia operacyjne – wpływające na codzienną działalność i procesy wewnątrz organizacji,
c) zagrożenia finansowe – dotyczące operacji finansowych i kapitałowych aspektów funkcjonowania organizacji,
d) zagrożenia zgodności – odnoszące się do przestrzegania obowiązujących przepisów prawnych[66].

Dokonując analizy zagrożenia w kontekście specyfiki działania określonej organizacji, można zastosować następujący podział:

a) zagrożenia niezależne od specjalistyczne wiedzy danej organizacji:
    a. zagrożenia środowiskowe, obejmujące oddziaływanie środowiska naturalnego na organizację i jej zasoby,
    b. zagrożenia związane z przerwaniem działalności organizacji[67].
b) zagrożenia wymagające wiedzy specjalistycznej, charakterystycznej dla danej organizacji:
    a. utrata kluczowych pracowników, co może prowadzić do straty cennej wiedzy organizacyjnej, sprzętu, chronionych informacji lub szczególnej wiedzy wewnątrzorganizacyjnej[68],
    b. rozstanie się z istotnym partnerem, na przykład w sferze politycznej, gospodarczej czy wojskowej,
    c. utrata dobrego wizerunku organizacji,
    d. problemy z systemami informatycznymi[69].

Biorąc pod uwagę znaczy rozwój technologii informacyjnych oraz przetwarzania i przesyłania danych poprzez sieć Internet, zagrożenia mające bezpośredni wpływ na systemy

[66] A. Żebrowski, M. Mielus, *Zagrożenia dla bezpieczeństwa informacji i wiedzy w organizacji*, Bezpieczeństwo. Teoria i Praktyka 2009 nr 3-4, s. 98.
[67] W. Rabik, *Information security as a global challenge for the 21st century*, Studia nad Bezpieczeństwem Nr 7 (2022), DOI: 10.34858/SNB.7.2022.003, s. 42
[68] T. Keary, *How mass layoffs can create new risks for corporate security*, Venture Beat 2023, https://venturebeat.com/security/how-mass-layoffs-can-create-new-risks-for-corporate-security/ [dostęp 15.01.2024 r.].
[69] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa 2008, s. 42

informacyjne i teleinformatyczne w organizacji można podzielić i sklasyfikować w następujący sposób:

a) czynniki nieprzewidywalne:
    a. zmiany w prawodawstwie, kryzysy finansowe, duża rotacja pracowników, zdarzenia naturalne – prowadzące do uszkodzenia zasobów informacyjnych, ograniczenia dostępu, obniżenia poziomu ich ochrony oraz utraty wiedzy zgromadzonej w organizacji,
b) działania nielegalne i przestępcze:
    a. zagrożenia związane z fizycznymi kradzieżami sprzętu, oprogramowania i dokumentów – co może skutkować głównie utratą dostępu do informacji i ich poufności,
    b. zagrożenia wynikające z podsłuchów, w tym wykorzystania tradycyjnych technik szpiegowskich – co może skutkować utratą poufności informacji,
    c. nieautoryzowane działania personelu – które mogą skutkować utratą dostępności, integralności i poufności informacji, a także obniżeniem poziomu ochrony,
    d. działania osób trzecich, które nie są uprawnione do dysponowania informacją – które również mogą skutkować utratą dostępności, integralności i poufności informacji oraz obniżeniem poziomu ochrony.
c) błędy personelu technicznego:
    a. pomyłki personelu obsługującego systemy komputerowe, mogące skutkować analogicznymi zagrożeniami.
d) negatywne efekty nieodpowiedniej organizacji pracy:
    a. zagrożenia związane z błędami w ochronie fizycznej i technicznej skutkujące utratą dostępności, integralności i poufności informacji.
e) awarie sprzętu i wady oprogramowania:
    a. zagrożenia w tym obszarze obejmują przede wszystkim utratę dostępności informacji oraz obniżenie poziomu ochrony[70].

Analizując również aktualne trendy związane z wojną informacyjną, czyli swoistym wyścigiem informacyjnym pomiędzy konkurującymi ze sobą organizacjami, można wyróżnić następujące obszary, będące źródłem zagrożeń dla bezpieczeństwa przedsiębiorstwa:

a) zakłócenie funkcjonowania systemów komputerowych,
b) szpiegostwo, w tym wykorzystanie technologii satelitarnych,

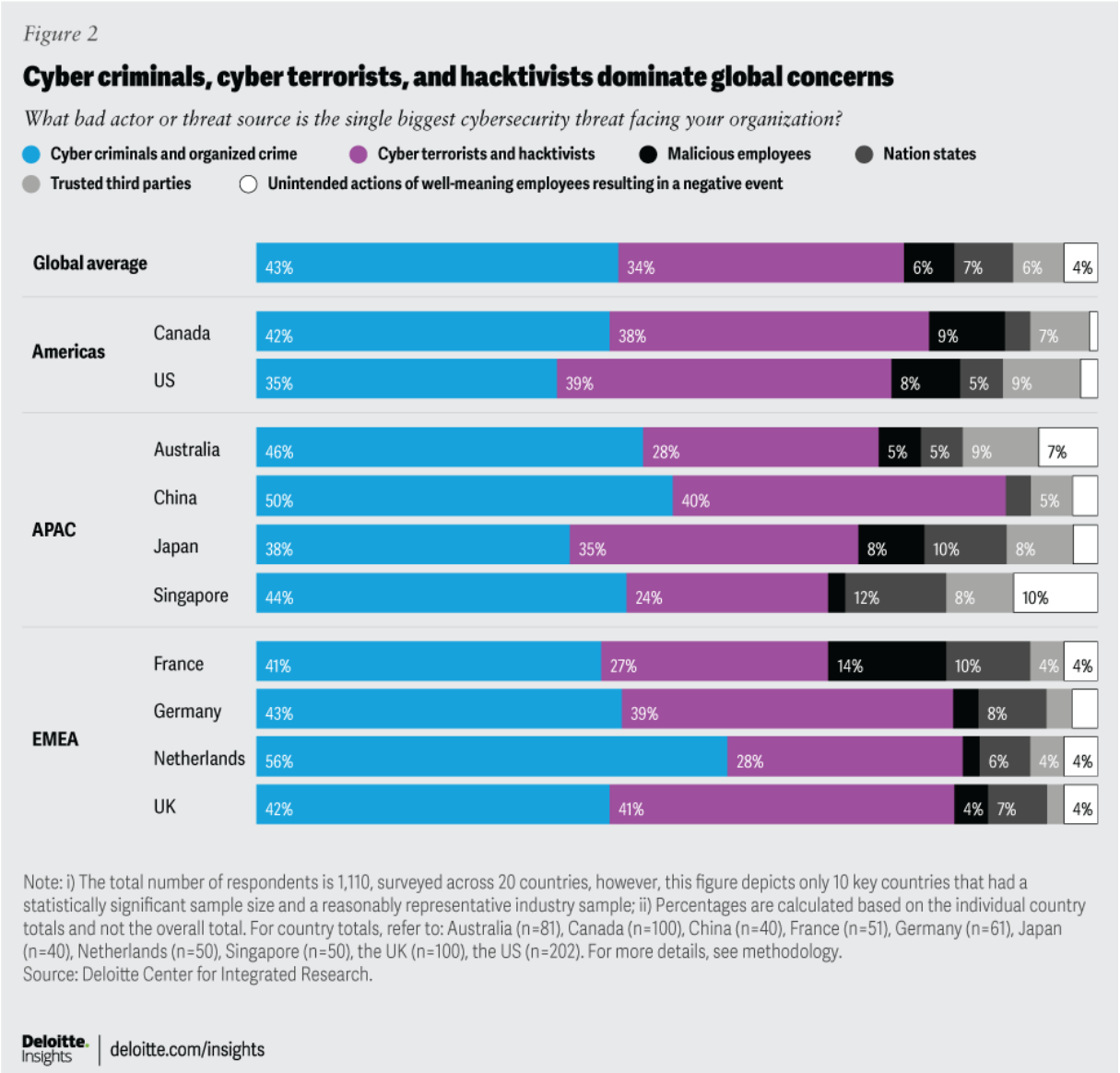
[70] Ibidem oraz A. Żebrowski, M. Mielus, *Zagrożenia dla bezpieczeństwa…*, op. cit., s. 99.

c) podsłuchy i monitoring za pomocą kamer,
d) fizyczne niszczenie sprzętu komunikacyjnego,
e) fałszowanie dokumentów, manipulowanie percepcją i stosowanie technik psychologicznych (socjotechniki),
f) wprowadzanie złośliwego oprogramowania do systemów komputerowych[71].

Pozostałe metody stosowane w ramach wojny informacyjnej obejmują takie działania jak kradzież poufnych informacji, naruszanie prywatności oraz fałszowanie korespondencji elektronicznej. Chociaż niektóre z tych działań pozostają nielegalne, inne uznawane są za nieetyczne, a jeszcze inne pozostają w sferze akceptowalnych praktyk stosowanych w szeroko pojętym biznesie, to wciąż stanowią istotne zagrożenie dla bezpieczeństwa organizacji i mogą skutecznie zakłócić procesy decyzyjne podejmowane przez czynniki decyzyjne. Takie działania mogą być powiązane z konfliktami militarnymi, osobistymi lub społecznymi, a także wpływać na działalność firm. Wszystkie te czynności łączy jeden cel – zdobycie lub wykorzystanie informacji dla korzyści agresora.

Analiza raportu przygotowanego przez firmę Deloitte zatytułowanego *2023 Global Future of Cyber Security*[72] wykazała, że przedsiębiorstwa, którym przedstawiono sześć potencjalnych zagrożeń do wyboru, prawie 40% respondentów z trzech regionów zgłosiło, że cyberprzestępczość (cyberprzestępcy i zorganizowana przestępczość) stanowi największe zmartwienie. Dane te, przedstawione na rysunku nr 5, ilustrują wszechobecną naturę cyberprzestępczości, która została zgłoszona jako budząca szczególnie duże obawy w Holandii (56%) i Chinach (50%). Drugim wiodącym aktorem zagrożeń dla organizacji byli cyberterroryści i hakerzy aktywiści (34%), na czele z Wielką Brytanią (41%) i Chinami (40 %). Chiny wydają się być szczególnie podatne, potencjalnie ze względu na rozprzestrzeniający się cyfrowy i e-commerce ekosystem w kraju.

[71] D. E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwo WNT, Warszawa 2002, s. 14.
[72] K. Fowler, K. Urbanowicz, W. Burns, *Cybersecurity threats and incidents differ by region*, Deloitte Center for Integrated Research, https://www2.deloitte.com/us/en/insights/topics/cyber-risk/global-cybersecurity-threat-trends.html [dostęp 15.01.2024 r.].



Rysunek 5 Największe zagrożenie cybernetyczne dla organizacji
Źródło: K. Fowler, K. Urbanowicz, W. Burns, Cybersecurity threats…, op. cit.

Organizacje z regionu Azji i Pacyfiku (APAC) były najbardziej zaniepokojone zagrożeniami ze strony państw narodowych i zaufanych podmiotów trzecich, na czele z Singapurem - 12% dla państw narodowych (5% powyżej średniej światowej) i Australią - 9% dla zaufanych podmiotów trzecich (3% wyżej niż średnia).

W przypadku Francji, dane wskazują na obawy powyżej średniej związane z nieuczciwymi pracownikami (o 8% wyższe niż średnia światowa). Może to być spowodowane dużym udziałem respondentów z branży usług finansowych we Francji (24% w porównaniu z 17% na świecie)[73], sektora uznawanego za podatnego na ataki od wewnątrz. Z drugiej strony, obawy związane z nieuczciwymi pracownikami w Amerykach, na czele z Kanadą - 9%, mogą mieć inne przyczyny. Zauważalnym jest, że jednym z kluczowych

[73] Ibidem.

czynników napędzających ataki od wewnątrz jest niezadowolenie pracowników dążących do pozyskania wrażliwych danych przedsiębiorstwa. W 2020 roku Kanada odnotowała dużą liczbę zwolnień, co mogło skłonić rozgoryczonych pracowników do działań przeciwko swoim byłym pracodawcom. Głównym zagrożeniem w analizowanych przypadkach, w dalszym ciągu pozostają zagrożenia ze stron cyberprzestępczości oraz przestępczości klasycznej, jak również ze strony cyberterrorystów oraz hacktywistów[74].

Obecne wyzwania w dziedzinie bezpieczeństwa przedsiębiorstwa wymagają holistycznego podejścia, które uwzględnia zarówno aspekty technologiczne, jak i ludzkie. Podstawową tezą jest, że skuteczna ochrona organizacji wykracza poza samo zastosowanie zaawansowanych technologii, obejmując także budowanie świadomości i kultury bezpieczeństwa. Świadomość zagrożeń, umiejętność rozpoznawania potencjalnych ataków, a także znajomość procedur postępowania w przypadku naruszeń bezpieczeństwa są niezbędne do skutecznego zarządzania bezpieczeństwem.

Ponadto, należy zwrócić szczególną uwagę na aspekty socjotechniczne i psychologiczne. Współczesne zagrożenia często wykorzystują słabości ludzkiego zachowania, takie jak naiwność, brak świadomości lub opór przed zmianą. W związku z tym, równie ważne jest kształtowanie kultury organizacyjnej, która promuje bezpieczeństwo jako priorytet i angażuje wszystkich pracowników w procesy ochrony danych. W rozpatrywaniu zagrożeń należy też uwzględnić postęp technologiczny, który niesie zarówno nowe możliwości, jak i nowe wyzwania[75]. Rozwój technologii cyfrowych, sztucznej inteligencji oraz nowych technologii wprowadza nowe wymiary zagrożeń, takie jak bardziej zaawansowane ataki cybernetyczne czy problemy związane z ochroną prywatności[76]. Tym samym, organizacje muszą ciągle aktualizować i dostosowywać swoje strategie bezpieczeństwa, aby sprostać tym zmieniającym się realiom.

Podsumowując, bezpieczeństwo organizacji jest dynamiczną i złożoną kwestią, która wymaga ciągłego monitorowania, adaptacji i holistycznego podejścia. Niezbędne jest połączenie zaawansowanych rozwiązań technologicznych, ciągłej edukacji i świadomości pracowników, efektywnego zarządzania ryzykiem oraz adaptacyjnej kultury organizacyjnej. Tylko poprzez takie zintegrowane podejście organizacje mogą efektywnie chronić swoje zasoby informacyjne i zapewniać długoterminową stabilność w obliczu rosnących zagrożeń cyfrowych.

---

[74] P. Krapp, *Terror and Play, or What Was Hacktivism?*, Grey Room – MIT (2005) (21), DOI: 10.1162/152638105774539770, s. 70-75.
[75] H. Świeboda, *Zagrożenia bezpieczeństwa współczesnych organizacji*, Ekonomiczne Problemy Usług 2012 nr 88, s. 827.
[76] Ibidem, s. 831.

Podrozdział ten koncentruje się na wyzwaniu bezpieczeństwa organizacyjnego w dobie globalizacji i cyfryzacji. Wskazuje, że postęp technologiczny wymusza na organizacjach zwiększenie nakładów na zarządzanie bezpieczeństwem, aby sprostać nowym, zaawansowanym zagrożeniom. Wzrost zależności od technologii informacyjnej i komunikacyjnej wprowadza nowe ryzyka – od cyberataków i wycieku danych po konieczność ochrony wizerunku i reputacji[77]. Przykłady, jak wyciek danych medycznych przedsiębiorstwa ALAB, pokazują, że naruszenia bezpieczeństwa mogą przynosić długotrwałe konsekwencje finansowe i wizerunkowe. Tekst podkreśla potrzebę klasyfikacji zagrożeń – od strategicznych i operacyjnych po finansowe i zgodności, oraz wskazuje na konieczność budowania kompleksowego systemu zarządzania bezpieczeństwem, który obejmuje zarówno aspekty technologiczne, jak i ludzkie.

Zgodnie z hipotezą szczegółową: *racjonalne zarządzanie bezpieczeństwem, w tym wdrażanie odpowiednich procesów decyzyjnych oraz strategii identyfikacji i minimalizacji ryzyka, warunkuje ciągłość działania organizacji oraz zabezpieczenie jej kluczowych zasobów*, podrozdział potwierdza kilka kluczowych elementów:

a) strategie identyfikacji i minimalizacji ryzyka – autor uwzględnił różnorodne klasyfikacje zagrożeń oraz konieczność dostosowywania strategii bezpieczeństwa do zmieniających się realiów. Opisanie nowoczesnych zagrożeń, jak ataki cybernetyczne oraz wskazanie na znaczenie zarządzania ryzykiem, potwierdza potrzebę aktywnego identyfikowania i minimalizowania ryzyka w organizacjach,
b) wdrażanie odpowiednich procesów decyzyjnych – zwrócono uwagę na potrzebę współpracy międzynarodowej, dostosowywania się do zróżnicowanych ram prawnych, a także budowania świadomości i kultury bezpieczeństwa w organizacji potwierdza rolę procesów decyzyjnych. Procesy te muszą uwzględniać analizę ryzyka, reakcję na incydenty i regularne aktualizacje procedur,
c) zabezpieczenie kluczowych zasobów – autor podkreślił potrzebę ochrony szerokiego zakresu zasobów organizacji, w tym informacji, kapitału ludzkiego, reputacji oraz infrastruktury IT, które są kluczowe dla stabilności i wiarygodności organizacji,
d) ciągłość działania organizacji – scharakteryzowanie potrzeby wdrożenia adaptacyjnej kultury organizacyjnej oraz integracji zaawansowanych rozwiązań technologicznych potwierdza, że organizacje muszą stale dążyć do utrzymania ciągłości operacyjnej w dynamicznie zmieniającym się środowisku.

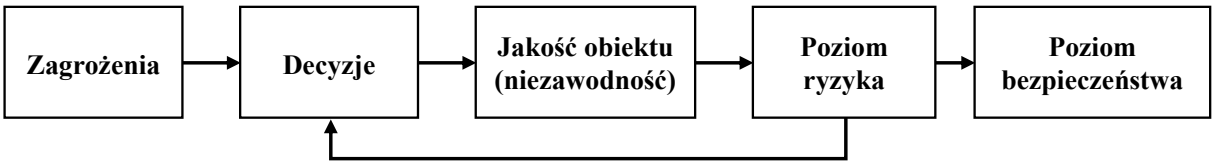
[77] P. Wróbel, *Implementing full-time remote work in the IT sector: Consequences and solutions*, „Scientific Papers of Silesian University of Technology. Organization and Management Series", 2023, nr 178, DOI: 10.29119/1641-3466.2023.178.43, s. 787.

Podsumowując, rozważanie przedstawione w niniejszym podrozdziale w sposób częściowy potwierdzają hipotezę, że racjonalne zarządzanie bezpieczeństwem, strategia identyfikacji i minimalizacji ryzyka oraz odpowiednie procesy decyzyjne są niezbędne dla zapewnienia ciągłości działania organizacji i ochrony jej zasobów.

1.4 Procesy i metody zarządzania bezpieczeństwem przedsiębiorstwa

Zarządzanie bezpieczeństwem przedsiębiorstwa stanowi fundament dla trwałego sukcesu i stabilności każdej organizacji w dzisiejszym, dynamicznie zmieniającym się środowisku biznesowym. W obliczu rosnących zagrożeń cybernetycznych, ewoluujących regulacji prawnych oraz ciągłych zmian w technologii i na rynkach, przedsiębiorstwa muszą nieustannie adaptować i doskonalić swoje strategie zarządzania bezpieczeństwem. Niniejszy wstęp do rozdziału pracy naukowej ma na celu zarysowanie kluczowych elementów procesu zarządzania bezpieczeństwem przedsiębiorstwa, podkreślając jego znaczenie, złożoność i wielowymiarowy charakter.

W perspektywie analizy systemowej, bezpieczeństwo organizacji można postrzegać jako cechę definiującą jej zdolność do przeciwstawiania się pojawieniu zagrożeń[78]. Skupić się tu należy na analizie słabych punktów systemu, czyli jego wrażliwości na niebezpieczne zdarzenia i działanie w danym okresie. Jednocześnie, bezpieczeństwo powinno być rozumiane jako zdolność organizacji do ochrony kluczowych wartości przed potencjalnymi zagrożeniami, co wiąże się bezpośrednio z takimi atrybutami systemowymi, jak jakość, wiarygodność, stabilność, równowaga i trwałość[79]. Podejście systemowe do zarządzania bezpieczeństwem przedsiębiorstwa zostało przedstawione na rysunku nr 6.

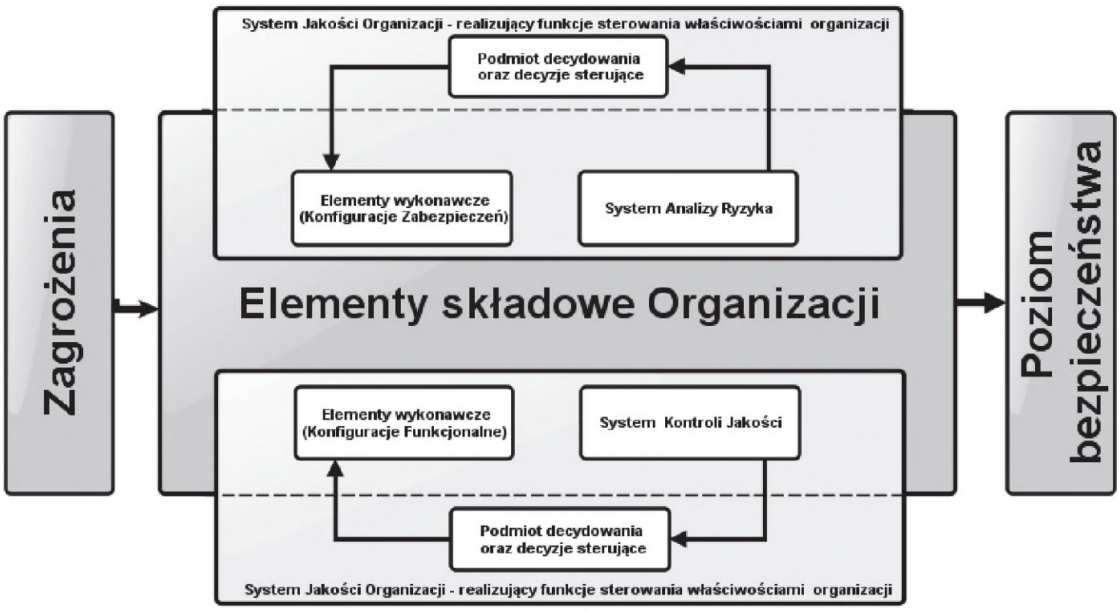


Rysunek 6 Łańcuch zarządzania bezpieczeństwem
Źródło: J. Stanik, R. Hoffman, J. Napiórkowski, Zarządzanie ryzykiem…, op. cit.

Dlatego też, zarządzanie bezpieczeństwem wewnątrz organizacji jest nierozerwalnie związane z systemowym podejściem do zarządzania, wymagającym wyboru optymalnych

[78] P. Sienkiewicz, *Badania naukowe bezpieczeństwa systemów*, W: *Wyzwania bezpieczeństwa cywilnego XXI wieku – Inżyniera działań w obszarach nauki, dydaktyki i praktyki* (red.) B. Kosowski, A. Włodarski, Fundacja Edukacja i Technika Ratownictwa, Warszawa 2007, s. 2007.
[79] J. Stanik, R. Hoffman, J. Napiórkowski, *Zarządzanie ryzykiem…,* op. cit., s. 322.

środków do utrzymania bezpieczeństwa w nieprzewidywalnym otoczeniu[80]. Celem tworzenia systemu bezpieczeństwa jest redukcja obaw i lęku przed nieznaną przyszłością, z uwzględnieniem, że zapewnienie absolutnego bezpieczeństwa jest nieosiągalne. Głównym celem jest minimalizacja, a nie całkowita eliminacja ryzyka, będącego nieodłącznym elementem egzystencji. Obszary bezpieczeństwa i niezawodności koncentrują się na zapobieganiu zagrożeniom poprzez zaplanowanie skutecznych zabezpieczeń o precyzyjnie określonych funkcjach, które muszą być efektywnie realizowane w warunkach rzeczywistego zagrożenia i w określonym czasie. Skuteczność i jakość mechanizmów ochronnych są kluczowe dla osiągnięcia żądanego poziomu bezpieczeństwa operacyjnego oraz dla zmniejszenia ryzyka wynikającego z sytuacji kryzysowych czy awarii. Wizualne przedstawienie struktury organizacji z perspektywy zarządzania jej codziennymi funkcjami użytkowymi i zapewnienia aktualnego poziomu bezpieczeństwa zostało opracowane przez naukowców z Wojskowej Akademii Technicznej. Powyższa myśl znajduje swoje odzwierciedlenie na rysunku nr 7.



Rysunek 7 Sterowanie właściwościami użytkowymi i poziomem bezpieczeństwa organizacji

Źródło: J. Stanik, R. Hoffman, J. Napiórkowski, Zarządzanie ryzykiem…, op. cit., s. 323.

Powyższy schemat, ilustrujący proces sterowania właściwościami użytkowymi i poziomem bezpieczeństwa organizacji wyróżnia trzy najistotniejsze elementy:

[80] Z. Ciekanowski, J. Majkowska, W. Załoga, *Wpływ otoczenia na funkcjonowanie organizacji*, Nowoczesne Systemy Zarządzania Zeszyt 13 (2018), nr 4 (kwiecień-czerwiec), s. 50.

a) komponenty strukturalne organizacji, definiowane jako zbiór zasobów i narzędzi oraz relacji między nimi, które umożliwiają dostarczenie produktów lub usług biznesowych określonych w misji lub wizji organizacji,
b) system bezpieczeństwa w organizacji, postrzegany jako kombinacja zasobów i metod oraz relacji pomiędzy nimi, gwarantuje osiągnięcie wymaganego poziomu bezpieczeństwa wewnątrz organizacji,
c) system jakości wewnątrz organizacji, definiowany jako zbiór zasobów i metod oraz ich wzajemnych relacji, umożliwia osiągnięcie niezbędnej lub wyjątkowej jakości i niezawodności oferowanych produktów lub usług. Jest to możliwe dzięki zarządzaniu ich użytkowymi cechami, ze szczególnym uwzględnieniem komponentów lub sektorów specyficznych dla danej organizacji[81].

Bezpieczeństwo operacyjne organizacji jest rezultatem bezpieczeństwa działania jej poszczególnych komponentów sektorowych, np.:

a) system produkcyjny czy wykonawczy, będący zespołem zasobów realizujących procesy biznesowe,
b) system zarządzania, odpowiedzialny za procesy informacyjno-decyzyjne, które wpływają na działanie podsystemu produkcyjnego,
c) systemy techniczne, które wspierają działanie systemu produkcyjnego czy zarządczego,
d) systemy informatyczne, które również są wsparciem dla produkcji lub zarządzania[82].

Poziom bezpieczeństwa operacyjnego tych komponentów jest określony przez ich indywidualne poziomy bezpieczeństwa sektorowego. Działanie każdego z tych elementów może być zakłócone przez różnorodne czynniki, w tym zagrożenia naturalne, awarie techniczne urządzeń i systemów, zagrożenia cywilizacyjne, wyzwania związane z lokalizacją i charakterem regionalnym organizacji, a także negatywne działania człowieka.

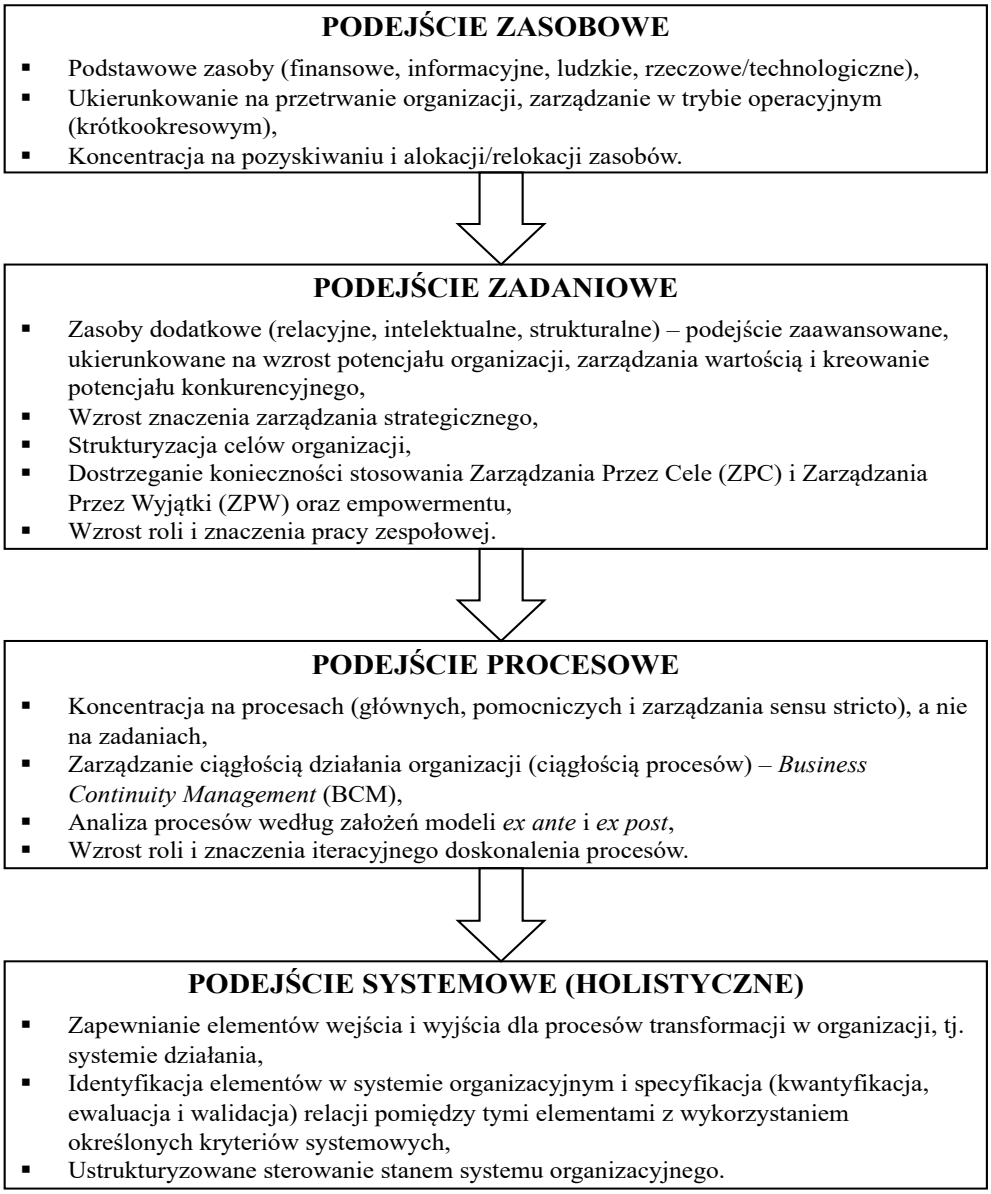
Różne typy zagrożeń mogą występować równocześnie i wywierać negatywny wpływ na komponenty organizacji. Istotne jest również uwzględnienie efektu synergii tych zagrożeń, co jest kluczowe w kompleksowej analizie bezpieczeństwa organizacji[83]. Aby zapewnić bezpieczeństwo działania organizacji, konieczne jest ciągłe zapobieganie pojawieniu się zagrożeń dla jej składowych (obiektów), systematyczne przygotowanie obiektów i jednostek odpowiedzialnych za bezpieczeństwo na możliwość wystąpienia zagrożeń, realizacja skutecznych interwencji naprawczych w razie ich wystąpienia oraz odbudowa funkcji obiektów po zneutralizowaniu zagrożeń.

[81] J. Stanik, R. Hoffman, J. Napiórkowski, *Zarządzanie ryzykiem…*, op. cit., s. 323-324.
[82] Ibidem.
[83] Ibidem, s. 325.

Poziom bezpieczeństwa organizacji w ujęciu holistycznym zależy od bezpieczeństwa specyficznych dla poszczególnych obszarów działalności. Osiągnięcie pożądanego poziomu bezpieczeństwa w danym obszarze może być realizowane na różne sposoby, nie tylko poprzez efektywne systemy zabezpieczeń bezpośrednio przeciwdziałające wystąpieniu zdarzeń. Wartość poziomu bezpieczeństwa można zwiększać przez zapobieganie zagrożeniom, przygotowanie organizacji na ewentualne aktywowanie się zagrożeń, poprawę efektywności systemów bezpieczeństwa w trakcie reagowania na zdarzenia oraz efektywne działania naprawcze po ich wystąpieniu.

Zabezpieczenie funkcjonowania organizacji może być osiągane poprzez metody zarówno zorganizowane, jak i spontaniczne (bez z góry zaplanowanego schematu działania), a także przez działania niezamierzone podejmowane przez personel, kadrę zarządzającą lub właścicieli. Należy zaznaczyć, że metoda działania nie ma pierwszorzędowego znaczenia, podstawową miarą jest rezultat w postaci realnie odczuwanego bezpieczeństwa. Jednakże, mimo że nieplanowane i sporadyczne reakcje mogą być czasami skuteczne, preferowane jest stosowanie świadomych i dobrze zorganizowanych strategii, z wyraźnie zdefiniowanymi celami i planem postępowania. W szerokim spektrum strategii zapewniania bezpieczeństwa organizacji, możemy wyróżnić głównie podejścia zasobowe, zadaniowe, procesowe oraz systemowe. Każda z tych metod opiera się na unikalnych przesłankach i charakteryzuje się różnym obszarem potencjalnych interwencji[84]. Można uznać, że każde następne podejście stanowi ewolucję i rozszerzenie o dodatkowe elementy koncepcji wcześniejszej. Wskazane metody zostały przedstawione na rysunku nr 8.

[84] J. Woźniak, *Percepcja i kształtowanie bezpieczeństwa w organizacji…,* op. cit., s. 54.



Rysunek 8 Podstawowe koncepcje zapewniania bezpieczeństwa organizacji
Źródło: opracowano na podstawie J. Woźniak, Kryterium bezpieczeństwa organizacji…, op. cit., s. 87.

Podstawową koncepcją w obrębie teorii bezpieczeństwa jest podejście zasobowe, skupiające się na kluczowych zasobach organizacji, jednak nie rozszerzające się poza granice ich pozyskiwania oraz optymalizacji ich wykorzystania w krótkoterminowej perspektywie[85]. Nie należy jednak zakładać, że ten model jest obecnie przestarzały – w szczególności w mikro i małych przedsiębiorstwach, gdzie zasoby finansowe i personel mogą być ograniczone, taka zredukowana metoda zapewniania bezpieczeństwa może okazać się wystarczająca do efektywnego osiągania celów biznesowych i generowania wartości dla interesariuszy.

[85] J. Woźniak*, Kryterium bezpieczeństwa organizacji…,* op. cit., s. 87 oraz A. Dawidczyk, *Podstawy badań bezpieczeństwa*, W: *Bezpieczeństwo. Teoria-Badania-Praktyka* (red.) A. Czupryński, B. Wiśniewski, J. Zboina, Wydawnictwo CNBOP-PIB, Józefów 2015, s. 55.

Podejście zadaniowe rozwija i poszerza koncepcję zasobową, kładąc nacisk na efektywne wykorzystanie zasobów organizacji przez skupienie się na wykonaniu istotnych zadań. W tej perspektywie, oprócz podstawowych zasobów, bierze się pod uwagę również takie kategorie jak zasoby relacyjne, intelektualne oraz strukturalne. W ramach tego podejścia, istotną rolę odgrywają zasoby ludzkie, zarządzanie wartościami, rozwijanie przewagi konkurencyjnej oraz strategiczne aspekty zarządzania[86].

Podejście procesowe stanowi rodzaj "rewolucji" w koncepcji zadaniowej, koncentrując się na procesach (które integrują różnorodne funkcje i zadania w strukturze organizacji), zamiast na pojedynczych zadaniach[87]. Kluczowe w tym podejściu jest skupienie na metodach wykonania zadań, czyli na mechanizmach zapewnienia bezpieczeństwa, a nie tylko na finalnym celu, jakim jest osiągnięcie określonego poziomu bezpieczeństwa[88]. Istotne jest również to, że podejście procesowe obejmuje wdrożenie koncepcji zarządzania ciągłością operacji w organizacji oraz tworzy fundament dla ciągłego usprawniania procesów[89]. Dlatego można uznać, że koncepcja procesowa jest bardziej adaptacyjna i umożliwia stopniowe dostosowywanie bezpieczeństwa organizacji do ewoluujących warunków otoczenia. Analiza procesowa opiera się na modelowaniu zapotrzebowania na działania przed ich implementacją (*ex ante*) oraz ocenie efektywności tych działań po ich zakończeniu (*ex post*).

Podejście systemowe (holistyczne) kładzie nacisk na wszechstronną, uwzględniającą wszelkie możliwości czasowe, kosztowe i personalne, perspektywę bezpieczeństwa organizacji oraz na kreację zintegrowanego i kompleksowego systemu jego zapewniania. Rozumiana jako najbardziej dojrzała i wymagająca koncepcja, wymaga ona znaczącego zaangażowania, pracy i zasobów ze strony organizacji. W pewnym sensie jest to model idealny, do którego organizacje powinny aspirować, aczkolwiek nie zawsze jest to konieczne lub możliwe[90]. Ponadto, takie podejście do bezpieczeństwa powinno również uwzględniać udział interesariuszy zewnętrznych, którzy nie tylko dostarczają kluczowe zasoby dla organizacji, ale również korzystają z jej działań. Ta sytuacja wydaje się potwierdzać, że interesariusze zewnętrzni mają wpływ na bezpieczeństwo organizacji, jednocześnie będąc od niego zależnymi.

---

[86] J. Woźniak*, Kryterium bezpieczeństwa organizacji…,* op. cit., s. 87 oraz S. Koziej, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, Bezpieczeństwo Narodowe II-2011 (18), Biuro Bezpieczeństwa Narodowego, Warszawa 2011, s. 21-29.

[87] A. Bitkowska, *Uwarunkowania realizacji projektów wdrożenia zarządzania procesowego*, Studia i Prace Kolegium Zarządzania i Finansów, Zeszyt Naukowy 186/2022, https://doi.org/10.33119/SIP.2022.186.2, s. 32.

[88] Ibidem, s. 34.

[89] J. Woźniak*, Kryterium bezpieczeństwa organizacji…,* op. cit., s. 87 oraz A. Czupryński, *Bezpieczeństwo w ujęciu teoretycznym…,* op. cit., s. 14.

[90] J. Woźniak*, Kryterium bezpieczeństwa organizacji…,* op. cit., s. 87 oraz P. Zaskórski, J. Woźniak, K. Szwarc, Ł. Tomaszewski, *Zarządzanie projektami w ujęciu systemowym*, Wojskowa Akademia Techniczna, Warszawa 2015, s. 398.

W odniesieniu do współczesnych przedsiębiorstw, nie można pomijać wpływu procesów cyfryzacji, które są kluczowym czynnikiem kształtującym ich operacje. Cyfryzacja oddziałuje na innowacyjność, budowanie relacji z akcjonariuszami, rozwijanie konkurencyjności, akwizycję oraz dystrybucję zasobów i zarządzanie wiedzą[91]. W ostatnich latach zaistniała konieczność badania i oceny nowych aspektów bezpieczeństwa, w tym bezpieczeństwa technologicznego i cyfrowego, bezpieczeństwa w kontekście współdzielenia zasobów i modeli biznesowych, a także bezpieczeństwa wynikającego z zarządzania wiedzą, reputacją i wartościami niematerialnymi[92]. Wzrosło także znaczenie bezpieczeństwa strategicznego i, co istotne, perspektywicznego, obejmującego planowanie na horyzont czasowy dłuższy niż pięć lat. Ewolucja rodzajów i percepcji zapewniania bezpieczeństwa organizacji została przedstawiona na rysunku nr 9.

[91] G. Gierszewska, *Wspomaganie zarządzania wiedzą we współczesnych organizacjach*, W: *Gospodarka cyfrowa 2016. Zarządzanie, innowacje, społeczeństwo i technologie* (red.) A. Gąsiorkiewicz, K. Sitarski, O. Sobolewska, M. Wiśniewski, Wydział Zarządzania Politechniki Warszawskiej, Warszawa 2017, s. 20-22.
[92] E. Kulej-Dudek, P. Pypłacz, *Rola zasobów niematerialnych w kształtowaniu wartości przedsiębiorstw*, W: *Zarządzanie zasobami niematerialnymi w organizacji. Człowiek, Informacja, Wiedza, Narzędzia IT* (red.) L. Kiełtyka, W. Jędrzejczyk, Wydawnictwo TNOIK, Toruń 2022, s. 87-89.

Rysunek 9 Ewolucja rodzajów, percepcji i zapewniania bezpieczeństwa organizacji
Źródło: opracowano na podstawie J. Woźniak, Zarządzanie ryzykiem w sektorach kreatywnych, Wydawnictwo CeDeWu, Warszawa 2019, s. 24 i 29.

Podsumowując dyskurs dotyczący fundamentalnych modeli zapewniania bezpieczeństwa organizacji, warto podkreślić ich zastosowanie w realiach cyfryzacji życia codziennego i gospodarczych procesów zarządzania. Nawet podejście koncentrujące się na zasobach uwzględnia kluczowe znaczenie zasobów informacyjnych oraz technologicznych i ich strategiczne wykorzystanie w działaniach operacyjnych organizacji. Współczesne organizacje coraz częściej implementują podejście holistyczne, które adekwatnie odpowiada na

wyzwania ekonomii cyfrowej[93], w tym integrację z sieciami i platformami wirtualnymi, rozwijanie współpracy bez granic organizacyjnych oraz angażowanie interesariuszy zewnętrznych (takich jak klienci – w kontekście prosumpcji, czy podwykonawców – w ramach otwartych modeli innowacyjności) w procesy tworzenia wartości wewnątrz organizacji.

Niniejszy podrozdział dotyczy charakterystyki koncepcji zarządzania bezpieczeństwem przedsiębiorstw w kontekście globalizacji i cyfryzacji. Wskazuje, że bezpieczeństwo organizacji jest kluczowym fundamentem dla jej stabilności i trwałości. W zmieniającym się środowisku biznesowym, obarczonym zagrożeniami cybernetycznymi, rosnącymi regulacjami prawnymi i szybkim postępem technologicznym, zarządzanie bezpieczeństwem wymaga ciągłego dostosowywania strategii ochronnych. Przedstawiono różne podejścia do zarządzania bezpieczeństwem: zasobowe, zadaniowe, procesowe oraz holistyczne (systemowe), z których każde ma swoje specyficzne zastosowanie i może być użyte w zależności od potrzeb organizacji. Holistyczne podejście jest najbardziej złożone i uwzględnia współpracę z interesariuszami zewnętrznymi, a także szerokie spektrum zagrożeń, jakie niesie cyfryzacja.

W odniesieniu do hipotezy szczegółowej: *racjonalne zarządzanie bezpieczeństwem, w tym wdrażanie odpowiednich procesów decyzyjnych oraz strategii identyfikacji i minimalizacji ryzyka, warunkuje ciągłość działania organizacji oraz zabezpieczenie jej kluczowych zasobów*, podrozdział potwierdza następujące elementy:

a) strategie identyfikacji i minimalizacji ryzyka – autor podkreśla znaczenie adaptacyjnych strategii zarządzania ryzykiem w obliczu złożonych zagrożeń, w tym cyfrowych i technologicznych. Przedstawiono różne modele zarządzania bezpieczeństwem, które umożliwiają identyfikację ryzyk i ich minimalizację w sposób dostosowany do specyfiki organizacji.
b) wdrażanie odpowiednich procesów decyzyjnych – przedstawiono charakterystykę systemowych oraz procesowych, a także uwzględnienie aspektu współpracy z interesariuszami, wskazuje na istotę procesów decyzyjnych w budowaniu kompleksowego systemu zarządzania bezpieczeństwem. Procesy te zapewniają reakcję na zmieniające się zagrożenia oraz ciągłe doskonalenie strategii ochrony.
c) zabezpieczenie kluczowych zasobów – dyskusja na temat zarządzania zasobami informacyjnymi, technologicznymi i ludzkimi potwierdza potrzebę ochrony kluczowych zasobów organizacji. Zastosowanie holistycznego podejścia, obejmującego m.in. zarządzanie wiedzą i reputacją, przyczynia się do trwałości organizacji.

[93] J. Woźniak, *Percepcja i kształtowanie bezpieczeństwa w organizacji…,* op. cit., s. 56-57.

d) ciągłość działania organizacji – przedstawiona charakterystyka podejść procesowych i systemowych do bezpieczeństwa organizacji uwzględnia elementy zapewniające operacyjną ciągłość działania. Wskazuje na dążenie do minimalizacji przerw w działaniu organizacji dzięki odpowiednim systemom reagowania i przywracania funkcji po wystąpieniu zagrożeń.

Podsumowując, podrozdział częściowo potwierdza hipotezę, wskazując na to, że racjonalne zarządzanie bezpieczeństwem, obejmujące procesy decyzyjne i strategie identyfikacji ryzyka, jest kluczowe dla ochrony zasobów i zapewnienia ciągłości działania organizacji w dynamicznym środowisku biznesowym.

Rozdział 2. PRZESŁANKI IMPLEMENTACJI ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W PRZEDSIĘBIORSTWIE

2.1 Specyfika bezpieczeństwa informacji w zarządzaniu przedsiębiorstwem

W obecnej erze informacyjnej, prawo do dostępu do specyficznych danych oraz zdolność do ich efektywnego wykorzystania kluczowo wpływają na zdolność do regulowania nie tylko indywidualnych działań, ale i kształtowania całych środowisk. W tym kontekście, informacje uznaje się za aktywa strategiczne, które nie tylko stanowią cel dla działań ekspansywnych, ale również mogą być obiektem celowych działań destrukcyjnych. Te cenne zasoby napędzają i wzmacniają bazę wiedzy wykorzystywaną w różnorodnych sferach operacyjnych wszelkich organizacji[94].

Znaczący wpływ informacji na poziom świadomości i kompetencji zarówno jednostek, jak i całych organizacji jest niezaprzeczalny. Dane dotyczące specyficznych obszarów działalności są przedmiotem zainteresowania nie tylko faktycznych przeciwników. Zapewnienie ich ochrony przed nieautoryzowanym ujawnieniem jest jednym z głównych wyzwań, przed którymi stoją zarówno instytucje rządowe, jak i pozarządowe.

W dobie powszechnego dostępu do informacji niemal każdego rodzaju i treści, mamy do czynienia z szerokim spektrum potencjalnych zagrożeń. Do najbardziej krytycznych należy ryzyko niezamierzonego wycieku lub celowego pozyskiwania danych objętych ochroną prawną. Problematyka bezpieczeństwa informacyjnego jest nieustannie aktualna i towarzyszy działalności ludzkiej od zawsze. Intensywność tych zagrożeń zależy od dynamiki pojawiających się konfliktów[95].

Rozwój technologiczny i związana z nim ekspansja informacyjna działają jak miecz obosieczny, tworząc zagrożenia zarówno dla potencjalnych przeciwników, jak i dla nas samych. Środowisko, w którym funkcjonują organizacje, staje się coraz bardziej skomplikowane i zróżnicowane na poziomie zarówno krajowym, jak i międzynarodowym, co w kontekście postępu technologicznego zwiększa ich podatność na zagrożenia wewnętrzne i zewnętrzne. Wymaga to podjęcia zintegrowanych działań prawnych i organizacyjnych, mających na celu ochronę integralności systemów informacyjnych i informatycznych przed nieautoryzowanym dostępem i ich zniszczeniem. Tego typu inicjatywy muszą być wspierane

[94] A. Białas, *Bezpieczeństwo informacji…*, op. cit., s. 27.
[95] A. Żebrowski, M. Mielus, *Zagrożenia dla bezpieczeństwa informacji i wiedzy w organizacji*, Bezpieczeństwo. Teoria i Praktyka 2009 nr 3-4, s. 89.

przez działania skierowane przeciwko potencjalnym zagrożeniom oraz mające na celu zdobycie przewagi informacyjnej w procesach zarządzania.

Informacje i zgromadzona wiedza są kluczowymi zasobami, decydującymi o rozwoju i prosperowaniu każdej organizacji[96]. Dlatego też, zabezpieczenie tych wartościowych aktywów i zarządzanie nimi wymaga szczególnej uwagi ze strony uprawnionych podmiotów, zarówno w kontekście ich rozbudowy, jak i ochrony.

Prawo do dostępu do danych i zdolność do ich wykorzystywania mają zasadnicze znaczenie dla kształtowania zarówno indywidualnych, jak i zbiorowych działań[97]. W związku z tym, informacje uznaje się za aktywa strategiczne, które wymagają szczególnej ochrony przed potencjalnymi zagrożeniami zarówno zewnętrznymi, jak i wewnętrznymi. W erze globalnej wymiany danych, gdzie postęp technologiczny oferuje niespotykane dotąd możliwości komunikacji i przetwarzania informacji, pojawiają się nowe wyzwania dotyczące bezpieczeństwa. Te wyzwania nie tylko podkreślają znaczenie ochrony danych, ale również wskazują na potrzebę ciągłego adaptowania strategii bezpieczeństwa do zmieniających się warunków.

Zagrożenia dla bezpieczeństwa danych są różnorodne i ewoluują wraz z postępem technologicznym, co wymaga od organizacji zarówno rządowych, jak i pozarządowych, podejmowania zintegrowanych działań mających na celu ochronę informacji. Działania te powinny obejmować zarówno aspekty prawne i organizacyjne, jak i techniczne, aby skutecznie chronić zasoby informacyjne przed nieautoryzowanym dostępem, wyciekiem czy destrukcją. Wstęp ten stanowi punkt wyjścia do głębszej dyskusji na temat bezpieczeństwa informacyjnego i bezpieczeństwa informacji, podkreślając ich znaczenie w nowoczesnym świecie, gdzie informacja jest zarówno walutą, jak i bronią. W dalszej części niniejszego rozdziału zdefiniowane zostaną kluczowe pojęcia, przedstawione zostaną różnice i zależności między bezpieczeństwem informacyjnym a bezpieczeństwem informacji, a także omówione zostaną główne wyzwania i strategie związane z ochroną danych w różnorodnych środowiskach operacyjnych.

Wybrane ujęcia bezpieczeństwa informacji, które posłużą jako punkt odniesienia do dalszych rozważań na temat całościowego procesu ochrony informacji w nowoczesnych organizacjach, zaprezentowano w tabeli nr 4.

[96] L. Kiełtyka, *Zarządzanie informacją w organizacji – podejście systemowe*, W: *Zarządzanie zasobami niematerialnymi w organizacji. Człowiek, Informacja, Wiedza, Narzędzia IT* (red.) L. Kiełtyka, W. Jędrzejczyk, Wydawnictwo TNOIK, Toruń 2022, s. 29-30.
[97] P. Maśloch, *Globalizacja a zarządzanie bezpieczeństwem współczesnych organizacji,* Wydawnictwo ASzWoj, Warszawa 2018, s. 25-26.

Tabela 4 Wybrane definicje terminu bezpieczeństwo informacji

Lp.	Autor	Definicja
1.	K. Liderman[98]	Bezpieczeństwo informacji oznacza uzasadnione (np. analizą ryzyka i przyjętymi metodami postępowania z ryzykiem) zaufanie, że nie zostaną poniesione straty wynikające z niepożądanej zmiany, na skutek realizacji zagrożenia, wymaganych wartości istotnych kryteriów jakości informacji,
2.	D. E. Denning[99]	Działania defensywne prowadzone w ramach walki informacyjnej, której celem jest obrona zasobów informacyjnych przed następującymi atakami: zwiększeniem dostępności dla strony atakującej, zmniejszeniem dostępności dla strony defensywnej lub zmniejszeniem integralności,
3.	B. Zdrodowski, J. Pawłowski[100]	Ochrona informacji przed nieuprawnionymi: dostępem, nielegalnym wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją, rejestracją oraz zniszczeniem. Zapewnia się przez ochronę fizyczną, elektromagnetyczną i transmisji, a także przez kryptografię oraz uniemożliwienie dostępu do urządzeń i sieci,
4.	A. Białas[101]	Dziedzina zajmującą się ochroną danych niezależnie od formy ich przechowywania, przetwarzania czy przekazywania. Obejmuje to zapewnienie poufności, integralności i dostępności informacji, zarówno w systemach teleinformatycznych, jak i w formatach analogowych, takich jak dokumenty papierowe czy mikrofilmy, oraz w kontekście informacji wymienianej między ludźmi. Bezpieczeństwo informacji wymaga zatem podejścia holistycznego, które bierze pod uwagę wszystkie potencjalne wektory ataku oraz zagrożenia dla danych, niezależnie od ich formy,
5.	L. Ciborowski[102]	Bezpieczeństwo informacji to „obrona informacyjna", która polega na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego oraz planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania, a także utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych,
6.	Narodowy Standard Cyberbezpieczeństwa[103]	Ochrona informacji i systemów przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem działania, modyfikacją lub zniszczeniem w celu zapewnienia poufności, integralności i dostępności.

[98] K. Liderman, *Bezpieczeństwo informacyjne …*, op. cit.
[99] D. E. Denning, *Wojna informacyjna i bezpieczeństwo…*, op. cit., s. 41.
[100] *Słownik terminów z zakresu bezpieczeństwa…*, op. cit., s. 23-24.
[101] A. Białas, *Bezpieczeństwo informacji…*, op. cit., s. 27-28.
[102] L. Ciborowski, *Walka informacyjna*, Wydawnictwo Adam Marszałek, Toruń 2001, s. 186.
[103] *Bezpieczeństwo informacji – wprowadzenie*, Narodowy standard cyberbezpieczeństwa NSC 800-12, Ministerstwo Cyfryzacji, s. 17 i 21.

Lp.	Autor	Definicja
		Staranne wdrożenie środków bezpieczeństwa informacji jest kluczowe dla ochrony aktywów informacyjnych organizacji, jak również jej reputacji, pozycji prawnej, personelu oraz innych aktywów materialnych i niematerialnych,
7.	Microsoft[104]	Zestaw narzędzi i procedur zabezpieczeń, które szeroko chronią poufne informacje przedsiębiorstwa przed nadużyciami, nieautoryzowanym dostępem, zakłóceniami lub zniszczeniem. InfoSec obejmuje bezpieczeństwo fizyczne i środowiskowe, kontrolę dostępu oraz cyberbezpieczeństwo,
8.	PKN[105]	Bezpieczeństwo informacji oznacza ochronę informacji przed różnymi zagrożeniami w taki sposób, aby zapewnić ciągłość w prowadzeniu działalności, minimalizować straty, maksymalizować zwrot nakładów na inwestycje i działania o charakterze biznesowym,
9.	S. B. Maynard, A. Ahmad[106]	Zorganizowane stosowanie formalnych, nieformalnych i technologicznych mechanizmów kontrolnych w celu ochrony poufności, integralności i dostępności zasobów informacyjnych organizacji, przy jednoczesnym utrzymaniu zgodności z misją organizacji,
10.	A. Rychły-Lipińska, W. Kamiński[107]	Ochrona poufności, integralności i dostępności danych przed nieuprawnionym dostępem, modyfikacją lub utratą, wspierająca zarządzanie ryzykiem i stabilność operacyjną organizacji, szczególnie w kontekście technologii cyfrowej i zaawansowanych zagrożeń.

Źródło: opracowanie własne z wykorzystaniem K. Kozłowski, Technological Advancements and Their Impact on Organisational Information Security, Applied Business and Economics Journal 2024 Vol. 2 No 1, DOI: 10.61089/abej.2024.2.87, s. 5-6.

Podsumowanie przedstawionych definicji bezpieczeństwa informacyjnego wydobywa z nich wspólne elementy, które można uznać za kluczowe dla zrozumienia tego pojęcia. Przede wszystkim, bezpieczeństwo informacji charakteryzuje się jako multidyscyplinarna dziedzina skupiona na ochronie danych, niezależnie od formy ich przechowywania, przetwarzania czy przekazywania. Przytoczone definicje podkreślają trzy fundamentalne cele bezpieczeństwa

[104] *Co to jest bezpieczeństwo informacji (InfoSec)?*, Microsoft Corporation, https://www.microsoft.com/pl-pl/security/business/security-101/what-is-information-security-infosec [dostęp 15.02.2024 r.].
[105] *Zarządzanie Bezpieczeństwem Informacji*, Polski Komitet Normalizacyjny, https://www.pkn.pl/informacje/2018/01/zarzadzanie-bezpieczenstwem-informacji [dostęp 15.02.2024 r.].
[106] S. B. Maynard, A. Ahmad, *Information Security Management in High Quality IS Journals: A Review and Research Agenda*, Cryptography and Security 2022 (arXiv:2208.13087), https://doi.org/10.48550/arXiv.2208.13087, s. 2.
[107] A. Rychły-Lipińska, W. Kamiński, *Bezpieczeństwo informacji w erze pracy zdalnej a rola modelu ISO 27001:2017*, Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie Nr 53 (2024), DOI: 10.17512/znpcz.2024.1.09, s. 108.

informacji: zapewnienie poufności, integralności oraz dostępności informacji. Kluczowe elementy przedstawionych definicji można ująć w następujący sposób:

a) zaufanie do ochrony przed zagrożeniami – podkreślenie znaczenia uzasadnionego zaufania do systemów i procedur, które mają na celu ochronę przed niepożądanymi zmianami i realizacją zagrożeń, które mogłyby negatywnie wpłynąć na wartości istotne dla jakości informacji,
b) obrona przed atakami – działania defensywne mające na celu ochronę zasobów informacyjnych przed atakami, które mogą zmniejszać dostępność, integralność lub poufność danych, są wspólnym mianownikiem w definicjach, podkreślając konieczność aktywnej obrony przed potencjalnymi zagrożeniami,
c) holizm w ochronie informacji – potrzeba holistycznego podejścia do bezpieczeństwa informacji, które obejmuje zarówno aspekty fizyczne, jak elektromagnetyczne, kryptograficzne, a także ochronę przed nieautoryzowanym dostępem do urządzeń i sieci. To podejście jest niezbędne do adresowania wszystkich potencjalnych wektorów ataku,
d) ochrona przed nieuprawnionymi działaniami – położenie nacisku na ochronę przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją, rejestracją oraz zniszczeniem informacji, co jest kluczowe dla utrzymania bezpieczeństwa danych,
e) ochrona niezależnie od formy danych – znaczącym elementem jest podkreślenie, że bezpieczeństwo informacji dotyczy ochrony danych niezależnie od ich formy;
f) kompleksowość narzędzi i procedur zabezpieczających – podkreślenie roli zestawu narzędzi i procedur zabezpieczających w ochronie informacji przed nadużyciami i nieautoryzowanym dostępem, co obejmuje bezpieczeństwo fizyczne, środowiskowe, kontrolę dostępu oraz cyberbezpieczeństwo[108].

Wspólnym elementem dla przedstawionych definicji jest postrzeganie bezpieczeństwa informacji jako kluczowego elementu strategii organizacji, mającego na celu nie tylko ochronę danych, ale również zapewnienie ciągłości działalności, minimalizację strat, a także maksymalizację zwrotu z inwestycji. Bezpieczeństwo informacji jest więc rozumiane jako kompleksowe działanie, które wymaga zaangażowania na wielu poziomach organizacji oraz stosowania zróżnicowanych metod i narzędzi ochrony.

Szczególną uwagę należy zwrócić na fakt, iż bezpieczeństwo informacji jest elementem szerszej koncepcji zapewniania bezpieczeństwa organizacji, która funkcjonuje

[108] K. Kozłowski, *Technological Advancements…*, op. cit., s. 16.

w dynamicznym, zglobalizowanym świecie[109]. Dynamika zachodzących procesów niejako wymusza nieustanne dokonywanie oceny uzyskiwanych, przetwarzanych, udostępnianych oraz gromadzonych informacji na potrzeby prowadzonej działalności. Analiza zagadnień związanych z bezpieczeństwem informacji nabiera szczególnego znaczenia w kontekście ciągłych zmian i ewolucji, które są napędzane przez szybki postęp w dziedzinie technologii, w tym metod akumulacji, magazynowania, obróbki oraz dystrybucji danych. W aspekcie informacyjnym, ochrona bezpieczeństwa wiąże się z ochroną strategicznych interesów organizacji przed działaniami zarówno zamierzonymi, jak i przypadkowymi, które mogą być skierowane przeciwko jej zasobom informacyjnym. W związku z tym, działania związane z zapewnieniem bezpieczeństwa informacyjnego powinny być prowadzone w ramach kompleksowych strategii mających na celu ochronę organizacji przed wszelkimi potencjalnie negatywnymi oddziaływaniami w obszarze informacji[110].

Wybrane ujęcia bezpieczeństwa informacyjnego, które posłużą jako punkt odniesienia do dalszych rozważań na temat całościowego procesu ochrony informacji w nowoczesnych organizacjach, zaprezentowano w tabeli nr 5.

Tabela 5 Wybrane definicje terminu bezpieczeństwo informacyjne

Lp.	Autor	Definicja
1.	B. Zdrodowski, J. Pawłowski[111]	Rodzaj bezpieczeństwa, dotyczy informacji, we wszystkich etapach ich wytwarzania, przetwarzania, przechowywania i przesyłania. Realizowane poprzez przeciwdziałanie przed bezprawnym dostępem i jakąkolwiek ingerencją w dane, informacje i systemy informacyjne,
2.	J. Stanik, M. Kiedrowicz[112]	Stanowi zbiór działań, metod, procedur, podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją, zniszczeniem,

[109] A. Brzozowska, D. Bubel, A. Pabian, *Implementation of technical and information systems in environmental management*, Procedia - Social and Behavioral Sciences 213 (2015), https://doi.org/10.1016/j.sbspro.2015.11.516, s. 7.
[110] J. Stanik, M. Kiedrowicz, *Model systemu zarządzania bezpieczeństwem organizacji jako podstawa kształtowania polityki bezpieczeństwa informacyjnego*, Ekonomiczne Problemy Usług nr 2/2018 (131), t. 1, DOI: 10.18276/EPU.2018.131/1, s. 331-332.
[111] *Słownik terminów z zakresu bezpieczeństwa…*, op. cit., s. 24.
[112] J. Stanik, M. Kiedrowicz, *Model systemu zarządzania…*, op. cit., s. 332.

Lp.	Autor	Definicja
3.	P. Bączek[113]	Rozumiane jest jako stan wolny od zagrożeń przekazywania informacji nieuprawnionym podmiotom, szpiegostwa, działalności dywersyjnej lub sabotażowej, Każde działanie, system bądź metoda, które zmierzają do zabezpieczenia zasobów informacyjnych gromadzonych, przetwarzanych, przekazywanych, przechowywanych w pamięci komputerów oraz sieci teleinformatycznych,
4.	J. Łuczak[114]	Składowa bezpieczeństwa fizycznego, prawnego, osobowo-organizacyjnego oraz teleinformatycznego organizacji,
5.	E. Szczepaniuk[115]	Stan, w którym elementy tworzące system bezpieczeństwa cechuje zdolność do ochrony przed obecnymi i przyszłymi zakłóceniami lub utraty określonych wartości. Osiągane i utrzymywane na założonym poziomie poufności, integralności i dostępności oraz niezawodności i integralności usług. Zapewniona jest autentyczność i rozliczalność podmiotów. Użytkownicy informacji i usług oraz odbiorcy informacji i usług mają świadomość i nie są podatni na zagrożenia bezpieczeństwa informacyjnego. Aktorzy zagrożeń mają małe możliwości wykorzystania systemów teleinformatycznych do generowania zagrożeń,
6.	P. Potejko[116]	Zbiór działań, metod, procedur podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem,
7.	A. Żebrowski[117]	Zagwarantowania przez dany podmiot integralności, kompletności oraz wiarygodności posiadanych zasobów informacyjnych w każdej formie, nie tylko elektronicznej. Odnosi się więc zarówno do wszelkiego rodzaju wysiłków, służących ochronie posiadanych informacji, istotnych w kontekście bezpieczeństwa (a więc mających wpływ na sprawne funkcjonowanie struktur państwowych i społeczeństwa), jak i zapewnieniu przewagi informacyjnej przez zdobywanie nowych

[113] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2015, s. 71.
[114] J. Łuczak (red.), *Zarządzanie bezpieczeństwem informacji*, Wydawnictwo „Oficyna Współczesna", Poznań 2004, s. 80.
[115] E. Szczepaniuk, *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa*, rozprawa doktorska, AON, Warszawa 2015 za J. Werner, E. Szczepaniuk, *Bezpieczeństwo informacyjne organizacji*, Zeszyty Naukowe AON nr 4 (105) 2016, s. 170.
[116] P. Potejko, *Bezpieczeństwo informacyjne*, W: *Bezpieczeństwo państwa: wybrane problemy* (red.) K. A. Wojtaszczyk, A. Materska-Sosnowska, Oficyna Wydawnicza Aspra, Warszawa 2009, s. 194.
[117] A. Żebrowski, *Bezpieczeństwo informacyjne Polski a walka informacyjna*, Roczniki Kolegium Analiz Ekonomicznych nr 29/2013, s. 452.

Lp.	Autor	Definicja
		lub bardziej aktualnych danych oraz akcje dezinformacyjne wobec ewentualnych przeciwników.

Źródło: K. Kozłowski, Technological Advancements…, op. cit., s. 6-7.

Porównując przedstawione definicje terminu „bezpieczeństwo informacyjne", można zauważyć kilka kluczowych aspektów wspólnych dla wszystkich opisów. Przede wszystkim, bezpieczeństwo informacyjne jest przedstawiane jako kompleksowe działanie, które obejmuje wszystkie etapy życia informacji: od ich wytwarzania, przez przetwarzanie i przechowywanie, aż po przesyłanie. Centralnym celem tych działań jest ochrona przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem oraz innymi formami ingerencji w dane, informacje i systemy informacyjne.

W przytoczonych definicjach wyraźnie pojawia się motyw integralności, poufności oraz dostępności zasobów informacyjnych jako kluczowych wartości, które bezpieczeństwo informacyjne ma za zadanie chronić. Ponadto, bezpieczeństwo informacyjne jest postrzegane nie tylko w kontekście ochrony przed zagrożeniami zewnętrznymi, takimi jak szpiegostwo czy działalność dywersyjna, ale także w aspekcie zapewnienia niezawodności i integralności usług oraz autentyczności i rozliczalności podmiotów.

Oprócz aspektów technicznych i operacyjnych, w definicjach pojawia się również wymiar organizacyjny i prawny, podkreślający rolę procedur, metod i działań podejmowanych przez uprawnione podmioty w celu ochrony informacji. Znaczenie ma także świadomość użytkowników i odbiorców informacji o potencjalnych zagrożeniach oraz ich zdolność do przeciwdziałania tym zagrożeniom.

Na podstawie powyższej analizy, można zaproponować następującą definicję terminu **bezpieczeństwo informacyjne –** zintegrowany system działań, metod, procedur i środków technicznych, organizacyjnych oraz prawnych, mający na celu ochronę informacji na wszystkich etapach ich cyklu życia – od generowania przez przechowywanie, przetwarzanie, do przekazywania. Jego podstawowe cele to zapewnienie poufności, integralności oraz dostępności zasobów informacyjnych, ochrona przed wszelkimi formami nieuprawnionej ingerencji, w tym dostępem, ujawnieniem, modyfikacją, zniszczeniem czy szpiegostwem. Obejmuje to także utrzymanie niezawodności i integralności usług, zapewnienie autentyczności i rozliczalności podmiotów działających w systemie oraz promowanie świadomości i odporności na zagrożenia wśród użytkowników i odbiorców informacji. W efekcie, bezpieczeństwo informacyjne wspiera ciągłość działania organizacji, chroniąc jej zasoby

informacyjne przed obecnymi i przyszłymi zagrożeniami, przyczyniając się do utrzymania jej stabilności, reputacji i przewagi informacyjnej.

W niniejszym podrozdziale dokonano analizy pojęcia bezpieczeństwa informacji w kontekście nowoczesnych wyzwań technologicznych i organizacyjnych. W rozważaniach podkreślono, iż w erze cyfrowej informacje stały się kluczowym zasobem, który wymaga ochrony przed zagrożeniami zarówno zewnętrznymi, jak i wewnętrznymi. Wskazano na różnorodne zagrożenia, takie jak nieuprawniony dostęp, wycieki danych czy celowe ingerencje, które mogą poważnie wpłynąć na stabilność organizacji. Zabezpieczenie zasobów informacyjnych, zwłaszcza tych o strategicznym znaczeniu, wymaga zastosowania kompleksowego podejścia, obejmującego zarówno środki techniczne, organizacyjne, jak i prawne.

Autor przedstawił przegląd definicji bezpieczeństwa informacyjnego, który wskazuje na trzy kluczowe cele: zapewnienie poufności, integralności i dostępności informacji. Zwrócono również uwagę na konieczność holistycznego podejścia do ochrony informacji, które uwzględnia zabezpieczenie danych niezależnie od ich formy oraz zapewnienie ciągłości działania organizacji. Definicje podkreślają także istotność wprowadzania procedur oraz metod przeciwdziałania zagrożeniom i budowania świadomości wśród użytkowników, co wzmacnia ogólną odporność organizacji na potencjalne ataki.

W odniesieniu do hipotezy szczegółowej: *stosowanie odpowiednich standardów i norm w zarządzaniu bezpieczeństwem informacji, pozwala na skuteczne rozpoznawanie zagrożeń, kształtując poziom ochrony danych oraz tajemnicy przedsiębiorstwa*, podrozdział potwierdza następujące elementy:

a) stosowanie odpowiednich standardów i norm – autor wskazuje na potrzebę wprowadzania zróżnicowanych norm i procedur, które są niezbędne do zbudowania kompleksowego systemu ochrony danych i zapewnienia ich bezpieczeństwa. Wskazane definicje podkreślają konieczność systematycznego zarządzania ryzykiem oraz tworzenia procedur zapobiegawczych,
b) skuteczne rozpoznawanie zagrożeń – podkreślono istotę identyfikacji i klasyfikacji potencjalnych zagrożeń oraz ich systematyczną analizę, co jest kluczowe dla skutecznego zarządzania ryzykiem. Podkreślono, że ochrona informacji wymaga aktywnej identyfikacji zagrożeń, które mogą wpływać na integralność, poufność i dostępność danych,
c) kształtowanie poziomu ochrony danych i tajemnicy przedsiębiorstwa – przedstawione definicje bezpieczeństwa informacji wyraźnie wskazują na potrzebę wdrażania procedur i technologii chroniących kluczowe dane przed nieuprawnionym dostępem,

wyciekiem czy uszkodzeniem. Przestrzeganie norm wpływa na stabilność i zaufanie wobec organizacji.

Podsumowując, podrozdział, w sposób częściowy, potwierdza hipotezę, wskazując, że stosowanie standardów i norm w zarządzaniu bezpieczeństwem informacji umożliwia skuteczne rozpoznawanie zagrożeń i kształtowanie ochrony danych, co jest kluczowe dla ochrony tajemnicy przedsiębiorstwa.

2.2 Koncepcje zarządzania poufnością informacji: wyzwania implementacyjne i znaczenie dla organizacji

Przy implementacji standardów i procedur dotyczących bezpieczeństwa informacji, wiele organizacji często nie jest świadomych bogactwa obowiązujących regulacji prawnych dotyczących tej materii. Istnieje wiele przepisów regulujących bezpieczeństwo informacji, co umożliwia ich klasyfikację według określonych kryteriów[118]. Na potrzeby niniejszej dysertacji, autor skorzystał z podsumowania norm i standardów dokonanego przez Krzysztofa Bobkowskiego. Na podstawie przytoczonego opracowania, w związku z istnieniem szerokiego wachlarza aktów normatywnych w zakresie bezpieczeństwa informacji, można dokonać ich podziału w następujący sposób[119]:

a) normy słownikowe:
    a. ISO / IEC 27000:2018 – System Zarządzania Bezpieczeństwem Informacji – Przegląd i terminologia.
b) normy zawierające wymagania:
    a. ISO / IEC 27001:2022 – System Zarządzania Bezpieczeństwem Informacji – Wymagania,
    b. ISO / IEC 27006:2015 – Wymagania dla jednostek prowadzących audyt i certyfikację Systemów Zarządzania Bezpieczeństwem Informacji,
    c. ISO / IEC 27009:2016 – Zastosowania sektorowe ISO / IEC 27001 – Wymagania[120].
c) normy zawierające wytyczne:

[118] G. Culot, G. Nassimbeni, M. Podrecca, M. Sartor, *The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda*, The TQM Journal Volume 33 Issue 7 (2021), s. 77 i 79.
[119] K. Bobkowski, *Zarządzanie bezpieczeństwem informacji w ujęciu wybranych aktów normatywnych w zakresie Systemu Zarządzania Bezpieczeństwem Informacji*, Zarządzanie i Finanse Journal of Management and Finance Vol. 16, No. 3/2/2018, s. 20-23.
[120] ISO / IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*, ISO, Geneva 2018, s. 19-20 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.

a. ISO / IEC 27002:2013 – Praktyczne zasady zabezpieczenia informacji,
b. ISO / IEC 27003:2017 – Systemy zarządzania bezpieczeństwem informacji – Wytyczne,
c. ISO / IEC 27004:2016 – Zarządzanie bezpieczeństwem informacji – Monitorowanie, pomiar, analiza i ocena,
d. ISO / IEC 27005:2018 – Zarządzanie ryzykiem w zakresie bezpieczeństwa informacji,
e. ISO / IEC 27007:2017 – Wytyczne dotyczące audytu Systemów Zarządzania Bezpieczeństwem Informacji,
f. ISO / IEC TR 27008:2011 – Wytyczne dla audytorów dotyczące zarządzania bezpieczeństwa informacji,
g. ISO / IEC 27013:2015 – Wytyczne do zintegrowanego wdrożenia ISO / IEC 27001 oraz ISO / IEC 20000-1,
h. ISO / IEC 27014:2013 –Zarządzanie bezpieczeństwem informacji – ład organizacyjny,
i. ISO / IEC TR 27016:2014 – Zarządzanie bezpieczeństwem informacji – Ekonomika organizacji,
j. ISO / IEC 27021: 2017 – Wymagania kompetencyjne dla specjalistów Systemów Zarządzania Bezpieczeństwem Informacji[121].

d) normy zawierające wytyczne dla specyficznych, określonych sektorów:
   a. ISO / IEC 27010:2015 – Zarządzanie bezpieczeństwem informacji w komunikacji międzysektorowej i międzyorganizacyjnej,
   b. ISO / IEC 27011:2016 – Zasady postępowania w zakresie zarządzania bezpieczeństwem informacji w oparciu o ISO / IEC 27002 dla organizacji telekomunikacyjnych,
   c. ISO / IEC 27017:2015 – Praktyczne zasady zabezpieczenia informacji na podstawie ISO / IEC 27002 dla usług w chmurze,
   d. ISO / IEC 27018:2014 – Praktyczne zasady ochrony danych identyfikujących osobę (PII) w chmurach publicznych działających jako przetwarzający PII,
   e. ISO / IEC 27019:2017 – Zarządzanie bezpieczeństwem informacji w przemyśle energetycznym,

[121] ISO / IEC 27000:2018, *Information technology…,* op. cit., s. 20-23 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.

f. ISO 27799:2016 – Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO / IEC 27002[122].

e) normy zawierające specyficzne zabezpieczenia:
   a. ISO / IEC 27031:2011 – zawiera wytyczne w zakresie gotowości technologii informacyjnej i komunikacyjnej do zapewnienia ciągłości działania[123],
   b. ISO / IEC 27032:2012 – zawiera wytyczne w zakresie poprawy stanu cyberbezpieczeństwa[124],
   c. ISO / IEC 27033 – (od 1 do 6) – zawiera wytyczne w zakresie bezpieczeństwa sieci[125],
   d. ISO / IEC 27034 – (od 1 do 7) – zawiera wytyczne w zakresie bezpieczeństwa aplikacji[126],
   e. ISO / IEC 27035 – (od 1 do 2) – zawiera wytyczne w zakresie postępowania z incydentem bezpieczeństwa informacji[127],
   f. ISO / IEC 27036 – (od 1 do 4) – zawiera wytyczne w zakresie bezpieczeństwa informacji w relacjach z dostawcami[128],
   g. ISO / IEC 27037:2012 – zawiera wytyczne dotyczące identyfikacji, gromadzenia, nabywania i przechowywania dowodów cyfrowych[129],
   h. ISO / IEC 27038:2014 – określa cechy technik wykonywania cyfrowej redakcji na dokumentach cyfrowych[130],

[122] Ibidem, s. 23-25.
[123] ISO / IEC 27031:2011, *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*, ISO, Geneva 2011, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.
[124] ISO / IEC 27032:2012, *Information technology – Security techniques – Guidelines for cybersecurity*, ISO, Geneva 2012, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.
[125] ISO / IEC 27033-1:2015, *Information technology – Security techniques – Network secu- rity – Part 1: Overview and concepts*, ISO, Geneva 2015, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.
[126] ISO / IEC 27034-1:2011, *Information technology – Security techniques – Application security – Part 1: Overview and concepts*, ISO, Geneva 2011, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.
[127] ISO / IEC 27035-1:2016, *Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management*, ISO, Geneva 2016, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.
[128] ISO / IEC 27036-1:2014, *Information technology – Security techniques – Information secu- rity for supplier relationships – Part 1: Overview and concepts*, ISO, Geneva 2014, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.
[129] ISO / IEC 27037:2012, *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*, ISO, Geneva 2012, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.
[130] ISO / IEC 27038:2014, *Information technology – Security techniques – Specification for digital redaction*, ISO, Geneva 2014, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.

i. ISO / IEC 27039:2015 – zawiera wytyczne pomagające organizacjom przygotować się do wdrożenia systemów wykrywania i zapobiegania włamaniom (IDPS)[131],

j. ISO / IEC 27040:2015 – dostarcza szczegółowych wskazówek technicznych, w jaki sposób organizacje mogą zdefiniować odpowiedni poziom ograniczenia ryzyka, stosując sprawdzone i spójne podejście do planowania, projektowania, dokumentacji i wdrażania zabezpieczeń przechowywania danych[132],

k. ISO / IEC 27041:2015 – zawiera wytyczne w zakresie mechanizmów zapewniających, że metody i procesy stosowane w dochodzeniach dotyczących incydentów związanych z bezpieczeństwem informacji są „odpowiednie do celu"[133],

l. ISO / IEC 27042:2015 – zawiera wytyczne dotyczące analizy i interpretacji dowodów cyfrowych w sposób odnoszący się do kwestii ciągłości, ważności, odtwarzalności i powtarzalności[134],

m. ISO / IEC 27043:2015 – zawiera wytyczne oparte na wyidealizowanych modelach dla wspólnych procesów dochodzeniowych incydentów w różnych scenariuszach dochodzeniowych, w których biorą udział dowody cyfrowe[135],

n. ISO / IEC 27050 – (od 1 do 3) – zawiera wytyczne i wskazówki dotyczące działań związanych z elektronicznym wykrywaniem, w tym między innymi identyfikację, przechowywanie, gromadzenie, przetwarzanie, przegląd, analizę i produkcję informacji przechowywanych elektronicznie (*electronically stored information* – ESI)[136],

o. ISO / IEC 29101:2013 – zawiera wytyczne architektury prywatności, która określa podatności dotyczące systemów technologii informacyjnych

[131] ISO / IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*, ISO, Geneva 2015, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.
[132] ISO / IEC 27040:2015, *Information technology – Security techniques – Storage security*, ISO, Geneva 2015, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.
[133] ISO / IEC 27041:2015, *Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method*, ISO, Geneva 2015, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.
[134] ISO / IEC 27042:2015, *Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*, ISO, Geneva 2015, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.
[135] ISO / IEC 27043:2015, *Information technology – Security techniques – Incident investigation principles and processes*, ISO, Geneva 2015, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.
[136] ISO / IEC 27050-1:2016, *Information technology – Security techniques – Electronic discovery – Part 1: Overview and concepts*, ISO, Geneva 2016, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.

i komunikacyjnych (TIK), które przetwarzają informacje umożliwiające identyfikację osób (PII)[137].

Nie jest trudno zauważyć, iż normy przewidziane do zapewnienia bezpieczeństwa informacji w organizacji zostały przygotowanie niemalże dla każdego sektora działalności przedsiębiorstwa oraz dla niemalże każdej dziedziny ochrony informacji przetwarzanych, wykorzystywanych, gromadzonych i udostępnianych przez organizację[138]. Implementacja wskazanych norm nie gwarantuje zapewnienia stuprocentowego bezpieczeństwa, jednak w znacznym stopniu może wpłynąć na zapewnienie jego wysokiego poziomu.

W ramach realizacji zadań związanych z ochroną informacji na poziomie państwowym jak również na poziomie bezpieczeństwa organizacji, niezwykle istotną rolę odgrywają przepisy zawarte w kluczowych aktach prawnych, takich jak ustawa o ochronie informacji niejawnych, ustawa o ochronie danych osobowych, ustawa Prawo telekomunikacyjne oraz ustawa o świadczeniu usług drogą elektroniczną. Wskazane regulacje prawne stanowią fundament systemu ochrony informacji, zarówno w kontekście bezpieczeństwa, jak i prywatności jednostek.

Ustawa o ochronie informacji niejawnych koncentruje się na zasadach klasyfikacji, przetwarzania oraz zabezpieczania informacji, które z różnych względów wymagają ograniczonego dostępu, by zapewnić bezpieczeństwo państwa i jego obywateli. Z kolei ustawa o ochronie danych osobowych skupia się na regulowaniu sposobów przetwarzania danych osobowych, zapewniając ochronę prywatności oraz autonomię personalną wobec rosnącej cyfryzacji życia społecznego. Prawo telekomunikacyjne natomiast, adresuje kwestie związane z infrastrukturą i usługami telekomunikacyjnymi, ustanawiając ramy prawne dla bezpiecznej komunikacji elektronicznej, co bezpośrednio wpływa na ochronę przesyłanych informacji. Natomiast ustawa o świadczeniu usług drogą elektroniczną reguluje *obowiązki usługodawcy związane ze świadczeniem usług drogą elektroniczną, zasady wyłączania odpowiedzialności usługodawcy z tytułu świadczenia usług drogą elektroniczną oraz zasady ochrony danych osobowych osób fizycznych korzystających z usług świadczonych drogą elektroniczną*[139].

Wspólnym celem wskazanych ustaw jest nie tylko ochrona różnych aspektów bezpieczeństwa informacyjnego, ale także wyważenie interesów państwa, społeczeństwa oraz jednostek, w świetle dynamicznie rozwijających się technologii informacyjno-komunikacyjnych.

---

[137] ISO / IEC 29101:2013, *Information technology – Security techniques – Privacy architecture framework*, ISO, Geneva 2013, s. 1 za K. Bobkowski, *Zarządzanie bezpieczeństwem informacji…*, op. cit.

[138] A. Kasprzak, *System zarządzania bezpieczeństwem informacji*, LexDigital, https://lexdigital.pl/system-zarzadzania-bezpieczenstwem-informacji [dostęp 10.09.2024 r.].

[139] Ustawa z dnia 18 lipca 2002 r. *o świadczeniu usług drogą elektroniczną* (Dz.U.2020.0.344, t.j.), Art. 1.

Ustawa z dnia 5 kwietnia 2010 r. o ochronie informacji niejawnych stanowi kluczowe ramy prawne dla bezpieczeństwa informacyjnego w Polsce. Jej główne założenia koncentrują się na zapewnieniu skutecznej ochrony informacji niejawnych, które ze względu na swoje znaczenie dla bezpieczeństwa państwa, wymagają specjalnych środków ochrony. Ustawa definiuje informacje niejawne jako *informacje których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania*[140]. Zgodnie z zapisami ustawy, przepisy mają zastosowanie do:

a) organów władzy publicznej, w szczególności:
    a. Sejmu i Senatu,
    b. Prezydenta Rzeczypospolitej Polskiej,
    c. organów administracji rządowej,
    d. organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych,
    e. sądów i trybunałów,
    f. organów kontroli państwowej i ochrony prawa.
b) jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych,
c) Narodowego Banku Polskiego,
d) państwowych osób prawnych i innych niż wymienione w pkt 1–3 państwowych jednostek organizacyjnych,
e) jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy,
f) przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych[141].

Następnie, na podstawie przyjętego kryterium szkodliwości ujawnienia, klasyfikuje je według stopni tajności co zostało przedstawione w tabeli nr 6.

Tabela 6 Klasyfikowanie informacji niejawnych

[140] Ustawa z dnia 5 kwietnia 2010 r. *o ochronie informacji niejawnych* (Dz. U. 2010 Nr 182 poz. 1228, t. j.), Art. 1 ust. 1.
[141] Ibidem, art. 1 ust. 2.

Lp.	Kategoria klasyfikacyjna	Opis
1.	Ściśle tajne	Informacjom niejawnym nadaje się klauzulę *ściśle tajne*, jeżeli ich nieuprawnione ujawnienie **spowoduje wyjątkowo poważną** szkodę dla Rzeczypospolitej Polskiej
2.	Tajne	Informacjom niejawnym nadaje się klauzulę *tajne*, jeżeli ich nieuprawnione ujawnienie **spowoduje poważną** szkodę dla Rzeczypospolitej Polskiej
3.	Poufne	Informacjom niejawnym nadaje się klauzulę *poufne*, jeżeli ich nieuprawnione ujawnienie **spowoduje szkodę** dla Rzeczypospolitej Polskiej
4.	Zastrzeżone	Informacjom niejawnym nadaje się klauzulę *zastrzeżone*, jeżeli **nie nadano im wyższej** klauzuli tajności, a ich **nieuprawnione ujawnienie może mieć szkodliwy wpływ** na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

Źródło: opracowanie własne na podstawie Ustawy z dnia 5 kwietnia 2010 r. o ochronie informacji…, op. cit., Art. 5.

Ponadto, określa zasady ich oznaczania, przetwarzania, przechowywania, a także przekazywania wewnątrz kraju i za granicę[142]. Podkreśla również obowiązki podmiotów zobowiązanych do ochrony takich informacji, w tym instytucji państwowych, przedsiębiorstw oraz indywidualnych pracowników, nakładając na nich odpowiedzialność za wdrożenie odpowiednich procedur i systemów zabezpieczających[143]. Ponadto, ustawa reguluje proces certyfikacji osób i jednostek organizacyjnych do dostępu do informacji niejawnych oraz wprowadza system kontroli i nadzoru nad przestrzeganiem przepisów ochrony informacji niejawnych, w tym sankcje za ich naruszenie[144]. W przypadku przedsiębiorcy, realizującego zadania związane z wykorzystaniem i przetwarzaniem informacji niejawnych, ustawa reguluje tryb obiegu wskazanych informacji w ramach pojęcia bezpieczeństwa przemysłowego, czyli potwierdzenia, poprzez uzyskanie przez przedsiębiorcę stosownego certyfikatu, *zdolności do ochrony informacji niejawnych o klauzuli poufne lub wyższej*[145]. W ramach certyfikacji, przedsiębiorca może uzyskać jedno ze świadectw, których klasyfikacja została przedstawiona w tabeli nr 7.

[142] Ibidem, Art. 6-9.
[143] Ibidem, Art. 13-17, Art. 19-20, Art. 21-34, Art. 48-53.
[144] Ibidem, Art. 42-47.
[145] Ibidem, Art. 54 ust. 2.

Tabela 7 Klasyfikacja świadectw bezpieczeństwa przemysłowego

Lp.	Kategoria klasyfikacyjna	Opis
1.	I stopień	Potwierdza pełną zdolność przedsiębiorcy do ochrony tych informacji,
2.	II stopień	Potwierdza zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych,
3.	III stopień	Potwierdza zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach

Źródło: opracowanie własne na podstawie Ustawy z dnia 5 kwietnia 2010 r. o ochronie informacji…, op. cit., Art. 55 ust. 1.

W kontekście dynamicznie rozwijającego się środowiska biznesowego, zarządzanie danymi osobowymi staje się kluczowym wyzwaniem dla przedsiębiorstw. Wymóg zapewnienia ochrony danych osobowych wynika nie tylko z etycznych standardów profesjonalizmu, ale również z rygorystycznych przepisów prawnych. Niniejszy artykuł ma na celu zgłębienie definicji danych osobowych, zbadanie obowiązków prawnych ciążących na przedsiębiorcach w kontekście zarządzania tymi danymi oraz zarysowanie implikacji tych wymogów dla praktyk biznesowych.

Zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, dane osobowe definiowane są jako *wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej*[146]. Tożsamość osoby może być określona bezpośrednio lub pośrednio, przy użyciu różnorodnych czynników, takich jak identyfikatory numeryczne (np. numer PESEL[147]) czy cechy fizyczne. Istotne jest, że definicja ta ma charakter otwarty, co oznacza, że zakres danych osobowych jest elastyczny i może obejmować różnorodne typy informacji, w zależności od kontekstu ich przetwarzania[148].

Wprowadzenie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, znanego jako RODO, znacząco wpłynęło na praktyki zarządzania danymi osobowymi w przedsiębiorstwach. Wprowadzenie wskazanego rozporządzenia wymusiło na polskim ustawodawcy aktualizacji przepisów ustawy o ochronie danych i implementacje przepisów

[146] Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz.U. 1997 Nr 133 poz. 883, t. j., akt utracił moc), Art. 6.
[147] Ustawa z dnia 24 września 2010 r. *o ewidencji ludności* (Dz. U. 2010 Nr 217 poz. 1427, t. j.), Art. 15.
[148] K. Gazda, *Które informacje stanowią dane osobowe w świetle RODO?*, Poradnik Przedsiębiorcy, https://poradnikprzedsiebiorcy.pl/-ktore-informacje-stanowia-dane-osobowe-w-swietle-rodo [dostęp 20.02.2024 r.].

europejskich do polskiego porządku prawnego w formie nowej ustawy o ochronie danych osobowych[149].

RODO rozszerza definicję danych osobowych, podkreślając, że możliwa do zidentyfikowania osoba fizyczna to taka, którą można zidentyfikować bezpośrednio lub pośrednio na podstawie szerokiego zakresu identyfikatorów. Rozporządzenie to nakłada na przedsiębiorstwa szereg obowiązków, w tym konieczność implementacji odpowiednich środków technicznych i organizacyjnych mających na celu ochronę danych osobowych.[150]

Zarządzanie danymi osobowymi w świetle obowiązujących przepisów prawnych wymaga od przedsiębiorstw nie tylko zrozumienia definicji i zakresu danych osobowych, ale również wdrożenia skutecznych mechanizmów ich ochrony. Przedsiębiorca, jako administrator danych, musi zapewnić, że przetwarzanie danych osobowych odbywa się zgodnie z zasadami określonymi w RODO, co obejmuje m.in. zasadę legalności, uczciwości, transparentności, ograniczenia celu, minimalizacji danych, dokładności, ograniczenia przechowywania, integralności, poufności oraz odpowiedzialności[151].

W dobie cyfryzacji i globalizacji gospodarki, ochrona danych osobowych staje się nie tylko obowiązkiem prawnym, ale również elementem budującym zaufanie klientów i konkurencyjność przedsiębiorstw[152]. Zrozumienie definicji danych osobowych oraz świadome zarządzanie nimi, zgodnie z obowiązującymi regulacjami prawnymi, jest kluczowe dla zapewnienia ich ochrony oraz minimalizacji ryzyka naruszeń danych[153]. Wymaga to jednak od przedsiębiorców nieustannej wiedzy na temat aktualnych wymogów prawnych oraz implementacji skutecznych strategii zarządzania danymi osobowymi, co stanowi wyzwanie w dynamicznie zmieniającym się środowisku biznesowym.

Kolejnym aktem prawnym, który reguluje zakres funkcjonowania przedsiębiorcy realizującego usługi telekomunikacyjne w kwestii ich gromadzenia, przetwarzania i przekazywania instytucjom uprawnionym jest Prawo telekomunikacyjne. Zgodnie z treścią art. 180a ust. 1 pkt 1 na operatorze publicznej sieci telekomunikacyjnej oraz dostawcy publicznie dostępnych usług telekomunikacyjnych spoczywa obowiązek zatrzymywania i przechowywania na własny koszt danych generowanych w sieci telekomunikacyjnej lub przez

[149] Ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych* (Dz. U. 2018 poz. 1000, t. j.), Art. 1.
[150] Rozporządzenie Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*.
[151] K. Gazda, *Które informacje stanowią…,* op. cit.
[152] A. Tomczak, E. Dostatni, F. Górski, *Narzędzie informatyczne wspomagające zarządzanie danymi klientów*, Zarządzanie Przedsiębiorstwem 2023 Vol. 26 No. 1, DOI: 10.25961/ent.manag.26.02.04, s. 26 i 28.
[153] N. Zacharska, *Jak budować zaufanie klientów poprzez transparentność w zakresie ochrony danych osobowych?*, iSecure, https://www.isecure.pl/blog/jak-budowac-zaufanie-klientow-poprzez-transparentnosc-w-zakresie-ochrony-danych-osobowych/? [dostęp 18.11.2024 r.].

nią przetwarzanych, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te zniszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi[154]. Ponadto, operator oraz dostawca wskazanych usług zobowiązani są do udostępnienia gromadzonych danych uprawnionym podmiotom, a także sądowi i prokuratorowi, na zasadach i w trybie określonych w odrębnych przepisach[155].

Wobec powyższego, pojawia się pytanie – jaki zakres danych jest gromadzony przez operatora i dostawcę? Zgodnie z zapisem art. 180c, ustawodawca narzucił na operatora i dostawcę obowiązek gromadzenia i udostępniania następujących danych, niezbędnych do:

a) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:
b) inicjującego połączenie,
c) do którego kierowane jest połączenie;
d) określenia:
e) daty i godziny połączenia oraz czasu jego trwania,
f) rodzaju połączenia,
g) lokalizacji telekomunikacyjnego urządzenia końcowego[156].

Wobec powyższego uprawnione służby i instytucje mają możliwość, w oparciu o powyższe zapisy ustawowe, oraz na podstawie rozporządzenia określonego w art. 180c ust. 2, na ustalenie i uzyskanie danych dotyczących:

a) urządzenia inicjującego połączenie i urządzenia, do którego kierowane jest połączenie,
b) daty, godziny i czasu połączenia z dokładnością do 1 sekundy oraz jego rodzaju,
c) lokalizację telekomunikacyjnego urządzenia końcowego,
d) imię i nazwisko lub nazwę i adres abonenta, któremu przydzielono dany numer telefonii stacjonarnej lub MSISDN (Mobile Subscriber Integrated Services Digital Network - numer przydzielony użytkownikowi końcowemu ruchomej publicznej sieci telefonicznej),
e) pierwsze 14 cyfr numeru IMEI (International Mobile Equipment Identity) — indywidualny międzynarodowy numer identyfikujący telekomunikacyjne urządzenie końcowe, używane w ruchomej publicznej sieci telefonicznej) lub numer ESN (Electronic Serial Number) — indywidualny numer identyfikujący telekomunikacyjne

[154] Ustawa z dnia 16 lipca 2004 r. – *Prawo telekomunikacyjne* (Dz. U. 2022, poz. 1648, t. j.), art. 180a ust. 1 pkt 1.
[155] Ibidem, Art. 180a ust. 1 pkt 2.
[156] Ibidem, Art. 180c ust. 1.

urządzenie końcowe, używane w ruchomej publicznej sieci telefonicznej wykorzystującej technologii CDMA (Code Division Multiple Access),

f) datę i godzinę pierwszego zalogowania telekomunikacyjnego urządzenia końcowego do ruchomej, publicznej sieci telekomunikacyjnej, zgodnie z czasem lokalnym,
g) współrzędne geograficzne lokalizacji stacji BTS (Base Transceiver Station) — urządzenie umożliwiające połączenie telekomunikacyjnego urządzenia końcowego, używanego w ruchomej publicznej sieci telefonicznej z częścią stałą tej sieci) poprzez którą dokonano tego połączenia zgodnie z czasem lokalnym,
h) analogiczne dane dotyczące użytkownika adresu IP pozwalające na jego identyfikację oraz identyfikację portu sieciowego i zakończenia sieci, daty i godziny połączenia, jak również daty i godziny zalogowania i wylogowania z usługi poczty elektronicznej i telefonii internetowej, zgodnie z czasem lokalnym,
i) raportów połączeń[157].

Ostatni z omawianych aktów prawnych regulujący świadczenie usług drogą elektroniczną wskazuje, iż przedsiębiorca może przetwarzać następujące informacje, stanowiące dane osobowe na potrzeby prowadzonej działalności gospodarczej:

a) nazwisko i imiona usługobiorcy,
b) numer ewidencyjny PESEL lub - gdy ten numer nie został nadany - numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość,
c) adres zameldowania na pobyt stały,
d) adres do korespondencji, jeżeli jest inny niż adres, o którym mowa w pkt c),
e) dane służące do weryfikacji podpisu elektronicznego usługobiorcy,
f) adresy elektroniczne usługobiorcy[158].

W ramach realizacji umów lub dokonywania innych czynności prawnych z usługobiorcą, usługodawca może przetwarzać dane niezbędne ze względu na charakter świadczonej usługi lub sposób jej rozliczenia. To podejście podkreśla zasadę minimalizacji danych, zgodnie z którą przetwarzanie powinno ograniczać się do informacji ściśle niezbędnych do wykonania określonej usługi. Zasada ta, będąca jednym z filarów RODO, ma na celu ochronę prywatności usługobiorców poprzez ograniczenie zakresu gromadzonych o nich informacji[159]. Usługodawcy, w celu zapewnienia transparentności procesów przetwarzania danych, są zobowiązani do wyróżnienia i oznaczenia danych, które są niezbędne

[157] Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. *w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania* (Dz.U. 2009 nr 226 poz. 1828), § 3.
[158] Ustawa z dnia 18 lipca 2002 r. *o świadczeniu usług drogą…,* op. cit., Art. 18 ust. 1.
[159] Ibidem, Art. 18 ust. 2.

do świadczenia usługi drogą elektroniczną. Taki wymóg pozwala usługobiorcom na świadome decydowanie o zakresie informacji, które udostępniają, co stanowi realizację zasady uczciwości i transparentności[160]. Zgodnie z zasadą celowości, usługodawca może przetwarzać dane usługobiorców, za ich zgodą, również w celach reklamy, badania rynku oraz analizy zachowań i preferencji, co ma na celu polepszenie jakości świadczonych usług. Takie działania, choć wykraczają poza bezpośrednią realizację umowy świadczenia usług, mogą przyczyniać się do zwiększenia satysfakcji klientów poprzez dostosowanie oferty do ich indywidualnych potrzeb i oczekiwań[161].

Usługodawca może również przetwarzać dane charakteryzujące sposób korzystania z usługi świadczonej drogą elektroniczną, takie jak oznaczenia identyfikujące usługobiorcę, informacje o czasie i zakresie korzystania z usługi czy dane dotyczące używanego systemu teleinformatycznego. Przetwarzanie tych danych, określanych jako dane eksploatacyjne, ma kluczowe znaczenie dla zapewnienia ciągłości i bezpieczeństwa świadczonych usług, a także dla diagnozowania i rozwiązywania problemów technicznych[162]. Ponadto, usługodawca nieodpłatnie udostępnia dane, o których mowa w ust. 1–5, organom państwa uprawnionym na podstawie odrębnych przepisów na potrzeby prowadzonych przez nie postępowań[163].
Dlatego biorąc pod uwagę powyższe, zasadnym jest dokonanie podsumowania dotyczącego informacji uzyskiwanych, gromadzonych, przetwarzanych i udostępnianych przez przedsiębiorcę świadczącego usługi teleinformatyczne. Podsumowanie zostało przedstawione w tabeli nr 8.

Tabela 8 Zarządzanie informacjami i danymi w przedsiębiorstwie

Podstawa prawna	Informacje	Dane	Dane osobowe
Ustawa o OIN	Informacje niejawne przetwarzane w ramach prowadzonej działalności gospodarczej oraz w ramach współpracy z instytucjami państwa,	Dane dotyczące formy przetwarzania, obiegu, gromadzenia i udostępniania informacji niejawnych instytucjom państwa lub podmiotom uprawnionym,	Dane osobowe funkcjonariuszy lub przedstawicieli instytucji państwa zwracających się z wnioskiem o udostępnienie informacji niejawnych, jak również osób odpowiedzialnych za współpracę z instytucjami

[160] Ibidem, Art. 18 ust. 3.
[161] Ibidem, Art. 18 ust 4.
[162] Ibidem, Art. 18 ust. 5.
[163] Ibidem, Art. 18 ust. 6.

Podstawa prawna	Informacje	Dane	Dane osobowe
			państwa z ramienia przedsiębiorcy
Ustawa o ODO	Informacje przetwarzane w ramach prowadzonej działalności gospodarczej dotyczące metod, form, środków i sposobów gromadzenia danych osobowych,	Dane dotyczące systemów gromadzenia danych prowadzonych przez przedsiębiorcę,	Dane osobowe klientów, pracowników, współpracowników oraz interesariuszy przedsiębiorstwa,
Ustawa – PT	Informacje na temat posiadanych systemów teleinformatycznych na potrzeby prowadzonej działalności gospodarczej oraz procesu ich eksploatacji i zabezpieczeń,	Dane gromadzone w dostępnych systemach monitorowania i eksploatacji urządzeń telekomunikacyjnych	Dane osobowe pozwalające na bezpośrednią identyfikację klientów usług telekomunikacyjnych oraz pracowników i współpracowników realizujących zadania w ramach prowadzonej działalności gospodarczej
Ustawa o ŚUDE	Informacje przetwarzane w ramach prowadzonej działalności gospodarczej dotyczące metod, form, środków i sposobów gromadzenia danych osobowych.	Dane gromadzone w dostępnych systemach dotyczące procesów sprzedażowych, ofertowych lub zapytań kierowanych przez potencjalnych usługobiorców.	Dane osobowe pozwalające na bezpośrednią identyfikację klientów lub potencjalnych usługobiorców oraz pracowników i współpracowników obsługujących procesy ofertowe i sprzedażowe.

Źródło: opracowanie własne.

W organizacjach, w zależności od ich charakteru oraz obowiązujących przepisów prawnych, dochodzi do przetwarzania różnorodnych zestawów danych. Specyfika i wymogi prawne, które kształtują działalność danej jednostki, mają bezpośredni wpływ na rodzaje gromadzonych zasobów informacyjnych. Naukowcy związani z Akademią Obrony Narodowej podkreślają, że polskie regulacje prawne identyfikują szereg kluczowych informacji, które podlegają ochronie prawnej, co ma istotne znaczenie dla atrybutów bezpieczeństwa informacji w kontekście działalności organizacyjnej. Ponadto, zgodnie z przeprowadzoną analizą, zwrócili uwagę na znaczącą liczbę aktów prawnych mających wpływ na bezpieczeństwo informacyjne

organizacji[164]. Szerokie spektrum, odmienne od przedstawionego przez autora, zostało zaprezentowane w tabeli nr 9.

Tabela 9 Wybrane rodzaje informacji prawnie chronionych a wymagania ich ochrony

Podstawa prawna	Zachowanie atrybutów bezpieczeństwa	Zabezpieczenie systemu teleinformatycznego	Dostęp osób do informacji
Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych	Poufność, integralność, dostępność	Trzy poziomy bezpieczeństwa: podstawowy, podwyższony i wysoki	Upoważnienie do przetwarzania danych: prowadzenie ewidencji osób upoważnionych, obowiązek zachowania tajemnicy danych i sposobów ich zabezpieczenia
Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych	Poufność (klauzule: zastrzeżone, poufne, tajne i ściśle tajne), integralność, dostępność	Wymagania w zależności od klauzuli niejawności	Poświadczenie bezpieczeństwa osobowego do dostępu do informacji o określonej klauzuli niejawności
Ustawa z 29 września 1994 r. o rachunkowości	Integralność, dostępność	Zabezpieczenie kopii danych przetwarzanych w systemie	Brak
Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi	Poufność (klauzula: informacje poufne), integralność, dostępność	Brak	Prowadzenie wykazu osób dopuszczonych do informacji poufnych, obowiązek zachowania poufności
Ustawa z dnia 8 września 2001 r. o dostępie do informacji publicznej	Integralność, dostępność	Wdrożenie modułu bezpieczeństwa – uniemożliwienie zniszczenia lub modyfikacji informacji oraz zablokowania dostępu	Uprawnienia dostępu do modułu administracyjnego BIP
Ustawa z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji	Poufność (warunek wskazania informacji), integralność, dostępność	Podjęcie działań zabezpieczających wybrane informacje	Dopuszczenie osób do wybranych informacji, zobowiązanie do zachowania poufności
Ustawa z 26 czerwca 1974 r. Kodeks pracy	Poufność (wskazanie informacji, których ujawnienie może narazić pracodawcę na szkodę), integralność, dostępność	Podjęcie działań zabezpieczających wybrane informacje	Zobowiązanie do zachowania poufności

Źródło: opracowanie własne na podstawie J. Werner, E. Szczepaniuk, Bezpieczeństwo informacyjne…, op. cit., s. 174.

[164] J. Werner, E. Szczepaniuk, *Bezpieczeństwo informacyjne…,* op. cit., s. 171.

W ramach zarządzania bezpieczeństwem informacyjnym kluczową rolę odgrywa adaptacja regulacji prawnych do dynamicznie ewoluującego kontekstu bezpieczeństwa cyfrowego, postępującej cyfryzacji sfery publicznej oraz kreowania zasad, które umożliwiają wdrożenie skutecznych mechanizmów ochrony danych. Efektywność systemu ochrony informacji w organizacji jest zatem uzależniona od formułowania adekwatnych norm prawnych, mających na celu usprawnienie działań w zakresie wspomnianego obszaru[165].

Polityka bezpieczeństwa w przedsiębiorstwie jest kluczowym składnikiem zarządzania ryzykiem oraz zapewnienia integralności danych. Jest to strategiczne narzędzie, które umożliwia organizacjom osiągnięcie ich celów strategicznych poprzez ochronę cennych danych i zasobów przed potencjalnymi zagrożeniami. Polityka ta, obejmująca szeroki zakres działań związanych z identyfikacją, oceną i ochroną, odgrywa centralną rolę w utrzymaniu operacyjności oraz pozytywnego wizerunku przedsiębiorstwa, a jednocześnie stanowi bazę do opracowania i wdrożenia akceptowalnych koncepcji bezpieczeństwa[166]. W dzisiejszym dynamicznie zmieniającym się świecie biznesowym, polityka bezpieczeństwa informacyjnego stanowi filar zarządzania ryzykiem i ochrony danych w organizacjach. Uznając jej znaczenie strategiczne, poniżej przytoczono wybrane definicje tego kluczowego elementu, podkreślając jego rolę w zapewnieniu ciągłości działania i budowaniu zaufania wśród interesariuszy:

a) **polityka bezpieczeństwa jako zbiór zasad**: polityka bezpieczeństwa definiowana jest jako zbiór formalnie zapisanych zasad i procedur, mających na celu ochronę informacji przed wszelkimi formami zagrożeń. Jest to zasadnicze narzędzie, które wzmacnia potencjał organizacji do realizacji jej misji i wizji, zapewniając bezpieczeństwo kluczowych danych i zasobów[167],
b) **polityka bezpieczeństwa jako strategia ochrony**: polityka ta jest strategią ochrony, obejmującą kompleksowe działania związane z ochroną danych osobowych oraz bezpieczeństwem operacji biznesowych. Strategia ta może przyjmować formę formalną, w postaci dokumentacji wewnętrznej lub nieformalną, manifestującą się w codziennych praktykach operacyjnych[168],
c) **polityka bezpieczeństwa jako narzędzie zarządzania ryzykiem**: polityka bezpieczeństwa jest również rozumiana jako integralna część zarządzania ryzykiem

[165] J. Werner, E. Szczepaniuk, *Bezpieczeństwo informacyjne…,* op. cit., s. 175.
[166] B. Ciecińska, J. Łunarski, R. Perłowski, D. Stadnicka, *Systemy zarządzania bezpieczeństwem w przedsiębiorstwie*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2006, s. 251.
[167] D. Mrowiec, *Polityka bezpieczeństwa – Czym jest i co decyduje o jej skuteczności?*, Bezpieczeństwo biznesu, https://bezpieczenstwobiznesu.com.pl/index.php/2018/09/09/polityka-bezpieczenstwa-cz-1-czym-jest-i-co-decyduje-o-jej-skutecznosci/ [dostęp: 20.02.2024 r.].
[168] K. Liderman, *Bezpieczeństwo informacyjne…,* op. cit., s. 173-174.

w organizacji, wymagająca zaangażowania na wszystkich poziomach organizacyjnych i ciągłego monitorowania, w celu adaptacji do zmieniających się warunków[169].

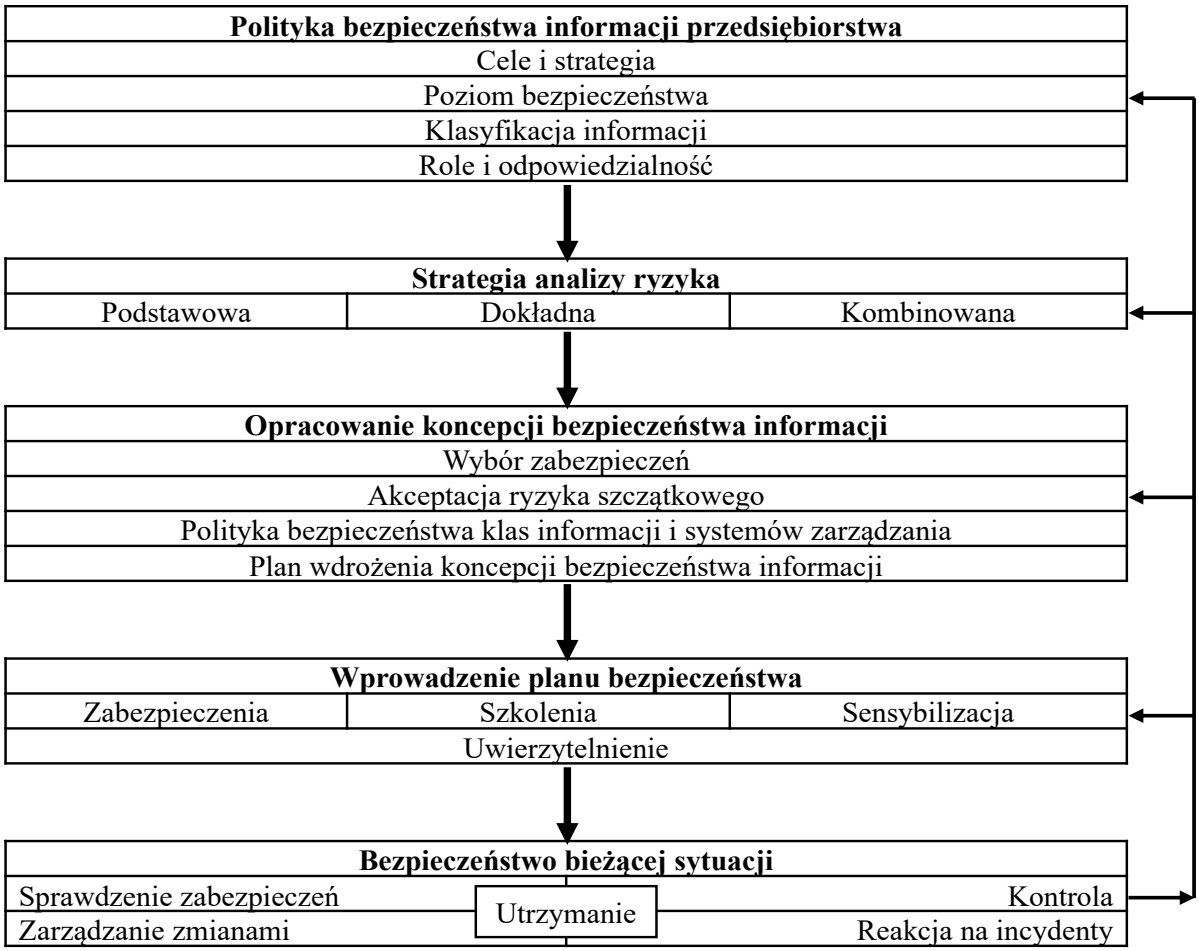
Wdrożenie i realizacja skutecznej polityki bezpieczeństwa jest niezbędna dla każdej organizacji pragnącej chronić swoje zasoby informacyjne i utrzymać wysoki poziom zaufania wśród klientów oraz partnerów biznesowych. Kluczowe elementy tej polityki obejmują:

a) **zaangażowanie kierownictwa**: kluczowym warunkiem efektywności polityki jest świadomość i wsparcie najwyższego kierownictwa w zakresie znaczenia bezpieczeństwa informacyjnego dla działalności biznesowej[170],
b) **zdefiniowane cele**: polityka powinna jasno określać cele ochrony informacji, które są zgodne z misją i celami strategicznymi organizacji[171],
c) **zasady i procedury**: musi zawierać zasady postępowania oraz procedury, które są stosowane w celu ochrony informacji, w tym zasady klasyfikacji danych, zasady dostępu, zarządzania ryzykiem, a także procedury reagowania na incydenty[172],
d) **analiza ryzyka**: wyciągnięcie wniosków z ostatniej lub dokonywanej okresowo analizy ryzyka, przygotowanie scenariuszy ryzyka uporządkowanych według jego wielkości[173],
e) **odpowiedzialność i obowiązki**: dokument określa role, obowiązki i zakresy odpowiedzialności wszystkich pracowników organizacji w procesie ochrony informacji[174],
f) **szkolenia i świadomość**: Polityka powinna przewidywać regularne szkolenia i działania na rzecz podnoszenia świadomości pracowników w zakresie bezpieczeństwa informacyjnego[175],
g) **monitoring i przegląd**: Polityka musi podlegać regularnemu monitorowaniu i przeglądom w celu aktualizacji i dostosowania do zmieniających się warunków[176],
h) **zgodność z przepisami prawnymi**: Musi być zgodna z obowiązującymi przepisami prawnymi, normami i standardami dotyczącymi ochrony informacji[177].

Utrzymanie adekwatnego poziomu zabezpieczenia danych wymaga nieustannej weryfikacji i dostosowywania do szybko zmieniających się warunków wewnętrznych oraz zewnętrznych organizacji. Aby zilustrować procesy zachodzące w analizie

[169] A. Woody, *Enterprise security…,* op. cit., s. 76-79.
[170] K. Liderman, *Bezpieczeństwo informacyjne…,* op. cit., s. 174.
[171] A. Woody, *Enterprise security…,* op. cit.
[172] K. Liderman, *Bezpieczeństwo informacyjne…,* op. cit., s. 175.
[173] A. Białas, *Bezpieczeństwo informacji…*, op. cit., s. 361.
[174] K. Liderman, *Bezpieczeństwo informacyjne…,* op. cit., s. 174-175.
[175] A. Woody, *Enterprise security…,* op. cit.,
[176] A. Białas, *Bezpieczeństwo informacji…*, op. cit.
[177] T. Polaczek, *Audyt bezpieczeństwa informacji w praktyce*, Wydawnictwo Helion, Gliwice 2006, s. 48-52.

ochrony informacji w kontekście polityki bezpieczeństwa organizacji, posłużono się odpowiednim schematem, przedstawionym na rysunku nr 10.



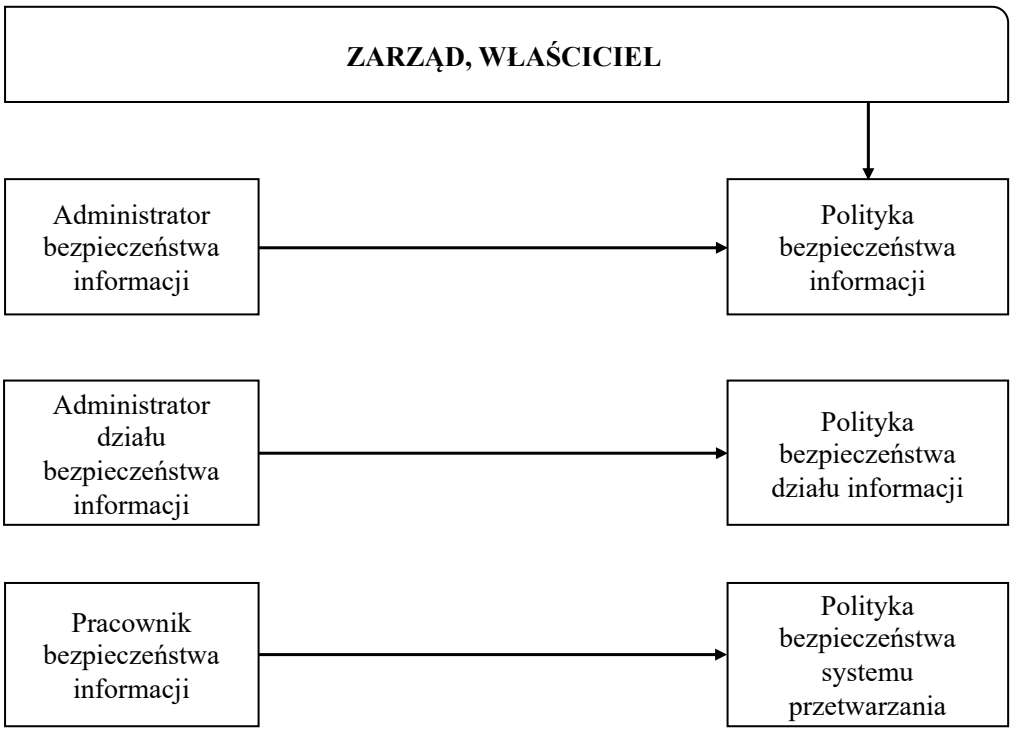
Rysunek 10 Procesy w zarządzaniu bezpieczeństwem informacji

Źródło: opracowano na podstawie J. Żywiołek, Zarządzanie zasobami informacji i wiedzy jako determinanta bezpieczeństwa przedsiębiorstwa, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2020, s. 68.

Realizacja i zachowanie należytego poziomu ochrony danych wymaga przeprowadzenia analizy aktualnego stanu, co stanowi wstęp do opracowania strategii bezpieczeństwa, gdzie kluczową rolę odgrywają często organizowane szkolenia. Podnoszenie poziomu świadomości pracowników umożliwia ich większe zaangażowanie w tworzenie koncepcji zabezpieczeń. Na tym etapie należy przystąpić do wykonania analizy ryzyka. Próba oceny ryzyka bez wcześniejszego zdobycia odpowiedniej wiedzy jest nieefektywna, gdyż nie można dokładnie ocenić potencjalnych zagrożeń bez uprzedniego zrozumienia ich kontekstu. Podjęcie tych kroków umożliwia opracowanie skutecznej polityki lub strategii bezpieczeństwa. Niezbędne jest również ciągłe sprawdzanie poziomu wiedzy pracowników i monitorowanie stanu bezpieczeństwa[178].

[178] J. Żywiołek*, Zarządzanie zasobami informacji…,* op. cit., s. 68-69.

Wszystkie osoby zainteresowane powinny być zaznajomione z polityką bezpieczeństwa informacji w zakresie, który ich dotyczy. Opracowanie tej polityki jest zadaniem angażującym całą organizację, jednakże konieczne jest wyznaczenie jednej osoby, która będzie odpowiedzialna za koordynację prac nad tym dokumentem[179]. Menedżerowie na odpowiednich poziomach zarządzania są zobowiązani do opracowywania konkretnych polityk bezpieczeństwa[180]. Struktura odpowiedzialności związana z bezpieczeństwem przedsiębiorstwa została zilustrowana na rysunku nr 11.



Rysunek 11 Zarządzanie bezpieczeństwem informacji – hierarchia odpowiedzialności
Źródło: opracowano na podstawie J. Żywiołek, Zarządzanie zasobami informacji…, op. cit., s. 71.

Polityka bezpieczeństwa powinna dokładnie określać, jakie struktury odpowiadają za zarządzanie bezpieczeństwem informacji w firmie, wskazując, kto zajmuje się kierowaniem, kto odpowiedzialny jest za działania operacyjne, a kto za nadzór[181]. Ważne jest, aby wyraźnie zdefiniować role, zadania oraz wzajemne relacje między tymi jednostkami. Konieczne jest również określenie ich uprawnień i zakresu odpowiedzialności w kontekście podejmowania decyzji[182].

Polityka bezpieczeństwa w przedsiębiorstwie jest fundamentem dla zapewnienia ciągłości operacyjnej, ochrony wartości biznesowej oraz budowania trwałych relacji

[179] Ibidem, s. 71.
[180] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection. Information security management systems Requirements,* ISO, https://www.iso.org/standard/27001 [dostęp 21.02.2024 r.].
[181] M. Ergan, T. Mather, *The Executive Guide to Information Security*, Addison-Wesley, Indianapolis 2005, s. 324.
[182] J. Żywiołek*, Zarządzanie zasobami informacji…,* op. cit., s. 71.

z klientami i partnerami na podstawie wzajemnego zaufania i bezpieczeństwa. Stanowi ona kompleksowe narzędzie zarządzania ryzykiem, które wymaga zaangażowania na wszystkich poziomach organizacji, adaptacji do zmieniających się warunków i ciągłego monitorowania. Kluczowe jest, aby była ona opracowana w sposób przemyślany, zrozumiały dla wszystkich pracowników i systematycznie aktualizowana, co pozwala na utrzymanie wysokiego poziomu bezpieczeństwa informacyjnego w dynamicznie zmieniającym się środowisku biznesowym. Jej skuteczność zależy od zintegrowanego podejścia do bezpieczeństwa, obejmującego aspekty personalne, fizyczne i technologiczne, oraz wymaga ciągłej analizy ryzyka i adaptacji strategii do wykrytych zagrożeń.

W niniejszym podrozdziale dokonano analizy wdrażania standardów i norm w zakresie bezpieczeństwa informacji, ze szczególnym uwzględnieniem ich wpływu na zabezpieczenie danych i zarządzanie ryzykiem. Autor podkreśla znaczenie szerokiej gamy regulacji prawnych oraz norm ISO, które umożliwiają organizacjom przegląd i wdrażanie adekwatnych działań ochronnych. Przedstawione standardy, jak np. ISO/IEC 27000 i ISO/IEC 27001, obejmują różne aspekty zarządzania bezpieczeństwem informacji, od słownikowych po sektorowe, co pozwala organizacjom skutecznie dostosowywać strategie ochronne do ich specyficznych potrzeb. Istotne są również akty prawne, takie jak ustawa o ochronie danych osobowych (RODO), ustawa o ochronie informacji niejawnych czy Prawo telekomunikacyjne, które regulują przetwarzanie i zabezpieczanie danych, zapewniając kompleksowy system ochrony.

W kontekście hipotezy szczegółowej: *stosowanie odpowiednich standardów i norm w zarządzaniu bezpieczeństwem informacji, pozwala na skuteczne rozpoznawanie zagrożeń, kształtując poziom ochrony danych oraz tajemnicy przedsiębiorstwa*, podrozdział potwierdza następujące elementy:

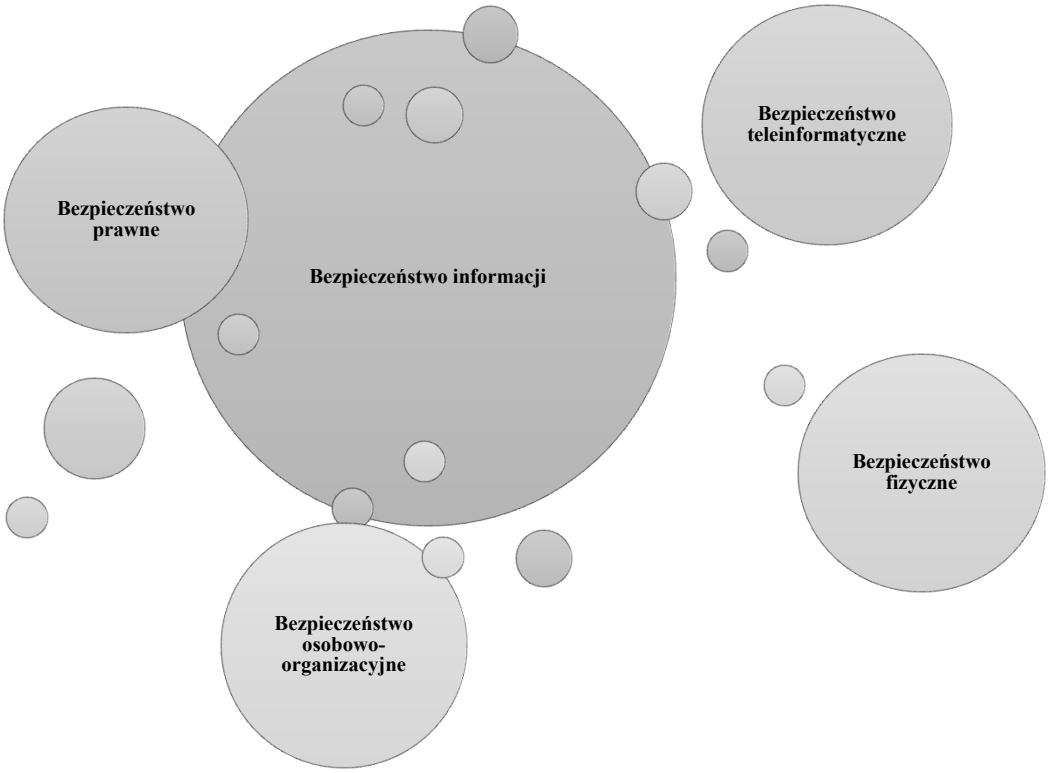
a) **s**tosowanie odpowiednich standardów i norm – przedstawiono szeroki wachlarz norm i standardów (np. ISO/IEC 27001, ISO/IEC 27005), które pomagają organizacjom tworzyć uporządkowany i skuteczny system zarządzania bezpieczeństwem informacji. Normy te wspierają precyzyjne wyznaczenie procedur i zabezpieczeń, odpowiadających na potrzeby ochrony danych,
b) skuteczne rozpoznawanie zagrożeń – normy, dotyczące zarządzania ryzykiem, są kluczowe dla identyfikacji zagrożeń i analizowania potencjalnych ryzyk związanych z bezpieczeństwem informacji. Wdrażanie tych norm pozwala na proaktywne rozpoznawanie zagrożeń i podejmowanie działań prewencyjnych,
c) kształtowanie poziomu ochrony danych oraz tajemnicy przedsiębiorstwa – przedstawione normy oraz regulacje prawne, kształtują standardy ochrony, obejmując procedury przetwarzania danych, zasadę minimalizacji i transparentności w zarządzaniu

danymi osobowymi. Ochrona danych osobowych i informacji niejawnych jest kluczowa dla utrzymania tajemnicy przedsiębiorstwa.

Podsumowując, niniejszy podrozdział częściowo potwierdza hipotezę szczegółową, że wdrożenie odpowiednich standardów i norm jest kluczowe dla skutecznego zarządzania bezpieczeństwem informacji, rozpoznawania zagrożeń oraz zapewnienia odpowiedniego poziomu ochrony danych i poufności w organizacji.

2.3 Taksonomia zagrożeń bezpieczeństwa informacji w aspekcie zarządzania bezpieczeństwem przedsiębiorstwa

Bezpieczeństwo jest procesem nieustannym, w którym dąży się do doskonalenia metod gwarantujących odczucie ochrony. Postrzeganie i podejście do bezpieczeństwa jako priorytetowego obszaru zainteresowania przedsiębiorstw manifestuje się w ich reakcjach na potencjalne zagrożenia[183]. Te działania, choć wymagające i często wiążące się z wysokimi kosztami, są kluczowe, jednak ich wyzwania mogą skłaniać niektóre organizacje do rezygnacji z ich realizacji. Podstawowe elementy ochrony informacji zostały zilustrowane na rysunku nr 12.



Rysunek 12 Elementy składowe bezpieczeństwa informacji
Źródło: opracowano na podstawie J. Łuczak (red.), Zarządzanie bezpieczeństwem informacji…, op. cit.

[183] Ibidem, s. 74.

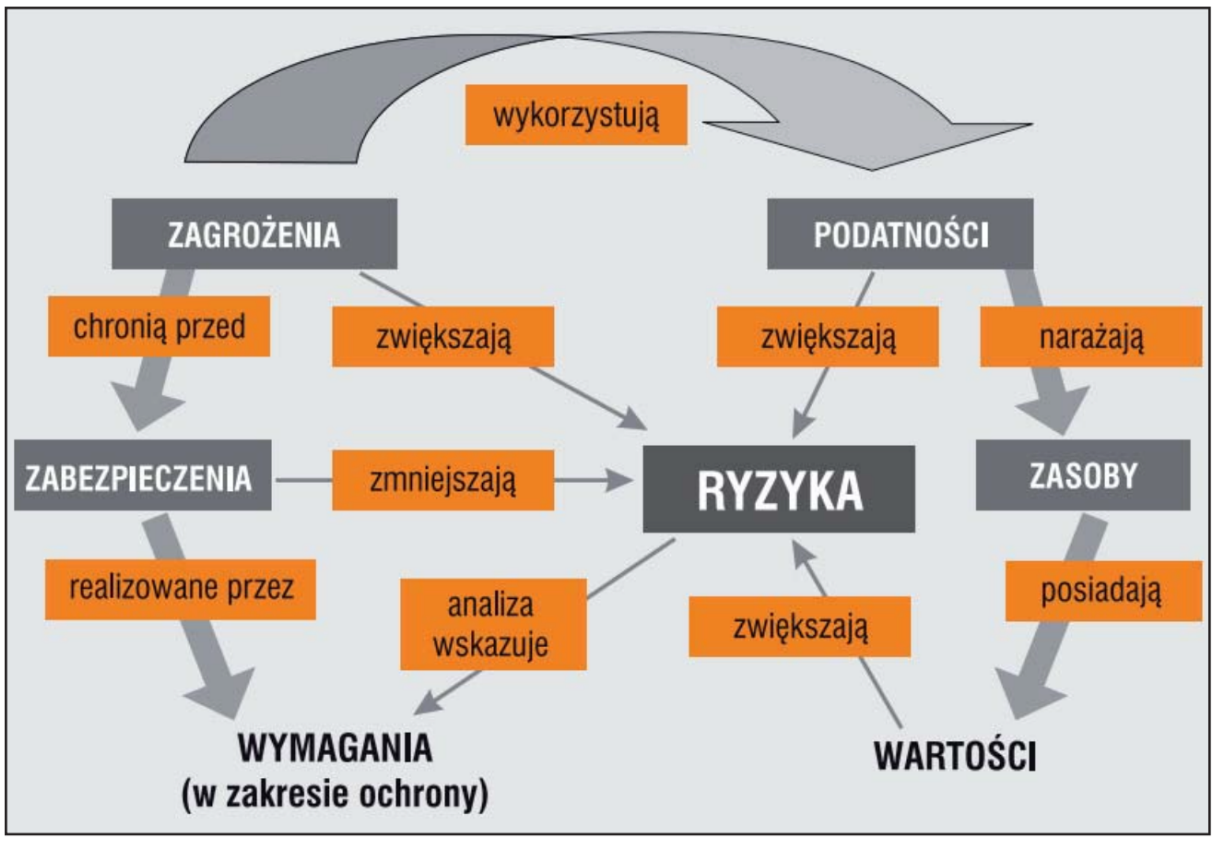
Kategoryzacja niebezpieczeństw dla bezpieczeństwa danych oraz ich precyzyjne określenie tworzą fundament ochrony informacji w firmie. W definicjach z dziedziny politologii, zwłaszcza tych dotyczących bezpieczeństwa, zagrożenia są często klasyfikowane jako wyzwania. Adekwatna identyfikacja i reagowanie na takie wyzwania mogą zamienić je w szanse, podczas gdy wyzwania zauważone nieodpowiednio lub zbyt późno mogą ewoluować w zagrożenia[184]. To podejście do zagrożeń znajduje odzwierciedlenie również w innych dziedzinach naukowych, takich jak zarządzanie czy socjologia. Organizacje skoncentrowane na innowacjach i poszukiwaniu nowych rozwiązań codziennie napotykają nowe wyzwania i zagrożenia, przy czym ich spektrum nieustannie się rozszerza. Na rysunku nr 13 przedstawiono wybrane zagrożenia dla bezpieczeństwa informacyjnego organizacji.

Rysunek 13 Kategorie zagrożeń informacyjnych
Źródło: opracowano na podstawie P. Bączek, Zagrożenia informacyjne a bezpieczeństwo…, op. cit., s. 30.

Zajmowanie się działalnością komercyjną wiąże się z ryzykiem, które manifestuje się w organizacji jako konkretne niebezpieczeństwo. Różnorodność tych ryzyk jest szeroka i może

[184] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo…*, op. cit., s. 30.

ewoluować wraz z upływem czasu[185]. Elementy bezpieczeństwa oraz ich wzajemne relacje zostały przedstawione na rysunku nr 14.

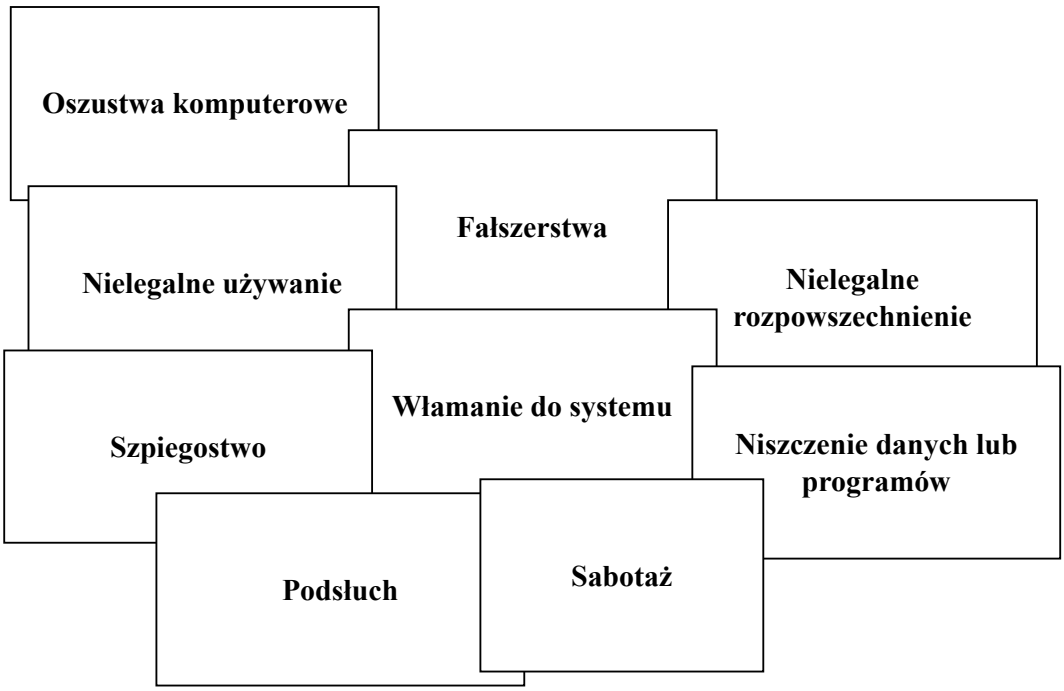


Rysunek 14 Elementy bezpieczeństwa oraz ich wzajemne relacje
Źródło: M. Blim, Teoria ochrony informacji (część 1), „Zabezpieczenia" nr 3/2007, s. 60 za J. Werner, E. Szczepaniuk, Bezpieczeństwo informacyjne…, op. cit., s. 170.

P. Sienkiewicz w swoich rozważaniach o niepewności i ryzyku w kontekście globalnego społeczeństwa informacyjnego wskazuje na konieczność powiązania ryzyka z pojęciem zagrożeń, zwłaszcza z akumulacją ryzyk pochodzących z różnorodnych źródeł niebezpieczeństw[186]. Na poziom niepewności wpływa dynamiczny rozwój technologiczny. Eksperci zauważają, że postęp w dziedzinie technologii informacyjnych tworzy sprzyjające warunki dla aktywności przestępczej. Nowe technologie, z jednej strony ułatwiają podejmowanie decyzji na wielu poziomach zarządzania firmą, z drugiej zaś wprowadzają nowe typy zagrożeń[187]. Te niebezpieczeństwa mogą zagrażać ludzkim, materialnym, finansowym

[185] F. A. Shaikh, M. Siponen, *Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity*, Computers & Security Volume 124, January 2023, https://doi.org/10.1016/j.cose.2022.102974, s. 3.
[186] P. Sienkiewicz, *Społeczeństwo informacyjne jako społeczeństwo ryzyka,* {w:] *Społeczeństwo informacyjne. Aspekty funkcjonalne i dysfunkcjonalne* (red.) W. Haber, M. Niezgoda, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006, s. 64.
[187] A. Żebrowski, M. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2006, s. 70.

oraz informacyjnym zasobom organizacji[188]. Rysunek nr 15 przedstawia typowe formy działalności przestępczej w obszarze IT i ich wzajemne relacje uwzględnione przez B. Fischera w rozważaniach z początku XXI w. Przedstawił 9 kluczowych kategorii dla bezpieczeństwa informacji w organizacji[189].



Rysunek 15 Kategorie i relacje przestępstw komputerowych
Źródło: B. Fischer, Przestępstwa komputerowe i ochrona…, op. cit.

Przed organizacjami stoi zadanie zabezpieczenia poufności, integralności oraz dostępności operacji związanych z gromadzeniem, przetwarzaniem i dystrybucją informacji, tak aby dostęp do nich mieli jedynie pracownicy upoważnieni na podstawie ich roli zawodowej lub powierzonych obowiązków. Wyróżnia się pięć głównych sfer ryzyka dla infrastruktury IT, obejmujących:

a) umiejętności i zaufanie pracowników,
b) zarządzanie systemami i sieciami,
c) infrastrukturę telekomunikacyjną,
d) tworzenie sprzętu i oprogramowania,
e) zasady użytkowania systemów informatycznych
f) obsługę nośników danych[190].

[188] J. Żywiołek*, Zarządzanie zasobami informacji…,* op. cit., s. 76.
[189] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Wydawnictwo Zakamycze, Kraków 2000, s. 33.
[190] A. Żebrowski, M. Kwiatkowski, *Bezpieczeństwo informacji…,* op. cit., s. 64.

W obliczu licznych ryzyk związanych z bezpieczeństwem informacji, kluczowe jest zidentyfikowanie najbardziej krytycznych obszarów potencjalnych zagrożeń, by móc następnie zaprojektować i zaimplementować strategie ich ochrony, ograniczyć dostęp dla autoryzowanych użytkowników, zorganizować szkolenia oraz prowadzić ciągły monitoring. W przedsiębiorstwach obserwuje się rosnącą skalę przestępczości gospodarczej i innych nieprawidłowości[191]. Tabela nr 10 prezentuje rodzaje zagrożeń dla sektora biznesowego, w tym przestępstwa ekonomiczne, cyberprzestępczość oraz aktywności szpiegowskie.

Tabela 10 Rodzaje zagrożeń dla sektora biznesowego

Przestępstwa w przedsiębiorstwach		
Gospodarcze i bankowe	**Komputerowe**	**Działalność ludzi**
a) Fałszerstwa dokumentów publicznych, b) Fałszerstwa dokumentów biznesowych, c) Oszustwa.	a) Niszczenie informacji, b) Fałszerstwa danych, c) Podsłuch, d) Sabotaż, e) Piractwo, f) Wandalizm, g) Hacking, h) Cracking.	a) Wywiad technologiczny, b) Wywiad handlowy, a) Wywiad konkurencyjny, b) Wywiad naukowy.

Źródło: opracowano na podstawie. M. Kuta, Polityka bezpieczeństwa informacji w przedsiębiorstwie – aspekty praktyczne, W: Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa (red.) R. Borowiecki, M. Kwieciński, Wydawnictwo Zakamycze, Kraków 2003, s. 267.

Zdarzenia przestępcze w sferze biznesowej należą do wyjątkowej kategorii, gdyż stanowią one ryzyko nie tylko dla samych firm lub instytucji, ale również dla ich zasobów. Dotyczy to danych zgromadzonych w bazach informacyjnych, środków finansowych, a także wartości niematerialnych przedsiębiorstwa, takich jak renoma, nabyte relacje czy handlowe uprawnienia[192].

Zagrożenia informacyjne dla organizacji można klasyfikować według pochodzenia ich źródeł na:

a) wewnętrzne, generowane w ramach samej organizacji, obejmujące ryzyko utraty lub zniszczenia danych, albo niemożności ich przetwarzania z przyczyn losowych lub błędów, jak również ryzyko wynikające z działań osób działających nieuczciwie wewnątrz organizacji,

[191] J. Żywiołek*, Zarządzanie zasobami informacji…,* op. cit., s. 77.
[192] M. Kuta, *Polityka bezpieczeństwa informacji…,* op. cit., s. 267

b) zewnętrzne, wynikające z działań poza strukturą przedsiębiorstwa, włączając w to ryzyko utraty, zniszczenia danych lub uniemożliwienia ich przetwarzania przez celowe lub niezamierzone akcje osób trzecich wobec systemów lub sieci,
c) fizyczne, gdzie utrata, zniszczenie danych lub brak możliwości ich przetwarzania są efektem awarii, katastrofy lub innych nieoczekiwanych wydarzeń, które mają wpływ na infrastrukturę IT lub urządzenia sieciowe[193].

Jednym z kluczowych źródeł ryzyka dla bezpieczeństwa danych w firmach jest nieautoryzowany dostęp do chronionych informacji przez osoby, które mają do nich dostęp. Wyzwaniem okazuje się również stosowanie przepisów dotyczących ochrony danych tajnych. Postęp w dziedzinie ICT i globalizacja rynku sprzyjają automatyzacji procesów biznesowych i księgowych, ułatwiają komunikację na skalę światową oraz umożliwiają zawieranie transakcji z partnerami z różnych części świata bez konieczności bezpośredniego kontaktu[194]. Jednak korzyści wynikające z cyfryzacji działalności gospodarczej wiążą się z ryzykiem. Systemy IT, które są projektowane do zbierania, przetwarzania i udostępniania informacji w szybki sposób, mogą przyciągać uwagę osób o zamiarach przestępczych. Różnorodność i charakter tych systemów, a szczególnie ich pochodzenie, budzą zainteresowanie nie tylko agencji wywiadowczych i innych oficjalnych instytucji potencjalnie stanowiących zagrożenie, ale również grup terrorystycznych i jednostek. Systemy te są narażone na działania każdego, kto dysponuje odpowiednią wiedzą i umiejętnościami[195].

Naruszenia bezpieczeństwa danych, które są klasyfikowane jako poufne lub chronione ze względów państwowych czy firmowych, mają na celu uzyskanie kontroli nad zabezpieczonymi systemami informatycznymi. Takie incydenty bezpieczeństwa komputerowego mają miejsce, kiedy działania są świadomie ukierunkowane na naruszenie integralności systemów. Można wyróżnić dwie główne kategorie ataków:

a) aktywne ataki, które obejmują bezpośrednie lub pośrednie interwencje w system, zmieniające przepływ danych lub wprowadzające fałszywe informacje,
b) pasywne ataki, charakteryzujące się brakiem bezpośredniego wpływu na system, do których zalicza się między innymi przechwytywanie komunikacji lub monitoring sieci w celu identyfikacji kluczowych komponentów, takich jak serwery lub stacje robocze[196].

[193] A. Żebrowski, M. Kwiatkowski, *Bezpieczeństwo informacji…,* op. cit., s. 72.
[194] J. Żywiołek*, Zarządzanie zasobami informacji…,* op. cit., s. 78.
[195] Ibidem, s. 63.
[196] A. Barczyk, T. Sydoruk, *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy Bellona, Warszawa 2003, s. 70.

Ryzyko ataku znacząco wzrasta w przypadku, gdy istnieje prawdopodobieństwo wystąpienia:

a) nieautoryzowanego dostępu do danych poufnych lub służbowych przechowywanych, przetwarzanych bądź przesyłanych, bez wpływu na system,
b) nieautoryzowanych działań wpływających na system, co może skutkować zmianą w funkcjonowaniu sieci, dostępem do danych, wprowadzeniem fałszywych informacji, uszkodzeniem danych i zasobów systemowych, lub nieuprawnionymi zmianami informacji[197].

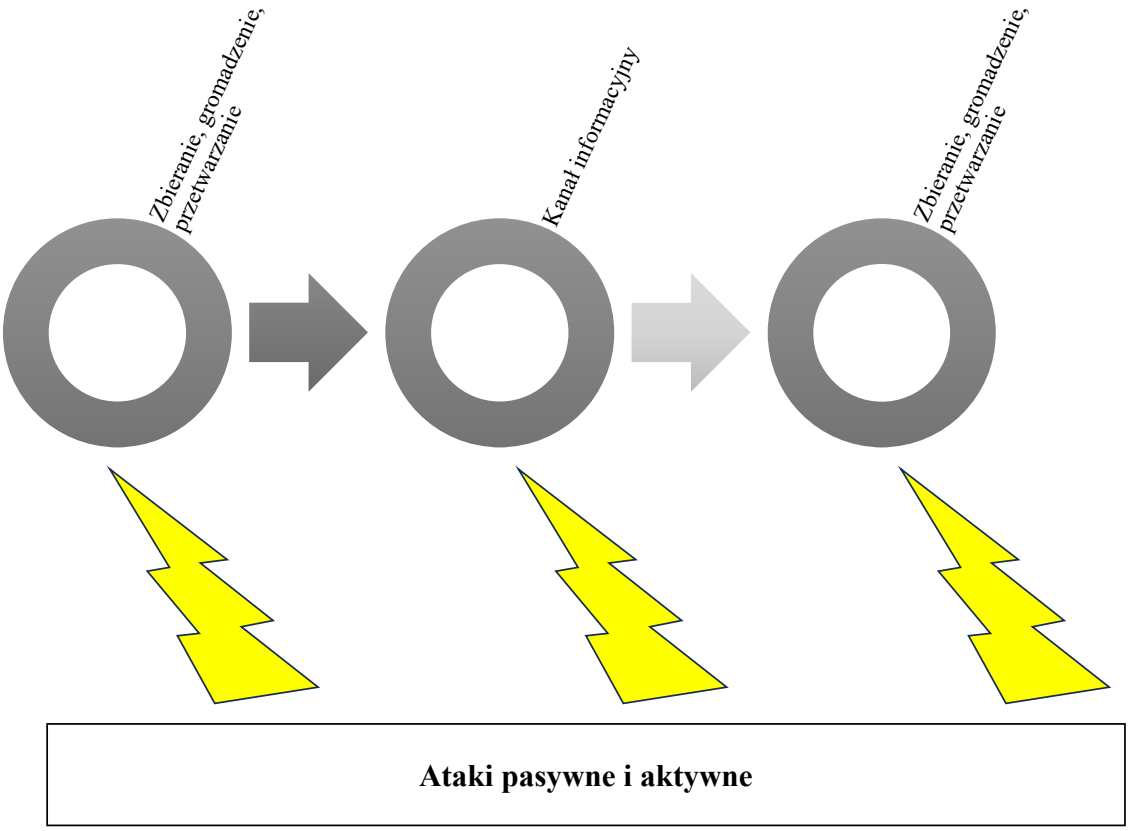
W erze nieograniczonego dostępu do informacji i obfitych zasobów online, użytkownicy sieci Internet muszą być świadomi ryzyka, które niosą za sobą nieautoryzowane osoby. Podczas prób włamania do systemu, intruz podąża za ustalonym schematem, identyfikuje słabości systemu i zdobywa dostęp do jego zasobów. Po przejęciu kontroli nad systemem, podejmuje działania mające na celu usunięcie dowodów swojej obecności. Zagrożenia mogą przybierać różne postaci, lecz konsekwencje są zawsze takie same - utrata lub zniszczenie danych, co skutkuje szkodami dla organizacji[198].

Identyfikacja zagrożeń umożliwia przystąpienie do oceny ryzyka w ramach organizacji. Kluczowe dla stworzenia kompleksowego planu zabezpieczeń informacyjnych jest efektywne zarządzanie ryzykiem. Analiza ryzyka w sferze bezpieczeństwa danych pozwala na określenie całkowitego ryzyka, które powinno być zredukowane do poziomu uznawanego za dopuszczalny. Wśród elementów, które mogą przyczyniać się do pojawienia się zagrożeń dla bezpieczeństwa informacji, wymienić można:

a) rozmieszczenie zasobów na obszernym terenie,
b) używanie sprzętu komputerowego bez licencji,
c) korzystanie z nieautoryzowanego oprogramowania,
d) wykorzystanie sprzętu i oprogramowania o nieznanym pochodzeniu,
e) opór ze strony użytkowników i twórców wobec implementacji zabezpieczeń informacyjnych[199].

Cyberataki są realizowane w różnych lokalizacjach, dotykając obszarów związanych z gromadzeniem, obróbką, magazynowaniem, transmisją oraz dystrybucją danych, co zostało zilustrowane na rysunku nr 16.

[197] Ibidem, s. 68.
[198] J. Żywiołek*, Zarządzanie zasobami informacji…,* op. cit., s. 80.
[199] B. Ciecińska, J. Łunarski, R. Perłowski, D. Stadnicka, *Systemy zarządzania bezpieczeństwem…*, op. cit., s. 171.



Rysunek 16 Uproszczony schemat informacyjny z miejscami narażonymi na ataki
Źródło: opracowano na podstawie B. Ciecińska, J. Łunarski, R. Perłowski, D. Stadnicka, Systemy zarządzania bezpieczeństwem…, op. cit.

W dziedzinie bezpieczeństwa informacji rozróżnienie między atakami pasywnymi i aktywnymi jest kluczowe dla zrozumienia i minimalizowania potencjalnych zagrożeń dla danych organizacyjnych oraz systemów. Ataki pasywne, charakteryzujące się nieautoryzowanymi próbami dostępu bez ingerencji w system, mają na celu skryte zebranie danych, co stanowi znaczące ryzyko dla poufności. Z kolei ataki aktywne obejmują bezpośrednią interakcję z systemem, potencjalnie zmieniając dane lub funkcjonowanie systemu, co kompromituje integralność i dostępność informacji. Oba typy ataków wymagają solidnych środków bezpieczeństwa oraz ciągłej czujności w celu ochrony cyfrowych zasobów przedsiębiorstwa.

W reakcji na wyzwania związane z bezpieczeństwem danych, przedsiębiorstwa podjęły inicjatywy mające na celu implementację oraz optymalizację swoich procedur ochrony danych. Działania te obejmowały rozwój:

a) systemów zarządzania bezpieczeństwem w ramach organizacji,
b) strategii bezpieczeństwa,
c) polityk dotyczących ochrony danych,

d) systemów zarządzania bezpieczeństwem informacji,
e) licznych wytycznych, standardów i technologii związanych z ochroną danych[200].

Różnorodność i złożoność tych metod spowodowały, że organizacje zaczęły eksplorować alternatywne podejścia i jednolite strategie ochrony danych. Biorąc pod uwagę, że zagrożenia informacyjne mogą wynikać z różnych sytuacji, takich jak braki, ograniczenia dostępu, nadmiar, manipulacja, fałszerstwo, nieczytelność, nielegalne pozyskanie, przestarzałość informacji, etc., zagrożenia te charakteryzują się jako sytuacje z ograniczeniami lub nadużyciami w legalnym dostępie do aktualnych, wiarygodnych, integralnych i poufnie chronionych informacji[201]. Podsumowując, dla skutecznego utrzymania wysokiego poziomu bezpieczeństwa informacyjnego, organizacje powinny realizować jak najwięcej działań wewnętrznie, opierając się na sprawdzonych modelach zarządzania bezpieczeństwem i najlepszych praktykach w zakresie formułowania polityk bezpieczeństwa, lub delegować te obowiązki na ekspertów w dziedzinie bezpieczeństwa informacyjnego.

Korzystając z wniosków z najnowszych prac naukowych, w tym badań Vinoda Pachghare[202] oraz prezentacji wyników badań na 30. Sympozjum Bezpieczeństwa USENIX dokonanej przez Nicolasa Huamana i innych[203], jest oczywiste, że zrozumienie natury zagrożeń bezpieczeństwa informacyjnego i wdrożenie kompleksowych ram bezpieczeństwa jest wysoce pożądane, a wręcz niezbędne. Studia te podkreślają znaczenie przyjęcia wielowarstwowych strategii bezpieczeństwa, które adresują różne wektory ataków i zapewniają odporność systemów informacyjnych na oba typy zagrożeń. Poprzez połączenie środków technicznych, formułowania polityk i szkolenia personelu, organizacje mogą znacząco zmniejszyć swoją podatność na te wszechobecne wyzwania bezpieczeństwa.

Kluczową funkcją w kierowaniu procesami informacyjnymi w ramach przedsiębiorstwa, które odzwierciedlają jego główne cele, jest utrzymanie bezpieczeństwa danych. Priorytetem zarządzania informacją jest zapewnienie, że wszystkie operacje i funkcje zarządcze na każdym poziomie organizacyjnym są integralnie związane z procesami informacyjnymi. W związku z kluczową rolą, jaką bezpieczeństwo informacyjne i zarządzanie informacją odgrywają w działaniach firm, wdrożenie przedstawionych strategii jest postrzegane jako konieczne i odpowiednie. Poruszone kwestie stanowią fundament dla

[200] J. Stanik, M. Kiedrowicz, *Model systemu zarządzania…*, op. cit., s. 335.
[201] Ibidem.
[202] V. K. Pachghare, *Cryptography and information security. Third edition*, Wydawnictwo PHI Learning Pvt. Ltd., Delhi 2019, s. 370-372.
[203] N. Huaman, B. Skarczinski, C. Stransky, D. Wermke, Y. Acar, A. Dreißigacker, S. Fahl, *A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises*, 30th USENIX Security Symposium 2021, https://www.usenix.org/system/files/sec21-huaman.pdf [dostęp 22.02.2024 r.], s. 1241-1243.

tworzenia modelu systemu i zarządzania bezpieczeństwem informacyjnym w przedsiębiorstwie.

Podrozdział koncentruje się na taksonomii zagrożeń związanych z bezpieczeństwem informacyjnym w przedsiębiorstwie, ukazując różnorodność i złożoność zagrożeń, które mogą wpłynąć na ochronę informacji w organizacji. Wprowadza on podział zagrożeń na wewnętrzne, zewnętrzne i fizyczne oraz omawia znaczenie klasyfikacji zagrożeń i metod przeciwdziałania im jako fundamentów ochrony informacji. Przedstawione zagrożenia obejmują ataki pasywne i aktywne, działania przestępcze oraz cyberataki, które zagrażają kluczowym aspektom, takim jak poufność, integralność i dostępność danych. W podrozdziale wskazano również na znaczenie środków zarządzania bezpieczeństwem, strategii ochrony, polityk oraz systemów zarządzania bezpieczeństwem informacji jako niezbędnych dla ochrony zasobów informacyjnych.

W kontekście hipotezy szczegółowej: *stosowanie odpowiednich standardów i norm w zarządzaniu bezpieczeństwem informacji, pozwala na skuteczne rozpoznawanie zagrożeń, kształtując poziom ochrony danych oraz tajemnicy przedsiębiorstwa*, niniejszy podrozdział potwierdza kilka kluczowych elementów tej hipotezy:

a) skuteczne rozpoznawanie zagrożeń – omówiono potrzebę identyfikacji i klasyfikacji zagrożeń, co jest niezbędnym krokiem w procesie ich rozpoznawania i zarządzania nimi. Analiza typów zagrożeń pozwala na lepsze przygotowanie organizacji do ich monitorowania i reagowania na nie, co wpisuje się w proces skutecznego rozpoznawania zagrożeń,
b) kształtowanie poziomu ochrony danych – scharakteryzowano systemy zarządzania bezpieczeństwem i strategie obronne, których celem jest ochrona danych, ich integralności, dostępności i poufności. Wskazuje to na potrzebę systematycznego podejścia, w którym implementacja procedur i standardów kształtuje poziom ochrony informacji w przedsiębiorstwie,
c) ochrona tajemnicy przedsiębiorstwa – scharakteryzowane działania ochronne, obejmujące m.in. zarządzanie ryzykiem, ochronę przed atakami oraz procedury ochrony danych, wspierają ochronę zasobów informacji, które są kluczowe dla tajemnicy przedsiębiorstwa. Podkreślono też konieczność ograniczenia dostępu do informacji wyłącznie dla osób upoważnionych, co jest istotne dla ochrony danych wrażliwych.

Podsumowując, rozważanie przedstawione w niniejszym podrozdziale częściowo potwierdzają hipotezę szczegółową, iż stosowanie odpowiednich standardów i norm w zarządzaniu bezpieczeństwem informacji, pozwala na skuteczne rozpoznawanie zagrożeń, kształtując poziom ochrony danych oraz tajemnicy przedsiębiorstwa.

2.4 Istota zarządzania bezpieczeństwem informacji w przedsiębiorstwie

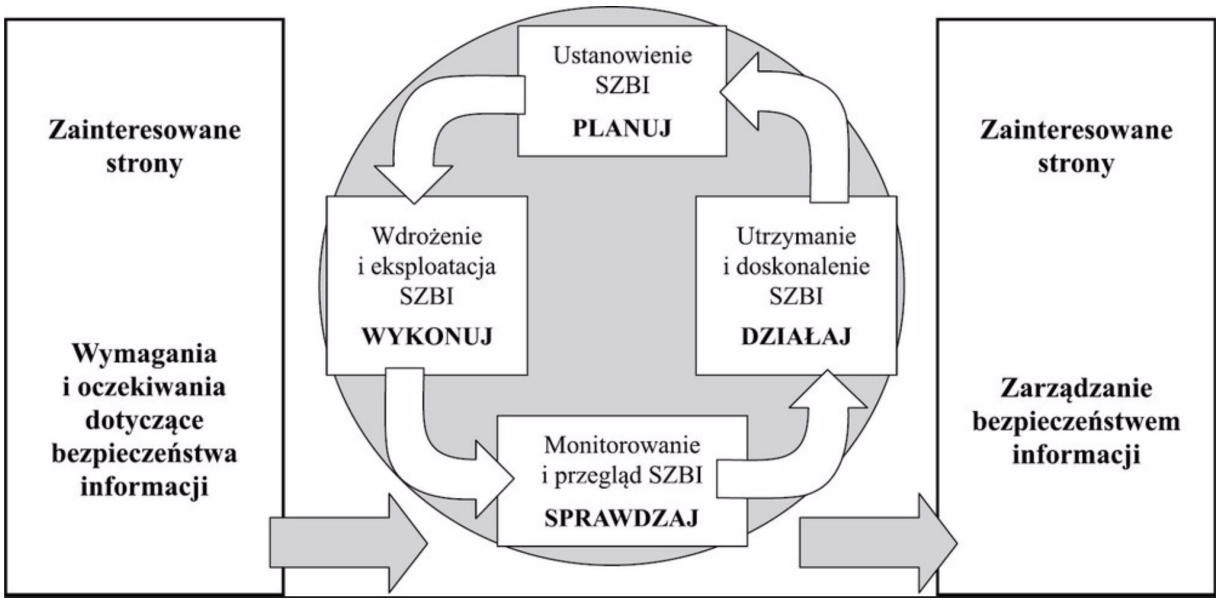
Zapewnienie ochrony informacji w organizacji wymaga skoordynowanych działań w różnych sektorach. Powinno się wdrażać strategie obejmujące kompleksowe zarządzanie procesami informacyjnymi i ich aplikację na wielu szczeblach decyzji. Takie strategie mogą okazać się efektywne przy zastosowaniu zintegrowanego zarządzania bezpieczeństwem informacji, które bierze pod uwagę wszystkie powiązania przyczynowo-skutkowe oraz zasoby organizacji. Realizacja takich strategii umożliwia udoskonalenie każdego aspektu systemu. Obecnie istnieje wiele metod systemowego zarządzania bezpieczeństwem informacji. W niniejszym podrozdziale przywołano cztery wybrane metody, które mogą być skutecznie zaimplementowane zarówno w sektorze publicznym, jak i prywatnym. Do omówionych modeli zaliczyć należy:

a) model ISO/IEC 27001,
b) model TISM,
c) metoda TRA,
d) metoda COBIT.

Model ISO/IEC 27001, stworzony przez *International Organization for Standardization* (ISO) i *International Electrotechnical Commission* (IEC), przedstawia metodykę praktycznego wdrożenia systemu zarządzania bezpieczeństwem informacji, dostosowaną do potrzeb dowolnej organizacji. Charakteryzuje się on procesowym podejściem, umożliwiającym zaplanowanie, uruchomienie, utrzymanie, nadzorowanie, ocenę i ulepszanie systemu. W normie zaakcentowano, że decyzja o implementacji systemu musi wynikać ze strategicznej analizy potrzeb biznesowych danej organizacji.

Przyjęcie tego modelu nie dopuszcza do pominięcia żadnego z wymogów określonych w standardzie ISO/IEC, ale pozwala na wprowadzenie ograniczeń w zakresie stosowania poszczególnych zabezpieczeń, pod warunkiem, że zostaną one poparte analizą i akceptacją ryzyka. Takie działanie wymaga uzasadnienia, dokumentacji i zatwierdzenia, nie powinno jednak negatywnie wpływać na poziom bezpieczeństwa w organizacji oraz na spełnienie obowiązków wynikających z oceny ryzyka, przepisów prawnych oraz wymogów standardu. Model ten opiera się na procesowym podejściu, wykorzystując cykl PDCA (Plan-Do-Check-Act) zaproponowany przez Williama Deminga[204], co jest ukazane na rysunku nr 17.

[204] Vide:. W. E. Deming, *Out of the crisis*, Massachusetts Institute of Technology, Cambridge 1986, s. 88.



Rysunek 17 Model działań PDCA w ramach Systemu Zarządzania Bezpieczeństwem Informacji

Źródło: K. Liderman, Bezpieczeństwo informacyjne…, op. cit., s. 266.

Model Zarządzania Bezpieczeństwem Informacji, opisany w standardzie, został stworzony w celu dostarczenia odpowiednich i zrównoważonych środków ochrony, które skutecznie zabezpieczają wartości informacyjne, umożliwiając tym samym budowanie zaufania u zainteresowanych podmiotów względem ogłaszanej efektywności w ochronie zasobów informacyjnych. Model ten opiera się o działanie w ramach wszystkich procesów Systemu Zarządzania Bezpieczeństwem Informacji na podstawie następujących etapów:

a) **planuj (ustanowienie SZBI)** – wprowadzenie polityki Zarządzania Bezpieczeństwem Informacji, ustalenie celów, procesów oraz procedur, które są kluczowe dla zarządzania ryzykiem i ulepszania ochrony danych, ma na celu osiągnięcie rezultatów, które są w harmonii z zasadami i zamierzeniami organizacji,
b) **wykonuj (wdrożenie i eksploatacja SZBI)** – realizacja i użytkowanie Systemu Zarządzania Bezpieczeństwem Informacji obejmuje aplikację polityk, środków ochronnych, procesów i procedur,
c) **sprawdzaj (monitorowanie i przegląd SZBI)** – ewaluacja oraz w odpowiednich przypadkach, kwantyfikacja efektywności procesów w kontekście polityki bezpieczeństwa, założeń strategicznych oraz zgromadzonej wiedzy praktycznej, a także przygotowanie sprawozdań dla kadry zarządzającej do analizy,
d) **działaj (utrzymanie i doskonalenie SZBI)** – inicjowanie środków korygujących i prewencyjnych w celu nieustannego ulepszania systemu zarządzania

bezpieczeństwem informacji, opierając się na rezultatach audytów wewnętrznych oraz analizie przeprowadzonej przez zarząd (lub innych znaczących danych)[205].

Nazwy rozdziałów w normie ISO odpowiadają zasadniczo zestawom działań wymaganych do stworzenia systemu zarządzania bezpieczeństwem informacji. Działania te obejmują:

a) zdefiniowanie kontekstu operacyjnego organizacji, co obejmuje zrozumienie warunków, w jakich funkcjonuje organizacja, w tym potrzeb i oczekiwań zainteresowanych stron, oraz określenie zakresu systemu zarządzania bezpieczeństwem informacji oraz deklarację jego implementacji.
b) zapewnienie kierowania, co wiąże się z wykazaniem przez najwyższe kierownictwo zaangażowania w implementację i utrzymanie systemu zarządzania bezpieczeństwem informacji, włącznie z opracowaniem i wdrożeniem polityki bezpieczeństwa oraz ustaleniem ról i odpowiedzialności związanych z bezpieczeństwem.
c) planowanie działań, opierając się na wynikach analizy ryzyka, aby osiągnąć określone cele bezpieczeństwa.
d) wspieranie realizowanych działań, dostarczając niezbędne zasoby, określając wymagane umiejętności personelu, podnosząc świadomość celów i działań, organizując efektywną komunikację z personelem i zainteresowanymi stronami oraz tworząc i utrzymując niezbędną dokumentację dotyczącą systemu zarządzania bezpieczeństwem informacji.
e) zarządzanie działaniami operacyjnymi w obszarze systemu zarządzania bezpieczeństwem informacji, koncentrując się głównie na monitorowaniu kluczowych wskaźników ryzyka i odpowiednim komunikowaniu stanu bezpieczeństwa w organizacji.
f) ocena jakość realizowanych działań, ustanawiając i nadzorując odpowiednie wskaźniki, monitorując wybrane procesy i zabezpieczenia, organizując audyty wewnętrzne oraz przeglądy zarządcze.
g) systematycznie doskonalenie działania systemu zarządzania bezpieczeństwem informacji[206].

Ponadto, w przytoczonej normie znalazła się definicja systemu zarządzania bezpieczeństwem informacji, który określony został jako *część całościowego systemu zarządzania oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia*

[205] Ibidem.
[206] Ibidem, s. 267.

bezpieczeństwa informacji; SZBI obejmuje strukturę organizacyjną, polityki, planowane działania, zakresy odpowiedzialności, zasady, procedury, procesy i zasoby[207].

Model ISO/IEC 27001 definiuje kompleksowe wymogi dotyczące tworzenia, operowania i podtrzymywania systemu zarządzania bezpieczeństwem informacji (SZBI), a także szczegółowo opisuje mechanizmy ochrony. W załączniku A do normy przedstawiono szczegółową listę wymagań zabezpieczeń, podzielonych na 11 kategorii, które dotyczą różnorodnych aspektów zabezpieczeń w kontekście ich celów wdrożeniowych. Zabezpieczenia określone w normie obejmują:

a) polityka bezpieczeństwa,
b) organizacja bezpieczeństwa informacji,
c) zarządzanie aktywami,
d) bezpieczeństwo zasobów ludzkich,
e) bezpieczeństwo fizyczne i środowiskowe,
f) zarządzanie systemami i sieciami,
g) kontrola dostępu,
h) pozyskiwanie, rozwój i utrzymywanie systemów informatycznych,
i) zarządzanie incydentami związanymi z bezpieczeństwem informacji,
j) zarządzanie ciągłością działania,
k) zgodność[208].

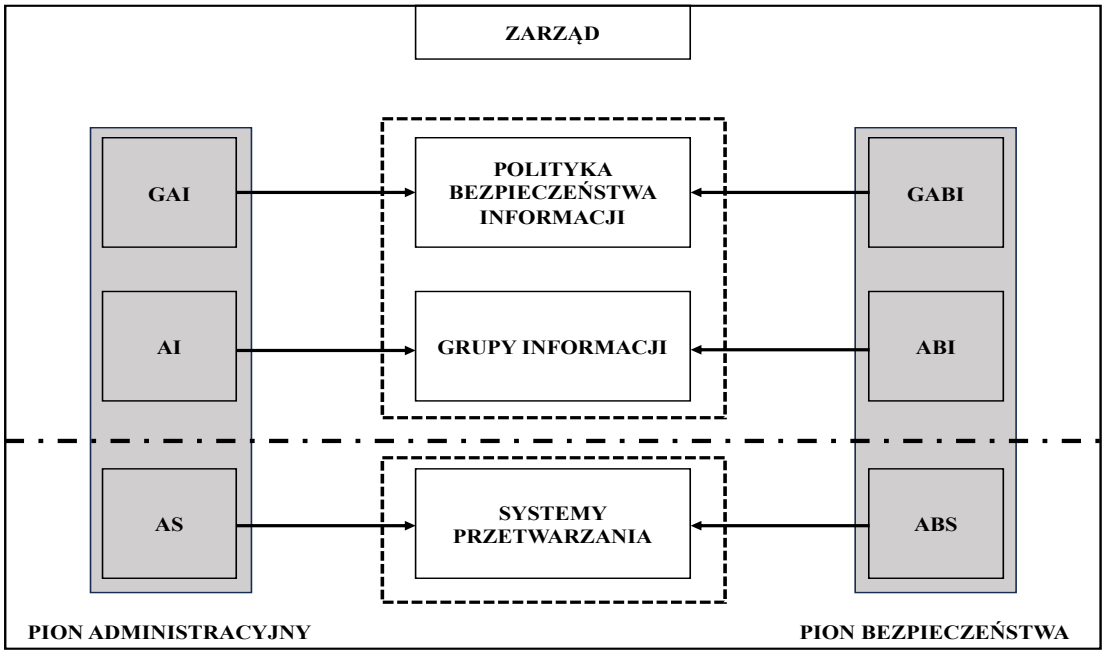
Rekomendacje te wskazują na szeroki zakres zabezpieczeń, nie ograniczających się jedynie do rozwiązań technologicznych, ale również procedur operacyjnych, zarządzania ludźmi oraz polityk bezpieczeństwa.

Implementacja tego modelu wymaga zastosowania metodyki zarządzania ryzykiem związanym z bezpieczeństwem informacji[209]. Wybór stosownych środków ochrony w danej organizacji powinien wynikać z oceny ryzyka, mającej na celu zabezpieczenie przed potencjalnymi zagrożeniami i minimalizację skutków incydentów bezpieczeństwa, zapewniając ochronę proporcjonalną do ryzyka oraz potencjalnych szkód.

Model TISM (Total Interpretive Structural Modeling) wyróżnia się poziomy bazujące na trzech kluczowych aspektach: strukturze organizacyjnej związanej z zarządzaniem bezpieczeństwem informacji, dokumentacji dotyczącej polityki bezpieczeństwa informacji (PBI) oraz identyfikacji lokalizacji przetwarzania i zbierania danych. Struktura zarządzania bezpieczeństwem danych definiuje role kierownicze (zarządzanie) i nadzorcze (ochrona

[207] Ibidem.
[208] J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Wydawnictwo Uniwersytetu Ekonomicznego, Poznań 2010, s. 118.
[209] J. Werner, E. Szczepaniuk, *Bezpieczeństwo informacyjne…*, op. cit., s. 177.

danych) w obrębie trzech wspomnianych poziomów bezpieczeństwa, które przedstawione zostały na rysunku nr 18.



Rysunek 18 Struktura zarządzania informacją i jej bezpieczeństwem według TISM
Źródło: opracowano na podstawie J. Werner, E. Szczepaniuk, Bezpieczeństwo informacyjne…, op. cit., s. 178.

Zgodnie przedstawionym schematem, na poziomie polityki bezpieczeństwa informacji (PBI) wyróżnia się funkcje głównego administratora danych (GAI) oraz głównego administratora ochrony danych (GABI). Na kolejnym poziomie, dotyczącym grup danych, ustanawiane są pozycje: administratora grupy danych (AI) oraz administratora ochrony grupy danych (ABI). Na najniższym poziomie, odnoszącym się do systemu przetwarzania danych, funkcjonują role administratora systemu (AS) oraz administratora ochrony systemu (ABS)[210]. W praktyce, w różnych działach organizacji może dochodzić do łączenia tych ról. Na przykład, zarząd może przejmować obowiązki GAI, ale połączenie funkcji między różnymi działami nie jest praktykowane.

Model TISM podkreśla znaczenie klasyfikacji danych w procesie określania odpowiednich środków ochronnych. Jak wcześniej zaznaczono, decyzja o ochronie konkretnych zbiorów danych może wynikać z wymogów prawnych (jak w przypadku danych osobowych) lub z własnych strategii organizacji (na przykład ochrona tajemnicy handlowej). W tym modelu sugeruje się trzy poziomy klasyfikacji danych:

a) dane chronione na drugim poziomie – dostęp ograniczony do określonej grupy osób,

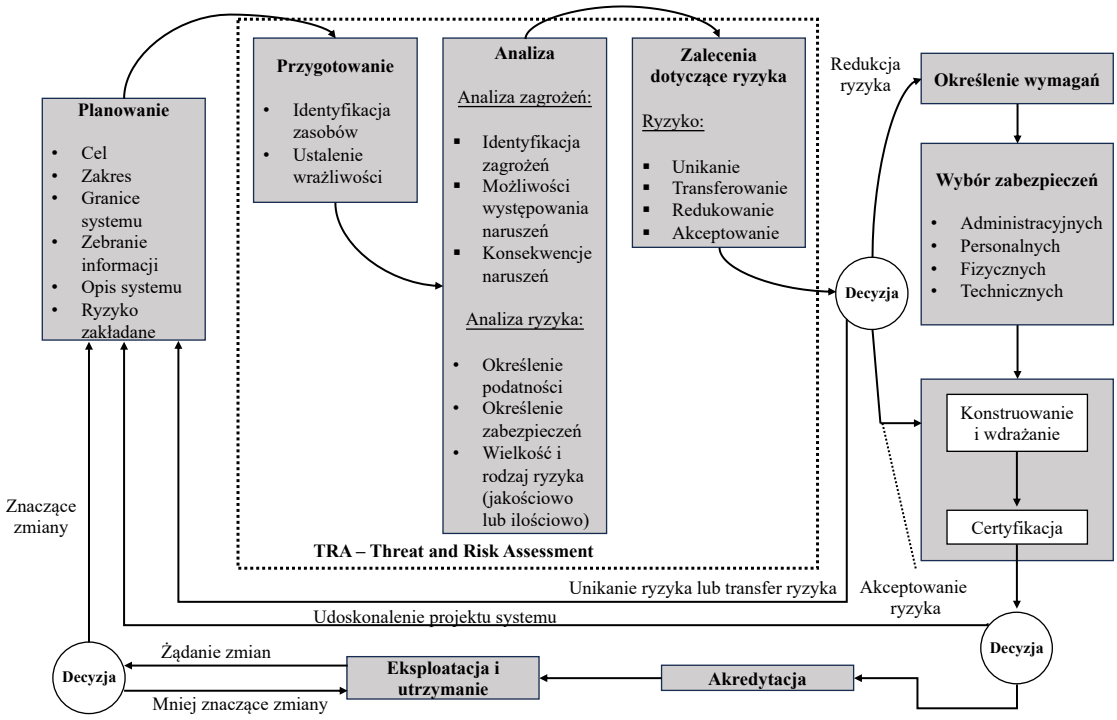
[210] Ibidem.

b) dane chronione na pierwszym poziomie – przeznaczone do użytku wewnątrzorganizacyjnego,

c) dane ochrony podstawowej – publicznie dostępne[211].

Model TISM pozwala na systematyczne ustrukturyzowanie relacji między działaniami biznesowymi a operacjami systemów informatycznych w organizacji. Metoda ta znajduje zastosowanie głównie w sektorze prywatnym, podczas gdy w sektorze publicznym jest stosowana znacznie rzadziej.

Organizacja rządowa Kanady, CSE (*Communications Security Establishment*), wprowadziła unikalną metodologię do zarządzania ryzykiem w obszarze zarządzania bezpieczeństwem informacji. Kluczowym składnikiem tej metodologii jest system oceny zagrożeń i ryzyka, znanym jako TRA (*Threat and Risk Assessment*)[212], który jest wykorzystywany na wszystkich etapach cyklu życia systemu, począwszy od fazy planowania aż do fazy eksploatacji. Schematyczne przedstawienie zaawansowanej i ostatecznej wersji systemu zarządzania TRA zostało dokładnie opisane na rysunku nr 19.



Rysunek 19 Metoda TRA do oszacowania ryzyka i zarządzania systemem
Źródło: opracowano na podstawie A. Białas, Bezpieczeństwo informacji…, op. cit., s. 126.

[211] Ibidem, s. 178.
[212] *Harmonized Threat and Risk Assessment (TRA) Methodology*, Communications Security Establishment, Ottawa 2007, https://www.cyber.gc.ca/sites/default/files/cyber/publications/tra-emr-1-e.pdf [dostęp 22.02.2024 r.].

Przerywana linia podkreśla etapy metodyki TRA, polegającej na ocenie zagrożeń i związanego z nimi ryzyka, wraz z proponowaniem odpowiednich środków ochronnych. Na etapie wstępnym planowania rozważa się:

a) definiowanie celów zarządzania ryzykiem,
b) określanie granic i zakresu obszaru zarządzania,
c) zbieranie danych historycznych o incydentach i słabościach,
d) opracowywanie opisu systemu,
e) ustalanie oczekiwanego minimalnego poziomu ryzyka, akceptowalnego dla systemu, rozumianego jako ryzyko minimalne, przy którym system działa bezpiecznie.

Główne cele TRA obejmują: rozpoznanie kluczowych aktywów, wskazanie potencjalnych metod ich kompromitacji przez zagrożenia, analizę powiązanego ryzyka oraz formułowanie zaleceń dotyczących zarządzania tym ryzykiem na różnych etapach cyklu życia.

Pierwszy etap przygotowania TRA skupia się na rozpoznawaniu aktywów oraz ocenie ich podatności na ryzyko, zilustrowanej przez potencjalną stratę poufności, integralności oraz dostępności danych. Przypisuje się również wartość kosztu wymiany dla każdego z tych zasobów. Ten proces ma na celu ustalenie wagi poszczególnych zasobów w kontekście ich znaczenia dla funkcji biznesowych, które charakteryzują się zróżnicowanym stopniem krytyczności[213].

W trakcie analizy TRA identyfikowane są potencjalne źródła zagrożeń, słabości oraz istniejące mechanizmy ochronne. Opracowywane są scenariusze ryzyka, przy czym ryzyko oceniane jest na podstawie prawdopodobieństwa wystąpienia określonych zdarzeń oraz ich potencjalnych konsekwencji. Analiza może przyjąć formę zarówno jakościową, jak i ilościową.

Na podstawie analizy, w tym oceny skuteczności obecnych mechanizmów ochrony, podejmuje się działania mające na celu zmniejszenie ryzyka. Działania te obejmują usprawnienie systemu, wprowadzanie nowych zabezpieczeń lub ich modyfikację, a także strategie omijania ryzyka przez zmianę lokalizacji zasobów lub jego przeniesienie, na przykład poprzez ubezpieczenie. Proces ten prowadzi do opracowania rekomendacji dla zarządu dotyczących sposobów zarządzania ryzykiem, z uwzględnieniem kosztów tych działań. W przypadku decyzji o zminimalizowaniu określonego ryzyka określa się wymogi dla mechanizmu ochronnego odpowiedzialnego za tę redukcję. Wymagania te mogą dotyczyć różnych metod zabezpieczeń, które różnią się kosztami – aspekt ważny dla decyzji kierownictwa. Wyselekcjonowanie odpowiednich zabezpieczeń prowadzi do rozpoczęcia procesu ich implementacji, który powinien zostać zakończony certyfikacją[214].

[213] A. Białas, *Bezpieczeństwo informacji…*, op. cit., s. 127.
[214] *Harmonized Threat and Risk…,* op. cit.

Certyfikacja systemu obejmuje serię kompleksowych ocen, w tym sprawdzenie zgodności zabezpieczeń z ustalonymi wymogami i strategią ochrony, testowanie ich efektywności, analizę technicznych aspektów bezpieczeństwa pod kątem wydajności i niezawodności, ocenę zabezpieczeń personalnych, materialnych i organizacyjnych, oraz porównanie aktualnego poziomu ryzyka z tym, który był przewidziany dla systemu. Decyzja o akredytacji, czyli zezwoleniu na użytkowanie systemu, jest oparta na rezultatach tych badań. W trakcie użytkowania systemu przeprowadzane są działania mające na celu jego ciągłe utrzymanie, w tym stałe zarządzanie ryzykiem, kontrola konfiguracji, monitoring zabezpieczeń, a także audyt i przegląd ryzyka[215].

Proces utrzymania powinien obejmować procedury dotyczące bezpiecznego usuwania informacji poufnych z zasobów przeznaczonych do likwidacji, takich jak nośniki danych, urządzenia czy komputery. Istotne jest również zarządzanie zmianami w systemie, które mogą wpłynąć na bezpieczeństwo. Zmiany takie mogą wymagać przeprowadzenia nowej oceny ryzyka przed ich wdrożeniem. Drobniejsze modyfikacje zazwyczaj pociągają za sobą jedynie niezbędne działania korygujące w ramach bieżącego utrzymania systemu[216].

W kontekście zarządzania IT w przedsiębiorstwie, metodyka COBIT[217] opracowana przez ISACA stanowi kluczowe narzędzie umożliwiające optymalizację governance IT. Poprzez integrację z międzynarodowymi standardami i najlepszymi praktykami branżowymi, COBIT umożliwia profesjonalistom nie tylko ulepszenie systemu zarządzania, ale i osiągnięcie lepszych wyników organizacyjnych w obszarach takich jak governance, zarządzanie ryzykiem, cyberbezpieczeństwo, kontrole i budowanie cyfrowego zaufania. Zatem, strategiczne wykorzystanie COBIT w ramach zarządzania IT może znacząco przyczynić się do wzrostu efektywności operacyjnej oraz zapewnienia zrównoważonego rozwoju przedsiębiorstwa w warunkach nieustannie zmieniającego się środowiska cyfrowego.

COBIT stanowi globalnie uznany zbiór najlepszych praktyk dotyczących oceny i gwarancji bezpieczeństwa informacji, został stworzony i jest nadal rozwijany przez ISACA, organizację skupiającą się na audycie, bezpieczeństwie systemów informacyjnych i zarządzaniu informatyką. W ramach swojej działalności, ISACA opracowuje metodologie, organizuje kursy szkoleniowe i programy certyfikacji. Wśród najbardziej rozpoznawalnych inicjatyw ISACA znajdują się:

a) programy certyfikacji zawodowej, takie jak:
    a. Certified in the Governance of Enterprise IT® (CGEIT®),

[215] Ibidem.
[216] A. Białas, *Bezpieczeństwo informacji…*, op. cit., s. 127-128.
[217] *COBIT An ISACA Framework*, ISACA, https://www.isaca.org/resources/cobit [dostęp 22.02.2024 r.].

b. Certified Information Systems Auditor® (CISA®),
c. Certified Information Security Manager® (CISM®),
d. Certified in Risk and Information Systems ControlTM (CRISCTM),

b) publikacja pierwszej edycji COBITTM w 1996 roku, czyli Control Objectives for Information and Related Technology.

W roku 2017 została udostępniona wersja 5.0 COBIT, będąca biznesowym modelem zarządzania IT w przedsiębiorstwie, składającym się z kilku kluczowych elementów:

a) COBIT 5 jako podstawowa metodyka,
b) Seria przewodników poświęconych „czynnikom umożliwiającym", które szczegółowo omawiają aspekty zarządzania i nadzoru, w tym przewodniki dotyczące procesów i informacji wspierających COBIT 5,
c) Specjalistyczne przewodniki, takie jak COBIT 5 dotyczące Implementacji, Bezpieczeństwa Informacji, Audytu i Ryzyka, oprócz innych,
d) Platforma współpracy online mająca na celu wsparcie użytkowania COBIT 5[218].

Podstawę COBIT 5 stanowi pięć zasad kierujących zarządzaniem IT, które obejmują spełnianie potrzeb interesariuszy, integrację wszystkich aspektów działalności przedsiębiorstwa, stosowanie jednej, zintegrowanej metodyki, przyjęcie holistycznego podejścia oraz rozgraniczenie nadzoru od zarządzania. Dodatkowo, COBIT 5 wskazuje na siedem kluczowych *czynników umożliwiających*[219], wspomagających wprowadzenie kompleksowego systemu zarządzania IT, które obejmują: zasady, polityki i metodyki; procesy; struktury organizacyjne; kulturę, etykę i zachowanie; informacje; usługi, infrastrukturę i aplikacje oraz kompetencje ludzkie. Te czynniki są wspierane przez cztery wspólne wymiary, takie jak interesariusze, cele, cykl życia i dobre praktyki.

W COBIT 5 znajdują się także szczegółowe wzorce organizacyjno-techniczne, klasyfikacje, wskaźniki i kryteria, które pomagają w klarownym przedstawieniu złożonych relacji między zarządzaniem biznesem a wsparciem IT, co sprzyja dokładnej ocenie stanu ładu informatycznego. Te elementy, zdefiniowane w poprzedniej COBIT, zawierają opis czterech domen informatycznych, 34 procesów IT, celów kontrolnych oraz innych aspektów kluczowych dla oceny i zarządzania IT.

W kontekście adaptacji i wdrożenia systemu zarządzania w erę cyfrową, identyfikacja i realizacja celów przedsiębiorstwa poprzez skuteczny system zarządzania staje się imperatywem strategicznym. Metodyka COBIT oferuje ramy wspierające integrację najlepszych praktyk branżowych z procesami zarządzania przedsiębiorstwem, co pozwala na

[218] K. Liderman, *Bezpieczeństwo informacyjne…,* op. cit., s. 259-261.
[219] Ibidem.

optymalizację wartości generowanej przez IT. Kluczowe aspekty takie jak zrozumienie celów przedsiębiorstwa, określenie zakresu i obszaru implementacji, identyfikacja i integracja celów COBIT oraz innych ram czy standardów, określenie zaangażowanych interesariuszy, planowanie czasowe oraz opracowanie i realizacja strategii implementacji stanowią fundament skutecznego wdrożenia systemu zarządzania. Ponadto, wdrożenie systemu zarządzania wydajnością i paneli kontrolnych do monitorowania realizacji i oceny efektywności wdrożenia, zapewnia ciągłą ocenę osiąganych wyników i umożliwia bieżące dostosowanie strategii do dynamicznie zmieniającego się środowiska[220].

W niniejszym rozdziale scharakteryzowano istotę zarządzania bezpieczeństwem informacyjnym w przedsiębiorstwie, prezentując główne modele i metody stosowane w tej dziedzinie, takie jak ISO/IEC 27001, TISM, TRA oraz COBIT. Modele te oferują kompleksowe podejścia do zarządzania bezpieczeństwem informacji, koncentrując się na strukturze organizacyjnej, klasyfikacji danych, zarządzaniu ryzykiem oraz kontrolach technicznych i proceduralnych. Omówiono również kluczowe procesy, takie jak planowanie, wdrażanie, monitorowanie i doskonalenie działań związanych z bezpieczeństwem informacji, co pozwala organizacjom skutecznie reagować na zagrożenia i minimalizować ryzyko utraty danych.

W oparciu o hipotezę szczegółową: *stosowanie odpowiednich standardów i norm w zarządzaniu bezpieczeństwem informacji, pozwala na skuteczne rozpoznawanie zagrożeń, kształtując poziom ochrony danych oraz tajemnicy przedsiębiorstwa*, niniejszy podrozdział potwierdza kilka kluczowych elementów tej hipotezy:

a) rozpoznawanie zagrożeń – modele, takie jak ISO/IEC 27001 oraz TRA, kładą duży nacisk na systematyczne zarządzanie ryzykiem, które obejmuje identyfikację zagrożeń oraz ich analizę. TRA wspiera ten proces przez dokładną ocenę ryzyka oraz proponowanie środków ochronnych na podstawie zidentyfikowanych zagrożeń, co odpowiada założeniom hipotezy,
b) kształtowanie poziomu ochrony danych – modele opisane w podrozdziale (np. ISO/IEC 27001 i COBIT) wskazują na tworzenie zintegrowanego systemu zarządzania, który obejmuje zarówno aspekty techniczne, jak i proceduralne. Zastosowanie procedur ochronnych, audytów oraz określenie polityk bezpieczeństwa w ramach tych modeli pomaga organizacjom utrzymać wysoki poziom ochrony danych, odpowiadając na zmieniające się zagrożenia,

[220] *Seven Tips for Implementing COBIT*, ISACA, https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/infographics/seven-tips-cobit-infographic_1223.pdf [dostęp 22.02.2024 r.].

c) ochrona tajemnicy przedsiębiorstwa – modele TISM oraz COBIT, które uwzględniają klasyfikację danych oraz rozbudowaną strukturę organizacyjną, wspierają ochronę informacji wrażliwych, takich jak tajemnica przedsiębiorstwa. Poprzez definiowanie dostępu na podstawie roli zawodowej oraz stosowanie odpowiednich poziomów zabezpieczeń, organizacje mogą skutecznie chronić swoje kluczowe zasoby.

Podsumowując, podrozdział dostarcza dowodów na to, że stosowanie uznanych standardów i norm pozwala na skuteczne rozpoznawanie zagrożeń i kształtowanie systemu ochrony informacji, co jest zgodne z założeniami hipotezy szczegółowej.

Rozdział 3. SZPIEGOSTWO KORPORACYJNE I JEGO SPECYFIKA W ASPEKCIE ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI PRZEDSIĘBIORSTWA SEKTORA TECHNOLOGII INFORMACYJNO-KOMUNIKACYJNYCH

3.1 Zarządzanie bezpieczeństwem informacji przedsiębiorstwa sektora ICT a problematyka szpiegostwa przemysłowego i szpiegostwa gospodarczego

Dzisiejszy szybko zmieniający się świat biznesu, podchodzi do kwestii związanych z bezpieczeństwem organizacji w kontekście informacyjnym z wielką uwagą. W tym kontekście, analiza dwóch kluczowych pojęć – szpiegostwa przemysłowego (ang. *industrial espionage*) oraz szpiegostwa gospodarczego (ang. *economic espionage*) staje się niezbędna dla zrozumienia zarówno ich wpływu na strategie konkurencyjne przedsiębiorstw, jak i na ich bezpieczeństwo informacyjne. Niniejszy rozdział ma na celu zbadanie tych praktyk, podkreślając różnice w ich podejściach, etyce i metodach, a także ich wpływ na ochronę i wykorzystanie informacji strategicznych.

W kontekście bezpieczeństwa informacyjnego, zrozumienie i odpowiednie zarządzanie ryzykiem związanym z obiema praktykami jest niezbędne dla utrzymania przewagi konkurencyjnej i ochrony przedsiębiorstwa przed potencjalnymi zagrożeniami[221]. W dalszej części przedstawiona zostanie szczegółowa analizy obu praktyk oraz ich implikacji dla bezpieczeństwa przedsiębiorstw w kontekście globalnej rywalizacji.

Takie podejście pozwala na kompleksowe zrozumienie, jak organizacje mogą efektywnie nawigować w złożonym i często ryzykownym środowisku biznesowym, maksymalizując korzyści płynące z legalnych praktyk informacyjnych, jednocześnie minimalizując ryzyko związane z nielegalnymi działaniami konkurencji[222]. Jednakże wciąż otwartą pozostaje kwestia właściwego zdefiniowana obu przedstawionych pojęć. Prawidłowe zrozumienie istoty obu praktyk stanowić będzie podstawę do dalszych rozważań dotyczących szpiegostwa korporacyjnego.

W obliczu rosnącej globalizacji i zaostrzającej się konkurencji na rynkach międzynarodowych, kwestia pozyskiwania i ochrony informacji gospodarczych nabiera szczególnego znaczenia. W tym kontekście, pojęcie szpiegostwa gospodarczego staje się przedmiotem zainteresowania nie tylko dla przedsiębiorców i menedżerów, ale także dla

[221] G. Mąkosa, *Zarządzanie ryzykiem jako determinanta cyberbezpieczeństwa*, Nowoczesne Systemy Zarządzania Instytut Organizacji i Zarządzania Zeszyt 14 (2019) nr 3 (lipiec-wrzesień), s. 74.
[222] K. Łusiakowski, *Model trzech linii w systemie zarządzania ryzykiem przedsiębiorstwa*, Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie, Nr 55 (2024), DOI: 10.17512/znpcz.2024.3.09, s. 118 i 124.

naukowców, analityków i decydentów politycznych. Szpiegostwo gospodarcze, będące jednym z najbardziej kontrowersyjnych i dyskutowanych zagadnień we współczesnym świecie biznesu, wywołuje szereg pytań dotyczących etyki, legalności oraz wpływu na stabilność i rozwój gospodarczy.

Powyższe, stanowi wstęp dla głębszej analizy i zrozumienia różnorodnych definicji szpiegostwa gospodarczego, które zostały zebrane w ramach prowadzonych badań. Przedstawienie tych definicji umożliwi nie tylko dokładniejsze określenie samego zjawiska, ale także pozwoli na zidentyfikowanie kluczowych aspektów, z którymi wiąże się ta problematyka. W kontekście dynamicznie zmieniającego się środowiska informacyjnego, zrozumienie granic między legalnymi a nielegalnymi działaniami w obszarze pozyskiwania informacji staje się kluczowe dla zapewnienia etycznych i zrównoważonych praktyk biznesowych. W tabeli nr 11 przedstawione zostały wybrane przez autora definicje pojęcia szpiegostwa gospodarczego.

Tabela 11 Wybrane definicje terminu szpiegostwo gospodarcze

Lp.	Autor	Definicja
1.	K. S. Søilen[223]	Działania rządów skoncentrowane na akumulacji danych, uzurpacji tajemnic komercyjnych oraz nieuprawnionym przejmowaniu know-how,
2.	R. E. Wagner[224]	Działalność wywiadowcza polegająca na celowym pozyskiwaniu tajemnic handlowych od przedsiębiorstw krajowych lub instytucji rządowych, z zamiarem świadomego przyniesienia korzyści państwu obcemu. Jest to forma szpiegostwa, w której głównym celem jest uzyskanie przewagi ekonomicznej dla państwa beneficjenta poprzez wykorzystanie pozyskanych nielegalnie informacji strategicznych,
3.	MSW Austrii[225]	Działania podejmowane przez obce służby wywiadowcze, które polegają na inwigilacji firm austriackich (lub ogólnie firm z danego kraju) z zamiarem pozyskania informacji strategicznych, mających na celu wzmocnienie gospodarki kraju, z którego te służby pochodzą. Jest to forma działalności wywiadowczej, która przyczynia się do transferu wartościowych danych gospodarczych, wiedzy technologicznej lub innych tajemnic handlowych, bezpośrednio wpływając na rozwój ekonomiczny kraju beneficjenta.

[223] K. S. Søile, *Economic and industrial espionage at the start of the 21 st century – Status quaestionis*, Journal of Intelligence Studies in Business Vol. 6, No. 3 (2016), s. 52.
[224] R. E. Wagner, *Bailouts and the potential for distortion of federal criminal law: Industrial espionage and beyond*, Tulane Law Review, 86(5) 2012, s. 1040.
[225] C. Konopatsch, *Fighting industrial and economic espionage through criminal law: lessons to be learned from Austria and Switzerland*, Security Journal Volume 33 (2020), https://doi.org/10.1057/s41284-019-00200-x, s. 86-87.

Lp.	Autor	Definicja
4.	R. W. Bellaby[226]	W szerokim rozumieniu, obejmuje tajne zbieranie informacji gospodarczych zarówno od innych państw, jak i prywatnych podmiotów gospodarczych jako narzędzie polityki państwowej, często przedstawiane jako forma (gospodarczego) bezpieczeństwa narodowego. Może to obejmować dostęp i zbieranie tajnych informacji o operacjach, strategii i zasobach celu,
5.	*Economic Espionage Ac*t – USA[227]	Szpiegostwo gospodarcze to działalność polegająca na świadomym i nieuprawnionym pozyskiwaniu tajemnic handlowych z zamiarem przyniesienia korzyści obcym rządom, instytucjom lub agentom. Obejmuje to nie tylko kradzież, przywłaszczenie, ukrywanie lub oszukańcze uzyskiwanie informacji o charakterze strategicznym, ale również nieautoryzowane kopiowanie, duplikowanie, dokumentowanie, niszczenie lub przekazywanie takich danych. Ponadto zakres szpiegostwa gospodarczego rozciąga się na otrzymywanie, kupowanie lub posiadanie tajemnic handlowych wiedząc, że zostały one pozyskane nielegalnie. Działalność ta obejmuje również próby popełnienia wymienionych przestępstw oraz spiskowanie w celu ich realizacji,
6.	S. D. Porteous[228]	Tajne lub nielegalne próby obcych interesów mające na celu wspieranie ich interesów gospodarczych poprzez pozyskiwanie wywiadu gospodarczego, który mógłby być wykorzystany do sabotażu lub w inny sposób ingerować w bezpieczeństwo gospodarcze innego kraju,
7.	R. M. Fort[229]	Pozyskiwanie za pomocą tajnych środków informacji dotyczących gospodarki, handlu i/lub własności intelektualnej przez tajną agencję/służbę, która używa tajnych źródeł i metod.

Źródło: K. Kozłowski, Ewolucja szpiegostwa biznesowego: Od konkurencji przemysłowej do cyberprzestrzeni, Management and Quality – Zarządzanie i Jakość, Vol. 6 No 1 (2024), s. 78-79.

Analiza przedstawionych powyżej definicji terminu szpiegostwo gospodarcze pozwala wyodrębnić kluczowe elementy tego zjawiska:

a) **działania rządów i obcych służb wywiadowczych:** szpiegostwo gospodarcze często jest inicjowane przez państwa lub ich służby wywiadowcze, mające na celu wzmocnienie własnej pozycji gospodarczej na arenie międzynarodowej,

[226] R. W. Bellaby, *The Ethics of Economic Espionage*, Ethics & International Affairs, 37 (2023), s. 120.
[227] *Economic Espionage Act of 1996*, PUBLIC LAW 104–294—OCT. 11, 1996, https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf [dostęp 24.02.2024 r.].
[228] S. D. Porteous, *Economic/Commercial Interests and the World's Intelligence Services: A Canadian Perspective*, International Journal of Intelligence and Counterintelligence Vol. 8, No. 3, 1995, s. 297.
[229] R. M. Fort, *Economic Espionage*, W: *U. S. Intelligence at the Crossroads: Agendas for Reforms* (red.) R. Godson, E. May, G. Schmitt, Wydawnictwo Brassey's, Waszyngton 1995, s. 181.

b) **celowe pozyskiwanie informacji:** działalność ta polega na świadomym i celowym zbieraniu tajemnic handlowych, danych gospodarczych oraz know-how, które nie są publicznie dostępne,
c) **nielegalne metody pozyskiwania danych:** szpiegostwo gospodarcze wykorzystuje tajne, nieuprawnione lub nielegalne środki do uzyskania informacji, w tym kradzież, oszustwo, nieautoryzowane kopiowanie czy spiskowanie,
d) **przyniesienie korzyści obcym państwom lub podmiotom:** głównym celem jest przekazanie pozyskanych informacji obcym rządom, instytucjom lub agentom, co może bezpośrednio wpływać na bezpieczeństwo gospodarcze innego kraju,
e) **szeroki zakres informacji docelowych:** szpiegostwo może dotyczyć różnych aspektów działalności gospodarczej, w tym operacji, strategii, zasobów, własności intelektualnej oraz handlu[230].

Działania te mogą obejmować różnorodne praktyki, od kradzieży po spiskowanie i mają na celu przyniesienie korzyści określonym państwom, instytucjom lub agentom na szkodę konkurencji i innowacyjności globalnej gospodarki.

Drugą z omawianych metod nielegalnego pozyskiwania informacji na temat przedsiębiorstwa jest szpiegostwo przemysłowe, które przez wielu badaczy i ekspertów mylnie utożsamiane jest z omówionym powyżej szpiegostwem gospodarczym. W celu pełnego wyjaśnienia samej istoty przytoczonej metody oraz wskazania podobieństw i różnic, autor przedstawił w tabeli nr 12 wybrane definicje terminu szpiegostwo przemysłowe.

Tabela 12 Wybrane definicje terminu szpiegostwo przemysłowe

Lp.	Autor	Definicja
1.	R. E. Wagner[231]	Szpiegostwo przemysłowe jest tożsame ze szpiegostwem gospodarczym, z tą różnicą, że zamiast przynosić korzyści obcemu rządowi, przynosi korzyści innej prywatnej jednostce,
2.	Rząd USA[232]	Szpiegostwo przemysłowe definiuje się jako działalność prowadzoną przez obcy rząd lub przez obcą firmę przy bezpośrednim wsparciu obcego rządu przeciwko prywatnej amerykańskiej spółce w celu pozyskania tajemnic handlowych,
3.	K. D. Mitnick, W. L. Simon[233]	Szpiegostwo przemysłowe definiowane jest jako kradzież tajemnic handlowych konkurencyjnej organizacji,

[230] K. Kozłowski*, Ewolucja szpiegostwa biznesowego…,* op. cit., s. 84.
[231] R. E. Wagner, *Bailouts and the potential…,* op. cit.
[232] National Counterintelligence and Security Center (NCSC), *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, Waszyngton 2000, https://fas.org/irp/ops/ci/docs/fecie_fy00.pdf [dostęp 26.02.2024 r.].
[233] K. D. Mitnick, W. L. Simon, *Sztuka podstępu*, Wydawnictwo Helion, Gliwice 2016, s. 255.

Lp.	Autor	Definicja
4.	B. A. Garner[234]	Szpiegostwo przemysłowe definiowane jest jako sytuacja, w której jedna firma szpieguje inną w celu kradzieży tajemnic handlowych lub innych informacji własnościowych,
5.	K. Surdyk, R. Nogacki[235]	Szpiegostwo przemysłowe to niejawne i nielegalne działania związane z nwigilacją konkurencji w celu uzyskania przewagi rynkowej. Stanowi rodzaj działań wywiadowczych prowadzonych w celach komercyjnych, w odróżnieniu od tych działań wywiadowczych, które prowadzone są przez państwa dla zabezpieczenia swoich interesów narodowych,
6.	D. A. Jameson[236]	Szpiegostwo przemysłowe odnosi się do tajnego pozyskiwania tajemnic handlowych przedsiębiorstwa lub innych poufnych informacji bez zgody i w niecnych celach.
7.	I. Sutherland[237]	Szpiegostwo przemysłowe w środowisku wysokich technologii może być skoncentrowane na zdobywaniu informacji dotyczących konkretnej organizacji lub może stanowić bardziej ogólne zbieranie przydatnych informacji korporacyjnych, które mogą być sprzedane zainteresowanym grupom lub osobom,
8.	A. Jones[238]	Szpiegostwo przemysłowe to działalność szpiegowska prowadzona w celach komercyjnych, a nie bezpieczeństwa narodowego. W najprostszych przypadkach są to korporacje szpiegujące konkurentów, aby uzyskać przewagę rynkową, co prawdopodobnie wiąże się z kradzieżą (lub kopiowaniem) tajemnic handlowych i/lub poufnych lub wartościowych informacji do wykorzystania,
9,	A. Latosińska[239]	Szpiegostwo przemysłowe to działania wywiadowcze skierowane przeciwko przedsiębiorstwom, mające na celu pozyskanie tajnych informacji gospodarczych.

Źródło: K. Kozłowski, Ewolucja szpiegostwa biznesowego…, op. cit., s. 80.

Fundamentalne składniki konceptualizacji szpiegostwa przemysłowego, jak zostały zaprezentowane w analizowanym materiale, obejmują:

[234] B. A. Garner, *Black's Law Dictionary*, Thomson Reuters, Toronto 2019, s. 1651.
[235] K. Surdyk, R. Nogacki, *Szpiegostwo przemysłowe w Polsce i na świecie*, PWG Skarbiec, https://www.wywiad-gospodarczy.pl/szpiegostwo-przemyslowe-polska-swiat.html [dostęp 26.02.2024 r.].
[236] D. A. Jameson, *The rhetoric of industrial espionage: the case of Starwood v. Hilton*, Business Communication Quarterly, 74(3) 2011, doi:10.1177/1080569911413811, s. 290.
[237] I. Sutherland, *Industrial espionage from residual data: risks and countermeasures*. School of Computer and Information Science, Perth 2008, doi:10.4225/75/57b2771540cc2, s. 3.
[238] A. Jones, *Industrial espionage in a hi-tech world*, Computer Fraud & Security, Volume 2008, Issue 1 2008, doi:10.1016/S1361-3723(08)70010-1, s. 7.
[239] A. Latosińska, *Wywiad gospodarczy a bezpieczeństwo ekonomiczne państwa*, W: *Wywiad i kontrwywiad gospodarczy Materiały z konferencji naukowych* (red.) H. Szafran, J. W. Wójcik, Wydawnictwo Wszechnicy Polskiej, Warszawa 2019, s. 31.

a) **odbiorcy korzyści:** w przeciwieństwie do szpiegostwa gospodarczego, korzyści ze szpiegostwa przemysłowego przynoszone są prywatnym jednostkom, a nie obcym rządom,
b) **źródła działania:** działalność może być inicjowana przez obce rządy lub organizacje, czasami przy ich bezpośrednim wsparciu,
c) **cel działania:** pozyskiwanie tajemnic handlowych lub innych poufnych informacji własnościowych,
d) **metody działania:** działania niejawne i nielegalne, w tym kradzież, kopiowanie, oraz tajne pozyskiwanie informacji bez zgody,
e) **zakres informacji:** dotyczy zarówno konkretnych informacji o konkretnej organizacji, jak i ogólnie przydatnych informacji korporacyjnych, które mogą być sprzedane.
f) **cel działania:** prowadzone w celach komercyjnych, głównie dla uzyskania przewagi rynkowej nad konkurentami[240].

Działalność ta może być inicjowana przez podmioty krajowe lub zagraniczne, w tym obce rządy lub organizacje, i ma na celu przyniesienie korzyści prywatnym jednostkom poprzez uzyskanie nieuprawnionego dostępu do wartościowych danych, co z kolei ma przyczynić się do zyskania przewagi rynkowej. Szpiegostwo przemysłowe stanowi zagrożenie dla bezpieczeństwa gospodarczego przedsiębiorstw, podważając uczciwą konkurencję i innowacyjność.

Analiza przytoczonych w tekście definicji szpiegostwa gospodarczego oraz szpiegostwa przemysłowego umożliwia identyfikację fundamentalnych rozbieżności i analogii między tymi dwoma pojęciami, które zostały zaprezentowane w tabeli nr 14.

Tabela 13 Porównanie szpiegostwa gospodarczego i szpiegostwa przemysłowego - podobieństwa i różnice

Podobieństwa	Różnice
Zarówno szpiegostwo gospodarcze, jak i przemysłowe polegają na świadomym i celowym zbieraniu tajemnic handlowych oraz innych danych strategicznych,	Szpiegostwo gospodarcze przynosi korzyści państwom lub instytucjom zagranicznym, natomiast szpiegostwo przemysłowe korzysta na rzecz innych prywatnych jednostek, niekoniecznie związanych z jakimkolwiek rządem,
Oba rodzaje szpiegostwa wykorzystują tajne, nieuprawnione lub nielegalne środki do uzyskania informacji, w tym kradzież, oszustwo, i nieautoryzowane kopiowanie,	Szpiegostwo gospodarcze jest często inicjowane przez państwa lub ich służby wywiadowcze, podczas gdy szpiegostwo przemysłowe może być prowadzone przez organizacje prywatne, czasami z wsparciem rządów,

[240] K. Kozłowski*, Ewolucja szpiegostwa biznesowego…,* op. cit., s. 84-85.

W obu przypadkach działania mogą dotyczyć szerokiego spektrum informacji, od tajemnic handlowych, przez dane gospodarcze, po know-how.	Głównym celem szpiegostwa gospodarczego jest wzmocnienie pozycji gospodarczej państwa beneficjenta, podczas gdy szpiegostwo przemysłowe ma na celu uzyskanie przewagi rynkowej przez prywatne podmioty.

Źródło: K. Kozłowski, Ewolucja szpiegostwa biznesowego…, op. cit., s. 86.

Opierając się na przeprowadzonej analizie, uniwersalna definicja omawianych terminów proponowana przez autora, przedstawia się następująco:

a) **szpiegostwo gospodarcze** to zorganizowana działalność wywiadowcza, prowadzona przez państwa lub ich służby, skierowana na nielegalne pozyskiwanie tajemnic handlowych, danych gospodarczych oraz know-how od przedsiębiorstw. Działalność ta ma na celu wzmocnienie gospodarki państwa beneficjenta, potencjalnie osłabiając bezpieczeństwo ekonomiczne innych krajów,
b) **szpiegostwo przemysłowe** to działalność wywiadowcza prowadzona w celach komercyjnych, obejmująca nielegalne i tajne pozyskiwanie tajemnic handlowych oraz innych poufnych informacji własnościowych od konkurencyjnych przedsiębiorstw. Ma na celu przyniesienie korzyści prywatnym jednostkom, prowadząc do zyskania przewagi rynkowej i podważając uczciwą konkurencję[241].

Prezentacja zagadnienia w ten sposób stanowi solidną podstawę do dalszych rozważań nad pojęciem szpiegostwa korporacyjnego, które można uznać za specyficzną formę szpiegostwa przemysłowego, lecz często realizowaną z jeszcze większą precyzją i skierowaną na bardzo szczegółowe cele strategiczne wewnątrz sektora korporacyjnego. Rozważanie tego tematu pozwoli na głębsze zrozumienie mechanizmów ochrony danych w warunkach intensyfikacji konkurencji i technologicznych wyzwań współczesnego świata biznesu.

W niniejszym podrozdziale omówiono zagadnienia związane z zarządzaniem bezpieczeństwem w przedsiębiorstwach sektora ICT, ze szczególnym uwzględnieniem problematyki szpiegostwa gospodarczego i przemysłowego. Autor wyjaśnia różnice między szpiegostwem gospodarczym, które jest zazwyczaj inicjowane przez państwa i ma na celu wzmocnienie ich gospodarki, a szpiegostwem przemysłowym, prowadzonym przez prywatne podmioty w celu uzyskania przewagi rynkowej. Oba te zjawiska opierają się na tajnym, nieuprawnionym lub nielegalnym pozyskiwaniu danych, w tym tajemnic handlowych i know-how, które nie są publicznie dostępne. W rozdziale zebrano definicje tych praktyk oraz

[241] K. Kozłowski*, Ewolucja szpiegostwa biznesowego…,* op. cit., s. 87.

przeanalizowano ich wpływ na uczciwość konkurencji i bezpieczeństwo gospodarcze przedsiębiorstw.

W kontekście współczesnej gospodarki globalnej oraz zaostrzonej konkurencji na rynkach międzynarodowych, zrozumienie i rozróżnienie między szpiegostwem gospodarczym a przemysłowym okazuje się kluczowe. Wyodrębniono również kluczowe elementy obu praktyk, takie jak odbiorcy korzyści, cele działania, metody pozyskiwania informacji oraz zakres docelowych informacji. Ponadto, rozważono problematykę szpiegostwa korporacyjnego jako specyficznej formy szpiegostwa przemysłowego, która charakteryzuje się precyzją i skupieniem na wybranych celach strategicznych w ramach korporacyjnych działań wywiadowczych.

Hipoteza szczegółowa: *szpiegostwo korporacyjne stawia przed zarządzaniem bezpieczeństwem przedsiębiorstwa konieczność przeciwdziałania środkom i metodom dostępu do danych oraz pozyskiwania informacji w celu zdobycia przewagi konkurencyjnej*, znajduje potwierdzenie w kilku aspektach omawianego podrozdziału:

a) przeciwdziałanie metodom dostępu do danych – podkreślono znaczenie identyfikacji i ochrony informacji strategicznych przedsiębiorstw przed nieuprawnionym pozyskiwaniem przez konkurencję. Zarządzanie bezpieczeństwem przedsiębiorstwa w sektorze ICT obejmuje odpowiednie zabezpieczenia, które mają na celu przeciwdziałanie takim działaniom,
b) rozróżnienie metod pozyskiwania informacji – wyróżniono metody stosowane w szpiegostwie gospodarczym i przemysłowym, takie jak kradzież, kopiowanie czy oszustwo. Wskazanie tych metod stanowi fundament do tworzenia środków obronnych, umożliwiających przeciwdziałanie zagrożeniom ze strony konkurencji,
c) cel zdobycia przewagi konkurencyjnej – wykazano, że szpiegostwo przemysłowe i gospodarcze mają na celu zdobycie przewagi rynkowej lub gospodarczej. Podrozdział potwierdza zatem, że przeciwdziałanie tym zagrożeniom jest niezbędne dla ochrony konkurencyjności przedsiębiorstw oraz zabezpieczenia ich tajemnic handlowych.

Podsumowując, podrozdział częściowo potwierdza hipotezę szczegółową, szczególnie w zakresie konieczności zarządzania bezpieczeństwem informacji w kontekście zagrożeń wynikających ze szpiegostwa korporacyjnego oraz podejmowania działań zabezpieczających przed metodami stosowanymi w pozyskiwaniu strategicznych danych.

3.2 Charakterystyka pojęcia szpiegostwa korporacyjnego w ramach zarządzania przedsiębiorstwem sektora ICT

Adaptacja modelu ekonomicznego neoliberalizmu i strategii deregulacyjnych przez główne gospodarki i rynki finansowe w latach osiemdziesiątych, w połączeniu z globalnymi zmianami politycznymi i technologicznymi, zainicjowała znaczące przekształcenia w zakresie inwestycji i prywatyzacji. Rozwój technologii mobilnych i przenośnych urządzeń komputerowych znacząco przyczynił się do intensyfikacji działań wywiadowczych na arenie międzynarodowej, co z kolei podkreśliło wagę bezpieczeństwa informacji w obliczu rosnących zagrożeń dla tajemnic handlowych i własności intelektualnej. W odpowiedzi na te wyzwania, korporacje na całym świecie zmuszone były do implementacji zaawansowanych strategii ochrony swoich cyfrowych aktywów, co doprowadziło do wykrystalizowania się nowego obszaru strategicznego działalności przedsiębiorstwa – bezpieczeństwa technologii i informacji[242].

Współczesne przedsiębiorstwa działają w dynamicznie zmieniającym się środowisku, w którym informacja stała się jednym z najcenniejszych zasobów. Zdolność do efektywnego gromadzenia, przetwarzania i ochrony informacji często decyduje o przewadze konkurencyjnej na rynku[243]. Jednak rosnąca wartość informacji sprawia, że staje się ona obiektem działań nie tylko legalnej konkurencji, ale również szpiegostwa korporacyjnego. W kontekście globalnej gospodarki, gdzie granice między państwami stają się coraz mniej wyraźne, a rywalizacja na rynkach międzynarodowych zaostrza się[244], zrozumienie i skuteczne zarządzanie ryzykiem związanym ze szpiegostwem korporacyjnym jest kluczowe dla zapewnienia bezpieczeństwa i stabilności przedsiębiorstw. Niniejsze rozważania mają za zadanie rzucić światło na te krytyczne aspekty, stanowiąc istotny wkład w dyskusję na temat bezpieczeństwa informacji w środowisku biznesowym. W związku z tym, głównym celem jest kompleksowa analiza szpiegostwa korporacyjnego jako zjawiska wpływającego zarówno na bezpieczeństwo informacyjne, jak i cały system bezpieczeństwa organizacji. Systematyczny przegląd literatury w zakresie szpiegostwa korporacyjnego pozwolił na wyodrębnienie definicji zjawiska proponowanych przed zachodnich badaczy naukowych. Wyniki zostały przedstawione w tabeli nr 14.

[242] K. M. Altintas, *Comparative Analysis of Strategic Relationship between Industrial versus Corporate Espionage within the Framework of Implementation Methods*, Global Security and Intelligence Studies Vol. 6, No. 1 2021, s. 107-108.
[243] F. Mizrak, *Effective Change Management Strategies: Exploring Dynamic Models for Organizational Transformation*, W: *Perspectives on Artificial Intelligence in Times of Turbulence: Theoretical Background to Applications* (red.) N. Geada, G. L. Jamil, IGI Global, Nowy Jork 2023, DOI: 10.4018/978-1-6684-9814-9.ch009, s. 4, 6 i 9.
[244] M. Farzaneh, R. Wilden, L. Afshari, G. Mehralian, *Dynamic capabilities and innovation ambidexterity: The roles of intellectual capital and innovation orientation*, Journal of Business Research 148 (2022), https://doi.org/10.1016/j.jbusres.2022.04.030, s. 18 i 22.

Tabela 14 Wybrane definicje terminu szpiegostwo korporacyjne

Lp.	Autor	Definicja
1.	A. Vashisth, A. Kumar[245]	Szpiegostwo korporacyjne jest działaniem polegającym na prowadzeniu aktywności szpiegowskiej przez osoby pozostające wewnątrz danej organizacji na jej szkodę. Działania te podejmowane są ze względu na personalne motywy takie jak, np. brak awansu, chęć wzbogacenia się, zatarg z przełożonymi itp.,
2.	M. Button[246]	Szpiegostwo korporacyjne polega na nieautoryzowanym i tajnym zbieraniu tajemnic korporacyjnych dla przewagi konkurencyjnej,
3.	J. Abd Jalil, H. Hassan[247]	Szpiegostwo korporacyjne jest działaniem prowadzonym w cyberprzestrzeni i postrzegane jest jako operacje i powiązane programy lub działania prowadzone w cyberprzestrzeni w celu tajnego zbierania wrażliwych informacji od konkurentów,
4.	M. Chan[248]	Szpiegostwo korporacyjne to działania podejmowane przez konkurujące ze sobą przedsiębiorstwa, polegające na zdobywaniu informacji na temat konkurenta w celu utrzymania zaufania do organizacji oraz odstraszania potencjalnych adwersarzy,
5.	B. Wimmer[249]	Szpiegostwo korporacyjne dotyczy działań między podmiotami gospodarczymi w obrębie jednego kraju, skoncentrowanych na rywalizacji i zdobywaniu przewagi konkurencyjnej przez pozyskiwanie poufnych informacji o działalności konkurentów. Stanowi kluczowy element strategii konkurencyjnej w środowisku biznesowym, gdzie wiedza i informacja są postrzegane jako cenne zasoby. Jednocześnie zaangażowanie rządów w takie działania może świadczyć o stopniu, w jakim interesy państwowe i korporacyjne są ze sobą splecione, oraz o potencjalnym wpływie szpiegostwa na polityki gospodarcze i relacje międzynarodowe,
6.	K. A. Altintas[250]	Szpiegostwo korporacyjne to zjawisko nieautoryzowanego dostępu do infrastruktury fizycznej lub cyfrowej korporacji przez podmioty zewnętrzne. Takie działania mogą mieć na celu pozyskanie poufnych danych korporacyjnych, tajemnic handlowych, a także innych wartościowych informacji, które mogą być wykorzystane do osiągnięcia

[245] A. Vashisth, A. Kumar, *Corporate espionage: The insider threat*, Business Information Review, 30(2) 2013, https://doi.org/10.1177/0266382113491816, s. 84-85
[246] M. Button, *Editorial: economic and industrial espionage*, Security Journal (2020) 33:1–5, https://doi.org/10.1057/s41284-019-00195-5, s. 2.
[247] J. Abd Jalil, H. Hassan, *Protecting trade secret from theft and corporate espionage: some legal and administrative measures*, International Journal of Business and Society, Vol. 21 S1, 2020, s. 206-207.
[248] M. Chan, *Corporate Espionage and Workplace Trust/Distrust*, Journal of Business Ethics Vol. 42, No. 1 (Jan., 2003), s. 45-46.
[249] B. Wimmer, *Business espionage. Risk, Threats and Countermeasures*, Elsevier, Oxford 2015, s. 13-15.
[250] K. M. Altintas, *Comparative Analysis of Strategic…,* op. cit., s. 109.

Lp.	Autor	Definicja
		nieuczciwej przewagi konkurencyjnej lub mogą zostać sprzedane trzecim stronom.

Źródło: K. Kozłowski, Ewolucja szpiegostwa biznesowego…, op. cit., s. 81.

Analiza przedstawionych definicji szpiegostwa korporacyjnego wskazuje na kilka kluczowych aspektów tego zjawiska:

a) **motywacja wewnętrzna:** szpiegostwo korporacyjne może być inicjowane przez osoby wewnątrz organizacji, motywowane czynnikami takimi jak niezadowolenie zawodowe, chęć zysku czy konflikty z przełożonymi,
b) **zbieranie informacji bez autoryzacji:** działania te obejmują tajne pozyskiwanie tajemnic korporacyjnych w celu uzyskania przewagi nad konkurencją,
c) **cyberprzestrzeń jako arena działań:** szpiegostwo to odbywa się również w cyberprzestrzeni, gdzie wykorzystywane są operacje i programy do tajnego zbierania informacji od konkurentów,
d) **konkurencja między przedsiębiorstwami:** działania szpiegowskie są podejmowane przez konkurujące ze sobą, w celu zdobycia informacji na temat działalności konkurentów,
e) **wymiar wewnętrzny i międzynarodowy:** szpiegostwo korporacyjne dotyczy zarówno działań w obrębie jednego kraju, jak i może mieć wpływ na polityki gospodarcze i relacje międzynarodowe, wskazując na powiązania między interesami państwowymi i korporacyjnymi,
f) **nieautoryzowany dostęp:** zjawisko to obejmuje nieautoryzowany dostęp do fizycznej i cyfrowej infrastruktury korporacji, z zamiarem pozyskania poufnych danych do nieuczciwego wykorzystania[251].

Wskazane działania motywowane są chęcią uzyskania przewagi konkurencyjnej na rynku, mogą odbywać się w cyberprzestrzeni i obejmują zarówno aspekty wewnętrzne, jak i międzynarodowe relacje gospodarcze. Szpiegostwo korporacyjne, postrzegane jako nielegalne i nieetyczne, niesie za sobą znaczące ryzyko dla bezpieczeństwa i stabilności korporacji, wymagając skutecznych strategii ochrony i zarządzania ryzykiem. Ze względu na nielegalne działania osób z zewnątrz przenikających do biur korporacyjnych lub sieci, może być bardzo szkodliwe[252]. Te rodzaje ataków mogą być opisane jako nielegalne i nieetyczne

[251] K. Kozłowski*, Ewolucja szpiegostwa biznesowego…,* op. cit., s. 85.
[252] S. Horan, *Corporate and Industrial Espionage and Their Effect on American Competitiveness - A statement before the House Subcommittee on International Economic Policy and Trade*, IO6 Congress. Serial No: 106-180, Waszyngton 2000, s. 29-30.

działania podejmowane przez organizacje w celu systematycznego zbierania, analizowania i zarządzania informacjami o konkurentach, aby uzyskać przewagę konkurencyjną na rynku[253], innymi słowy działania te mogą wynikać z nieuczciwej konkurencji między firmami[254].

Szpiegostwo korporacyjne, stało się wielomiliardowym przemysłem. Dokładna wartość strat spowodowanych szpiegostwem korporacyjnym jest trudna do określenia, a wiele kradzieży informacji własnościowych pozostaje niewykrytych i niezgłoszonych. Nawet gdy szpiegostwo jest odkryte przez pracodawcę, skala i wpływ naruszenia często nie mogą być określone[255]. Amerykańskie studia rządowe szacują roczne straty dla firm z powodu szpiegostwa korporacyjnego na setki miliardów dolarów[256].

Szpiegostwo korporacyjne jest również wykorzystywane do badania produktów lub składników pod kątem postrzeganych lub rzeczywistych ryzyk, do planowania rynków i ustalania cen. Stosunkowo często organizacje stają się celami takiej działalności bez wiedzy lub metodologii, aby skutecznie jej przeciwdziałać[257]. W przypadku dowodów na istnienie obcego rządu lub zaangażowania wrogiego szpiegostwa, przedsiębiorstwa zaangażowane w takie nielegalne działania podlegają ściganiu prawnemu. Czynniki, które określają prawne granice prób szpiegostwa korporacyjnego, są również ściśle związane z stopniem szkody gospodarczej wyrządzonej właścicielowi tajemnic handlowych lub własności intelektualnej oraz z potencjałem odstraszającym ścigania[258].

Przypadki kradzieży tajemnic handlowych z firm Lucent Technologies, IDEXX i Avery Dennison pokazują, jak przebiegli pracownicy mogą wykorzystać naiwność innych pracowników i infrastrukturę komputerową organizacji do wspierania ich działań szpiegowskich oraz że korporacyjne rozpoznanie tych naruszeń bezpieczeństwa nastąpiło dopiero po przeniesieniu ich technologii do konkurentów[259].

Strategiczne znaczenie inicjatyw szpiegostwa przemysłowego prowadzonych dla korporacji działających na skalę globalną staje się coraz bardziej znaczące w ostatnich latach. Co więcej, w tej fazie, krajowe organy wywiadowcze przekształciły się w niewidzialnych interesariuszy swoich krajowych firm i zaczęły pracować we współpracy/koordynacji w kierunku wspólnych celów bezpieczeństwa gospodarczego.

---

[253] A. Vashisth, A. Kumar, *Corporate espionage…,* op. cit., s. 83.
[254] B. Wimmer, *Business espionage. Risk, Threats…*, op. cit., s. 26.
[255] K. M. Altintas, *Comparative Analysis of Strategic…,* op. cit.
[256] C. Koen, B. London, *To Catch a Thief: Protecting Proprietary Information Including Trade Secrets from Corporate Espionage*, The Health Care Manager, Oct/Dec 2019; 38 (4), doi: 10.1097/HCM.0000000000000283, s. 331.
[257] B. Rothke, *Corporate Espionage and What Can Be Done to Prevent It*, Information Systems Security. (2001) 10:5, doi: 10.1201/1086/43315.10.5.20011101/31716.3, s. 1.
[258] K. M. Altintas, *Comparative Analysis of Strategic…,* op. cit., s. 110.
[259] W. M. Fitzpatrick, S. A. DiLullo, D. R. Burke, *Trade Secret Piracy and Protection: Corporate Espionage. Corporate Security and the Law*, Advances in Competitiveness Research, Vol. 12, No. 1 2004, s. 66.

Zjawisko szpiegostwa korporacyjnego może wystąpić w organizacjach, gdy inni aktorzy mają konkurencyjne interesy. To czyni każdego z konkurencyjnych interesariuszy potencjalnym szpiegiem[260]. Jednakże, jeśli organizacja chce ograniczyć możliwy wpływ szpiegostwa, może wprowadzić stosunkowo proste środki łagodzące. Pierwszym krokiem jest przyjęcie założenia, że akt szpiegostwa może wystąpić i organizacja jest jego potencjalnym celem. Drugim krokiem jest analiza ryzyka, która identyfikuje krytyczne środki i procesy oraz ich podatności. Na podstawie tej świadomości i analizy ryzyka, organizacja może opracować polityki dotyczące tego, komu zezwolić na dostęp do poufnych informacji korporacyjnych.

Autoryzacja dostępu do poufnych informacji powinna być przyznawana tylko po stwierdzeniu braku ograniczeń podczas procesu przesiewowego. Niemniej jednak, kradzież poufnych informacji korporacyjnych nie może być całkowicie wykluczona. Dlatego też istnieje potrzeba przygotowania na sytuacje, w których szpiegostwo faktycznie miało miejsce. W celu stworzenia odporności po szpiegostwie, korporacje muszą opracować plany awaryjne z wyprzedzeniem, przeprowadzać oceny szkód i poprawiać środki łagodzące, aby uniknąć przyszłego zagrożenia ataku[261].

Celem podsumowania dotychczasowych rozważań, autor proponuje finalną konkluzję w zakresie różnic i podobieństw zaobserwowanych w toku analizy definicji rodzajów szpiegostwa występujących we współczesnych organizacjach. Synteza została przedstawiona w tabeli nr 15.

Tabela 15 Porównanie szpiegostwa gospodarczego, przemysłowego i korporacyjnego - podobieństwa i różnice

Podobieństwa	Różnice
Wszystkie trzy formy szpiegostwa obejmują pozyskiwanie tajemnic handlowych lub innych poufnych informacji bez autoryzacji,	**Szpiegostwo gospodarcze** jest często inicjowane przez państwa lub ich służby wywiadowcze i ma na celu wzmocnienie własnej pozycji gospodarczej na arenie międzynarodowej. Beneficjentami są zazwyczaj państwa lub instytucje zagraniczne,
Działalność szpiegowska w każdym przypadku jest motywowana chęcią uzyskania przewagi konkurencyjnej, choć beneficjenci tych działań różnią się w zależności od typu szpiegostwa,	**Szpiegostwo przemysłowe** przynosi korzyści głównie prywatnym jednostkom lub firmom, a nie państwom. Może być inicjowane zarówno przez obce rządy, jak i przedsiębiorstwa prywatne, czasami przy

[260] K. M. Altintas, *Comparative Analysis of Strategic…,* op. cit.
[261] M. Ijzermans, W. Van den Berge, *Resilience after Corporate or Industrial Espionage*, The BCI Netherlands & Belgium Conference, Utrecht 2019, s. 1.

Podobieństwa	Różnice
	ich wsparciu, w celu pozyskania tajemnic konkurencyjnych przedsiębiorstw,
Szpiegostwo gospodarcze, przemysłowe i korporacyjne może odbywać się zarówno w przestrzeni fizycznej, jak i cyfrowej, wykorzystując nowoczesne technologie do zbierania danych.	**Szpiegostwo korporacyjne** jest często działaniem wewnętrznym, inicjowanym przez osoby znajdujące się wewnątrz organizacji lub przez konkurencyjne przedsiębiorstwa. Motywacje mogą być różne, od personalnych po chęć uzyskania przewagi konkurencyjnej. Szpiegostwo korporacyjne obejmuje szeroki zakres działań, od nieautoryzowanego dostępu do infrastruktury fizycznej lub cyfrowej, po zbieranie danych na szkodę własnej organizacji lub konkurentów.

Źródło: K. Kozłowski, Ewolucja szpiegostwa biznesowego…, op. cit., s. 86.

Wobec powyższego oraz na podstawie przedstawionych uprzednio kluczowych elementów, charakteryzujących zjawisko szpiegostwa korporacyjnego, autor proponuje ogólną definicję pojęcia w następującym brzmieniu – **szpiegostwo korporacyjne** to złożone działania wywiadowcze podejmowane zarówno przez osoby wewnątrz organizacji, jak i podmioty zewnętrzne, skierowane na nieautoryzowane pozyskiwanie poufnych danych korporacyjnych, tajemnic handlowych oraz informacji strategicznych[262].

W kontekście rosnącej konkurencji i globalizacji rynków, metody pozyskiwania informacji przez przedsiębiorstwa nabierają nowego wymiaru, przechodząc często granice legalności. Szpiegostwo korporacyjne jako złożona działalność wywiadowcza obejmująca zarówno osoby wewnątrz organizacji, jak i podmioty zewnętrzne, staje się coraz bardziej wyrafinowane i różnorodne w swoich metodach. W dobie cyfryzacji i nieustannego postępu technologicznego, techniki te ewoluują, dostosowując się do zmieniającego się środowiska biznesowego i technologicznego, co zmusza organizacje do ciągłego rozwijania strategii ochrony swoich cennych zasobów informacyjnych. Jednak adwersarze również nie ustają w rozwijaniu metod penetracji systemów zabezpieczeń oraz uzyskiwania informacji na temat najsłabszych ogniw w organizacji, które można wykorzystać w celu uzyskania przewagi.

W niniejszym podrozdziale przedstawiono istotę szpiegostwa korporacyjnego jako zagrożenia dla bezpieczeństwa informacji w przedsiębiorstwach sektora ICT. Omówiono, jak globalizacja i rozwój technologiczny zwiększyły podatność firm na nieautoryzowany dostęp do strategicznych informacji. Szpiegostwo korporacyjne jest definiowane jako działania

[262] K. Kozłowski*, Ewolucja szpiegostwa biznesowego…,* op. cit., s. 87.

wywiadowcze podejmowane przez osoby wewnętrzne i zewnętrzne, mające na celu pozyskanie poufnych danych oraz tajemnic handlowych w celu uzyskania przewagi konkurencyjnej. W analizie zawarto także klasyfikację różnych motywacji oraz metod stosowanych przez szpiegów korporacyjnych, podkreślając, że działania te często wiążą się z naruszeniem legalności i etyki w środowisku biznesowym. Przedstawiono przegląd definicji, wyróżniając wspólne elementy szpiegostwa korporacyjnego, takie jak nieautoryzowany dostęp do infrastruktury i cyberprzestrzeń jako arena działań.

Hipoteza szczegółowa: *szpiegostwo korporacyjne stawia przed zarządzaniem bezpieczeństwem przedsiębiorstwa konieczność przeciwdziałania środkom i metodom dostępu do danych oraz pozyskiwania informacji w celu zdobycia przewagi konkurencyjnej*, znajduje potwierdzenie w kilku aspektach omawianego podrozdziału:

a) przeciwdziałanie środkom dostępu do danych – szpiegostwo korporacyjne zmusza organizacje do tworzenia zaawansowanych strategii ochrony przed nieautoryzowanym dostępem, zarówno fizycznym, jak i cyfrowym. Organizacje muszą skutecznie zabezpieczać swoje zasoby informacyjne, aby przeciwdziałać zagrożeniom, które w dużym stopniu wynikają z działań wewnętrznych i zewnętrznych,
b) metody pozyskiwania informacji – podrozdział definiuje szpiegostwo korporacyjne jako działalność o różnorodnych metodach działania, w tym tajne pozyskiwanie informacji i nieautoryzowany dostęp do infrastruktury cyfrowej. Skuteczność zarządzania bezpieczeństwem przedsiębiorstwa wymaga monitorowania i adaptacji strategii ochronnych wobec stale rozwijających się metod szpiegowskich stosowanych przez konkurencję,
c) cel zdobycia przewagi konkurencyjnej – kluczowym motywem omawianego zjawiska jest dążenie do zdobycia przewagi rynkowej, co podkreśla znaczenie przeciwdziałania tym działaniom dla ochrony interesów i pozycji rynkowej przedsiębiorstwa.

Podsumowując, podrozdział częściowo potwierdza hipotezę szczegółową, podkreślając, że zarządzanie bezpieczeństwem musi być kompleksowe i dynamiczne, aby skutecznie chronić informacje przed działaniami szpiegowskimi nastawionymi na uzyskanie nieuczciwej przewagi.

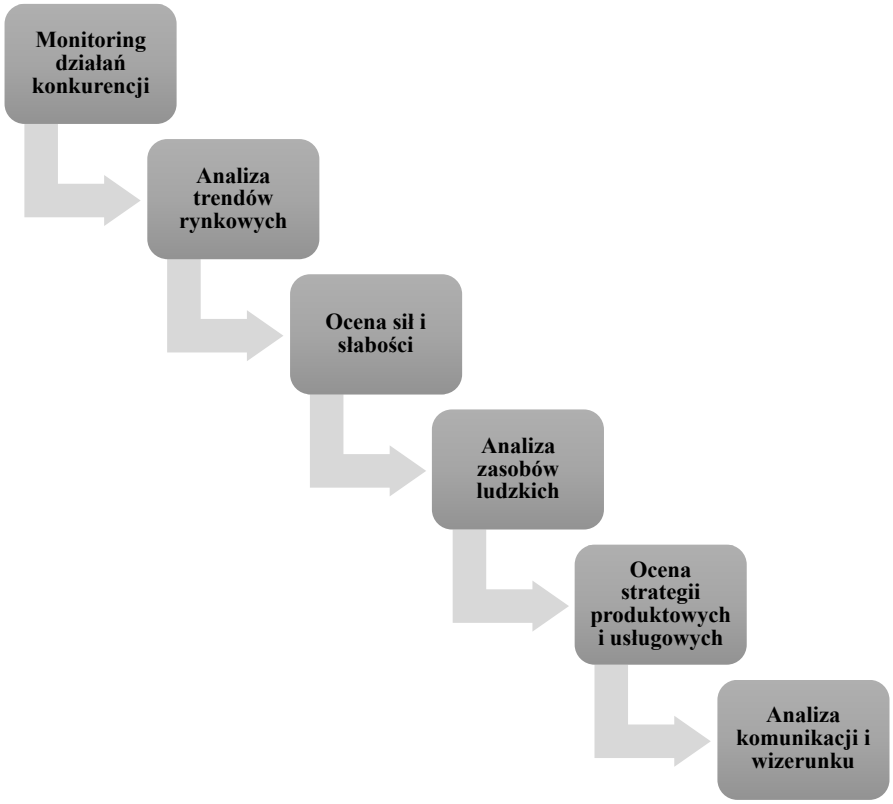
3.3 Specyfika zarządzania w przedsiębiorstwach ICT w kontekście operacyjnego pozyskiwania informacji

Analiza operacyjna w środowisku korporacyjnym i konkurencyjnym odgrywa kluczową rolę w dostosowywaniu się do dynamicznie zmieniającego otoczenia biznesowego.

W obu kontekstach, celem jest zdobycie kompleksowej wiedzy o wewnętrznych i zewnętrznych aspektach działalności przedsiębiorstw, ich konkurentach, firmach współpracujących, jak również o osobach wchodzących w skład organów zarządzających.

Jednakże poniższy podrozdział skupi się na zgoła odmiennym rozumieniu wskazanego pojęcia. Analiza operacyjna w kontekście pozyskiwania informacji o przedsiębiorstwie rozumiana będzie jako wszelkie działania, które prowadzone są przez osoby spoza organizacji w celu uzyskania danych, wiedzy i informacji wrażliwych o przedsiębiorstwie będącym w zainteresowaniu. Istotą tej metody jest uzyskanie możliwie szerokiej perspektywy na temat organizacji będącej w zainteresowaniu i służyć ma wskazaniu miejsc lub elementów systemu bezpieczeństwa przedsiębiorstwa, które można wykorzystać na potrzeby przeprowadzenia ataku na gromadzone prze nie zasoby. Krótko mówiąc, analiza operacyjna prowadzona jest przez atakującego w celu wykrycia i wykorzystania najsłabszych elementów systemu, aby wejść w posiadanie danych i informacji o tej organizacji i wykorzystać je na potrzeby zastosowania innych metod, dobranych adekwatnie do uzyskanych luk w systemie.

Analiza operacyjna obejmuje systematyczne i metodyczne zbieranie danych, ich analizę i interpretację, by uzyskać wgląd w aktualne i potencjalne możliwości ataku. Jest to proces skupiający się na dokładnym rozważeniu złożonych zbiorów danych z różnych źródeł, umożliwiający identyfikację kluczowych trendów rynkowych, którymi podąża atakowana organizacji, analizę strategii konkurencji oraz ocenę skuteczności planowanych metod ataku. Przykładowy schemat analiz operacyjnej został przedstawiony na rysunku nr 20.



Rysunek 20 Przykładowy schemat analizy operacyjnej
Źródło: opracowanie własne.

Kluczowe elementy prowadzonej analizy operacyjnej w kontekście złamania zabezpieczeń przedsiębiorstwa to:

a) **monitoring działań konkurencji:** regularne śledzenie działań konkurentów w mediach społecznościowych, na stronach internetowych, w raportach branżowych oraz analiza ich strategii marketingowych i inwestycyjnych na potrzeby ustalenia obszarów informacji o istotnej wartości[263],
b) **analiza trendów rynkowych:** zrozumienie, w jakim kierunku zmierza rynek, jakie nowe technologie są wprowadzane przez organizację stanowiącą cel ataku i jakie są aktualne preferencje konsumentów, w przypadku ewentualnej odsprzedaży informacji uzyskanej podczas ataku[264],
c) **ocena sił i słabości:** wykorzystanie narzędzi takich jak analiza SWOT do oceny wewnętrznych mocnych i słabych stron konkurencyjnych organizacji oraz identyfikacja

[263] K. Piotrowska, *Etapy procesu innowacyjnego jako obszary ryzyka w audycie wewnętrznym*, Finanse, Rynki Finansowe, Ubezpieczenia nr 6/2016 (84), cz. 1, DOI: 10.18276/frfu.2016.84/1-30, s. 354.
[264] A. R. Anugerah, P. S. Muttaqin, W. Trinarningsih, *Social network analysis in business and management research: A bibliometric analysis of the research trend and performance from 2001 to 2020*, Heliyon 8 (2022), https://doi.org/10.1016/j.heliyon.2022.e09270, s. 6 i 8.

możliwości przeprowadzenia ataku wynikających z zewnętrznego i wewnętrznego otoczenia organizacji stanowiącej cel ataku[265],

d) **analiza zasobów ludzkich:** zrozumienie, jakie talenty i umiejętności posiadają pracownicy organizacji stanowiącej cel ataku, które mogą wskazywać na ich potencjalne zdolności innowacyjne oraz możliwości rozwoju w przypadku próby pozyskania pracownika na rzecz konkurencyjnego przedsiębiorstwa[266]. Ponadto, w przypadku próby pozyskania tzw. *insider'a*, analiza ma na celu uzyskanie informacji o występujących konfliktach oraz ich podłożu,

e) **ocena strategii produktowych i usługowych:** analiza oferty analizowanego przedsiębiorstwa pod kątem unikalności, jakości oraz cen, co może pomóc w identyfikacji luk w rynkowej ofercie, które można wykorzystać lub w celu uzyskania informacji wyprzedzającej na temat innowacyjnych ofert, które dopiero są opracowywane,

f) **analiza komunikacji i wizerunku:** ocena sposobów, w jakie analizowana organizacja komunikuje się z klientami oraz buduje swój wizerunek, może ujawnić słabe punkty[267], które mogą zostać wykorzystane do przeprowadzenia ataków teleinformatycznych lub kampanii phisingowych.

Analiza operacyjna umożliwia potencjalnemu adwersarzowi lepsze rozumienie otoczenia operacyjnego, identyfikację słabych punktów w operacjach i strategiach, oraz odkrywanie nowych możliwości penetracji aktywów atakowanej organizacji. Jest niezbędna do opracowania skutecznych strategii przeprowadzenia ataku, uzyskania bieżącego dostępu do systemu informacyjnego atakowanej organizacji oraz kluczowych osób posiadających specjalistyczną wiedzę w zakresie produktów, usług i strategii zarządzania. Jednocześnie ma na celu zapewnienie minimalizacji ryzyka szybkiego wykrycia takiego ataku i bezpośredniego powiązania z atakującym.

W toku prowadzonej analizy operacyjnej stosuje się działania, które na pierwszy rzut oka wydają się być zgodne z prawem (korzystając z nich w sposób, który tylko sprawia wrażenie legalności). To obejmuje różnorodne techniki stosowane w ramach tak zwanego białego wywiadu, uczestnictwo w wydarzeniach branżowych lub dostęp do danych

[265] M. A. Benzaghta, A. Elwalda, M. M. Mousa, I. Erkan, M. Rahman, *SWOT analysis applications: An integrative literature review*, Journal of Global Business Insights Issue 1 (2021) Vol. 6, https://www.doi.org/10.5038/2640-6489.6.1.1148, s. 57 i 59.

[266] A. M. A. Ausat, B. Permana, M. A. K. Harahap, *Do Information Technology and Human Resources Create Business Performance: A Review*, Journal of Professional Business Review 2023 8 (8), https://doi.org/10.26668/businessreview/2023.v8i8.2206, s. 5 i 8.

[267] P. Chodorowska, M. Brańko, E. Tomaszewska, *Real-Time Marketing jako narzędzie budowania wizerunku przedsiębiorstwa w mediach społecznościowych*, Akademia Zarządzania, vol. 8 (2) 2024, DOI: 10.24427/az-2024-0022, s. 209

ekonomicznych, a także operacje nielegalne, kwalifikujące się jako nieuczciwa konkurencja lub działania przestępcze[268].

Analizę operacyjną należy traktować jako przygotowanie do przeprowadzenia bardziej inwazyjnych czynności mających na celu penetrację zasobów informacyjnych przedsiębiorstwa stanowiącego przedmiot prowadzonej przez adwersarza analizy.

W polskiej literaturze prawniczej i ustawodawstwie istnieje brak szczegółowych uregulowań definiujących pojęcia takie jak **biały wywiad, wywiad z otwartych źródeł** (ang. Open Source Intelligence, skrótowo: OSINT) czy otwarte źródła informacji. W związku z tym, specjaliści z dziedziny prawa tworzą własne interpretacje tych terminów. Na przykład, Krzysztof Liedel i Tomasz Serafin sugerują, że przez informację z otwartych źródeł należy rozumieć *serię danych pochodzących z jednego lub wielu otwartych źródeł, które są poddawane ocenie z uwzględnieniem momentu ich publikacji oraz treści*[269]. W podobnym duchu wypowiada się Krzysztof Mroziewicz, definiując biały wywiad jako *przetwarzanie informacji z legalnie dostępnych źródeł*[270], uznając jednocześnie tę formę za *najbezpieczniejszą i najbardziej przyjazną metodę pozyskiwania danych*[271].

W międzynarodowych opracowaniach znajdujemy bardziej szczegółowe wyjaśnienia terminu Open Source Intelligence, na przykład w dokumencie NATO zatytułowanym „Open Source Intelligence Reader" z 2002 roku, który opisuje OSINT jako *wynik przetwarzania informacji. Informacje te są celowo poszukiwane, porównywane pod kątem treści i selekcjonowane ze względu na ich znaczenie dla odbiorcy*[272]. Dokument ten nawiązuje do wytycznych wydanych przez dyrektora CIA w 1994 roku, podkreślając publiczną dostępność danych i sugerując, że termin *otwarte dane* może być stosowany do każdej informacji używanej w kontekście otwartym, bez ryzyka dla źródeł, metod wywiadowczych i bezpieczeństwa państwa[273].

W literaturze międzynarodowej przedstawione są również cztery główne etapy analizy otwartych danych:

---

[268] P. Łabuz, T. Safjański, *Charakterystyka wybranych metod działania z obszaru szpiegostwa gospodarczego*, W: *Ochrona przedsiębiorstwa przed szpiegostwem gospodarczym. Prawne i praktyczne aspekty zapewnienia bezpieczeństwa aktywów przedsiębiorcy* (red.) P. Herman, P. Łabuz, T. Safjański, Wydawnictwo Difin, Warszawa 2021, s. 20.

[269] K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Wydawnictwo Difin, Warszawa 2011, s. 51.

[270] K. Mroziewicz, *Czas pluskiew*, Wydawnictwo: Wołoszański, Warszawa 2007, s. 334

[271] Ibidem.

[272] K. Jarczewska-Walendziak, *Wykorzystanie otwartych źródeł informacji przez służby śledcze*, Toruńskie Studia Bibliologiczne 2017 nr 1 (18), doi: http://dx.doi.org/10.12775/TSB.2017.008, s. 137.

[273] Director of Central Intelligence Directive 2/12, *Community Open Source Program*, https://irp.fas.org/offdocs/dcid212.htm [dostęp 28.02.2024 r.].

a) zbieranie surowych danych (ang. Open Source Data, OSD), które pochodzą z oryginalnych źródeł (np. publikacje, media, strony internetowe, zdjęcia) i ich prezentacja w najbardziej podstawowej formie,
b) analiza zebranych danych (ang. Open Source Information, OSINF), obejmująca ich edycję, kompilację w jeden dokument i przekazanie kierownictwu do dalszego rozprowadzania,
c) planowane pozyskiwanie informacji, czyli biały wywiad (ang. Source Intelligence, SINT) – dystrybucja danych do wyselekcjonowanej grupy odbiorców zgodnie z zasadami ustalonymi przez zapytującego (każda służba policyjna czy wywiadowcza opracowuje własne procedury postępowania z danymi),
d) weryfikacja informacji, czyli zweryfikowany, potwierdzony biały wywiad (ang. Validated Open Source Intelligence, OSINT-V) – potwierdzenie wiarygodności informacji na podstawie różnych źródeł[274].

Otwarte źródła danych, które są powszechnie wykorzystywane przez organy ścigania, mogą być sklasyfikowane do następujących kategorii:

a) media tradycyjne, obejmujące:
    a. prasę w formie papierowej, taką jak gazety, periodyki specjalistyczne i dokumenty oficjalne,
    b. kanały informacyjne telewizyjne i stacje radiowe,
    c. literaturę, w tym książki, eseje, analizy oraz reportaże dziennikarskie.
b) Internet, który zawiera:
    a. cyfrowe wersje gazet i magazynów,
    b. blogi oraz platformy mikroblogowe,
    c. serwisy społecznościowe,
    d. witryny typu wiki,
    e. platformy wideo,
    f. serwisy udostępniające zdjęcia,
    g. strony internetowe firm,
    h. bazy danych WHOIS dla domen,
    i. mapy online, zdjęcia satelitarne oraz lotnicze.
c) usługi komercyjne, w tym:
    a. przedsiębiorstwa dostarczające płatne raporty i analizy na zamówienie,
    b. publikacje marketingowe.

[274] B. Sromczyński, P. Waszkiewicz, *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, Prokuratura i Prawo 2014 nr 5, s. 149.

d) szarą literaturę (*grey literature*), czyli analizy i informacje dostępne jedynie przez specjalistyczne kanały, tworzone przez środowiska akademickie, instytucje państwowe i organizacje pozarządowe.
e) Bazy danych i katalogi, oferujące szeroki zakres informacji[275].

Ogólna analiza trendów pozwala zaobserwować, że korzystanie z otwartych źródeł danych, zwłaszcza internetowych, stanowi integralną część działań wywiadowczych. Co istotne, metody te znajdują zastosowanie również wśród zorganizowanych grup przestępczych, które adaptują techniki charakterystyczne dla wywiadu otwartego do własnych celów[276].

Ponadto, na szczególną uwagę w przypadku wykorzystania wywiadu jawnoźródłowego zasługują sieci społecznościowe. Obecnie większość ludzi przenosi swoje życie prywatne i zawodowe bezpośrednio do cyberprzestrzeni, publikując tam zarówno swoje dane osobowe, jak również zdjęcia, adres miejsc, które odwiedzali, wydarzenia, w których uczestniczyli itp. Kluczowe funkcjonalności platform społecznościowych obejmują między innymi: galerie zdjęć, funkcję bloga, notatnik, bazę kontaktów, listę znajomych, grupy użytkowników, możliwość blokady innych użytkowników oraz wewnętrzną komunikację[277].

Na takich platformach, użytkownicy po rejestracji mają możliwość tworzenia sieci społecznych i grup, wymiany wiadomości oraz zdjęć, a także korzystania z różnorodnych aplikacji. W kontekście wywiadu otwartego, często wykorzystywanymi źródłami danych są platformy takie jak Facebook, Instagram, Twitter, Pinterest, a nawet serwisy randkowe. Dzięki tym serwisom, można zgromadzić szereg informacji, takich jak:

a) dane osobowe, w tym imię i nazwisko, data urodzenia, zdjęcia, pseudonimy,
b) dane kontaktowe, w tym adres zamieszkania, adres e-mail, numer telefonu,
c) informacje zawodowe, w tym miejsce pracy, zajmowane stanowisko, wykształcenie, ukończone kursy, doświadczenie zawodowe oraz historię zatrudnienia,
d) informacje o relacjach, takie jak lista znajomych, obserwatorzy, rodzina czy koledzy z pracy,

---

[275] G. Dobrowolski, W. Filipkowski, M. Kisiel-Dorohnicki, W. Rakoczy, *Wsparcie informatyczne dla analizy otwartych źródeł informacji w Internecie w walce z terroryzmem. Zarys problemu*, W: *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu* (red.) L. K. Paprzycki, Z. Rau, Wydawnictwo Wolters Kluwer, Warszawa 2009, s. 281-282.

[276] E. Wójcik, *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej*, https://wspia.eu/media/00jnsacq/44-w%C3%B3jcik.pdf [dostęp 28.02.2024 r.] oraz B. Sarmak, *„Biały wywiad" w służbie terroryzmu*, W: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji* (red.) K. Liedel, P. Piasecka, T. R. Aleksandrowicz, Wydawnictwo Difin, Warszawa 2014, s. 183-195.

[277] P. Herman, T. Safjański, *Zbieranie informacji biznesowych na poziomie operacyjnym – wywiad gospodarczy*, W: *Wywiad i analityka w biznesie. Prawne i praktyczne aspekty analizy wywiadowczej* (red.) P. Herman, P. Łabuz, T. Safjański, Difin, Warszawa 2023, s.74.

e) informacje o miejscach, które użytkownik odwiedza, na przykład restauracje, kina czy hotele,
f) dane o zainteresowaniach, na przykład modzie, muzyce czy hobby,
g) preferencje seksualne,
h) sympatie polityczne,
i) informacje majątkowe, w tym posiadane pojazdy, nieruchomości czy zagraniczne podróże[278].

W obliczu rosnącej popularności mediów społecznościowych, wielu profesjonalistów decyduje się na założenie profilu na platformach zawodowych. Dla doświadczonych analityków, publicznie udostępnione informacje stanowią cenne źródło danych, które mogą być wykorzystane do przygotowania celowanych ataków na daną osobę lub instytucję, w której jest zatrudniona.

Obserwacja stanowi jedną z najstarszych metod pracy operacyjnej wykorzystywaną przez różne służby, zarówno policyjne, jak i specjalne, a obecnie również przez zorganizowane grupy przestępcze. Posiada kluczowe znaczenie w kontekście ochrony przedsiębiorstw i ich pracowników przed potencjalnymi zagrożeniami. Obserwacja, zdefiniowana jako systematyczne śledzenie lub podsłuchiwanie osób i obiektów w celu uzyskania istotnych informacji na temat osoby lub obiektu będącego w zainteresowaniu[279] i może obejmować zarówno działania legalne, jak i te balansujące na granicy prawa.

W ramach przygotowania do przeprowadzenia ataku na zasoby informacyjne przedsiębiorstwa, obserwacja wykorzystywana jest do przede wszystkim do dokumentowania:

a) zachowania obserwowanych osób, czyli uzyskania informacji o:
    a. miejscu pobytu osoby będącej w zainteresowaniu,
    b. miejscu, czasie i charakterze kontaktu z osobami trzecimi oraz ich danych personalnych,
    c. adresów miejsc odwiedzanych przez osobę będącą w zainteresowaniu,
    d. personaliów osób przychodzących do mieszkania osoby obserwowanej, pokoju hotelowego, zakładu pracy, punktu usługowego, itp.,
    e. kontaktów korespondencyjnych,
    f. kontaktów handlowych,
    g. sposobu zachowania się osoby obserwowanej w określonym środowisku czy okolicznościach.

[278] Ibidem.
[279] F. Musiał, *Teoria pracy operacyjnej Służby Bezpieczeństwa w świetle wydawnictw resortowych Ministerstwa Spraw Wewnętrznych PRL (1970-1989),* Wydanie III, Kraków-Warszawa 2018, s. 345 oraz *Poselski projekt ustawy o czynnościach operacyjno-rozpoznawczych* z dn. 7 lutego 2008 r. (Druk nr 353), Art. 2 ust. 3 pkt 6.

b) określonych zjawisk i wydarzeń związanych z osobą lub przedsiębiorstwem będącym w zainteresowaniu,
c) osób pojawiających się w pobliżu obiektów znajdujących się w zainteresowaniu,
d) stałe zabezpieczenie wybranych miejsc związanych z osobą lub przedsiębiorstwem będącym w zainteresowaniu[280].

W przypadku objęcia obserwacją konkretnego obiektu na potrzeby dokumentowania ustala się przede wszystkim:

a) wszystkie drogi dojścia do niego,
b) drogi zabezpieczające możliwość umknięcia lub schowania się,
c) rozkład dnia przebywających w nim osób lub sąsiadów,
d) rozkład jazdy przejeżdżających obok środków komunikacji miejskiej,
e) czasy pojawiania się osłony dźwiękowej (szum przejeżdżającej komunikacji miejskiej, dźwięk dzwonów itp.),
f) systemy ochrony,
g) wewnętrzny rozkład obiektu[281].

Różnorodność metod obserwacji, takich jak obserwacja piesza, ruchoma, mieszana, a także wykorzystanie stałych punktów obserwacyjnych czy skrytego sprzętu technicznego, w tym dronów czy urządzeń GPS, stanowi o jej skuteczności. Jednakże, rosnące zastosowanie tych metod, szczególnie w kontekście obserwacji prowadzonej przez organizacje konkurencyjne, rodzi istotne zagrożenia dla bezpieczeństwa informacji przedsiębiorstw i prywatności ich pracowników[282].

Potencjalnymi miejscami, gdzie obserwacja może być najczęściej stosowana, są w szczególności:

a) miejsce pracy,
b) zamieszkania,
c) parkingi pojazdów, którymi porusza się osoba w zainteresowaniu,
d) miejsca odwiedzane podczas wykonywania czynności służbowych, w tym hotele, lotniska czy miejsca spotkań biznesowych,
e) miejsca prowadzenia działalności biznesowej, logistycznej lub finansowej przedsiębiorstwa będącego w zainteresowaniu[283].

---

[280] Na podstawie F. Musiał, *Teoria pracy operacyjnej…,* op. cit., s. 191.
[281] *Metody i formy pracy operacyjnej stosowane przez oficerów Głównego Zarządu Rozpoznania Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej,* WSI, Warszawa 2004, s. 25.
[282] P. Herman, *Ochrona komunikacji biznesowej przez szpiegostwem*, W: *Ochrona przedsiębiorstwa przed szpiegostwem gospodarczym. Prawne i praktyczne aspekty zapewnienia bezpieczeństwa aktywów przedsiębiorcy* (red.) P. Herman, P. Łabuz, T. Safjański, Wydawnictwo Difin, Warszawa 2021, s. 206.
[283] Ibidem.

Wykorzystanie obserwacji może prowadzić do nieautoryzowanego uzyskania wrażliwych informacji, co stanowi realne zagrożenie dla przedsiębiorstw i ich pracowników. Szczególnie w dzisiejszym świecie, gdzie granice między legalnymi a nielegalnymi metodami pozyskiwania informacji są coraz bardziej zatarte, ważne jest, aby przedsiębiorstwa były świadome tych zagrożeń i stosowały odpowiednie środki ochronne.

Ochrona przed takimi działaniami jest stosunkowo trudna i wymaga nie tylko stosowania zaawansowanych technologii bezpieczeństwa informacji, ale również budowania świadomości wśród pracowników na temat potencjalnych zagrożeń i metod ich przeciwdziałania. Edukacja pracowników na temat bezpieczeństwa informacji, w tym sposobów ochrony przed nieautoryzowaną obserwacją, staje się zatem istotnym elementem dla strategii bezpieczeństwa przedsiębiorstwa w dzisiejszym świecie.

Socjotechnika polega na manipulowaniu zachowaniami i przekonaniami osób poprzez techniki perswazyjne, mające na celu przekonanie ich do przyjęcia fałszywej tożsamości prezentowanej przez manipulatora, stworzonej specjalnie w ramach danej manipulacji[284]. Dzięki temu, socjotechnik jest w stanie wykorzystać swoich rozmówców, przy dodatkowym lub nie, użyciu środków technologicznych, do zdobycia poszukiwanej informacji[285]. Według Komisji Nadzoru Finansowego, socjotechnika to działanie obejmujące oddziaływanie na osoby poprzez stosowanie strategii opartej na oszustwie, która wykorzystuje ogólne schematy reakcji psychologicznych[286].

Głównym celem jest zdobycie dostępu do informacji poufnych lub inaczej niedostępnych bez upoważnienia. Efektywność i powszechność zastosowania socjotechniki jest efektem ludzkiej podatności na wpływy zewnętrzne oraz skłonności do popełniania błędów w procesie myślenia. W obliczu postępu w dziedzinie technicznych metod zabezpieczania danych, człowiek coraz częściej uznawany jest za najmniej odporny element systemu zabezpieczeń informacyjnych.

Termin *socjotechnika* jest terminem cechującym się wieloznacznością, co oznacza, że może być różnie interpretowany w zależności od kontekstu działań i rozumienia przez różne grupy ludzi. W języku osób korzystających z Internetu, szczególnie specjalistów ds. cyberbezpieczeństwa, termin ten jest rozumiany w sposób opisany powyżej. Dotąd podjęto stosunkowo niewiele prób precyzyjnego zdefiniowania tego pojęcia w kontekście

[284] M. Konieczny, *Manipulacja, perswazja i socjotechnika jako formy wywierania wpływu*, Studia Prawnicze. Rozprawy i Materiały 2023, nr 2 (33), DOI: 10.48269/2451-0807-sp-2023-2-006, s. 156 i 159.
[285] K. D. Mitnick, W. L. Simon, *Sztuka podstępu…*, op. cit., s. 4.
[286] Komisja Nadzoru Finansowego, *Cyberoszustwa inwestycyjne. Termin – socjotechnika*, https://www.knf.gov.pl/dla_konsumenta/kampanie_informacyjne/cyberoszustwa_inwestycyjne/slownik [dostęp 01.03.2024 r.].

bezpieczeństwa informacji. Klasyfikacje socjotechnik zazwyczaj nawiązują do sześciu zasad wpływu społecznego sformułowanych przez Roberta Cialdiniego[287]. Proponuje się jednak alternatywne podejście klasyfikacyjne, które pozwala na podział socjotechnik na dwie główne kategorie:

a) bazujące na indukowaniu emocji.
b) opierające się na przyjmowaniu określonych ról społecznych[288].

W ramach pierwszej kategorii, skoncentrowanej na wywoływaniu emocji, można wyróżnić następujące powszechnie stosowane metody:

a) **quid pro quo** – eksploatacja zasady wzajemności;
b) **zeitnot** (presja czasu) – stworzenie sytuacji wymagającej szybkiego podjęcia decyzji, co może prowadzić do pochopnych i błędnych wyborów;
c) **baiting** (przynęta) – przedstawienie fałszywej obietnicy w celu skłonienia do podjęcia określonych działań;
d) **poor thing** (biedactwo) – odgrywanie roli osoby potrzebującej wsparcia;
e) **ingracjacja** (pochlebstwo) – psychologiczna gratyfikacja, która sprawia, że osoba odczuwa potrzebę akceptacji i dąży do spełnienia stawianych jej wymagań.

Natomiast w kategorii technik opartych na przyjmowaniu ról społecznych znajdują się:

a) **stress the position** (podkreślanie pozycji) – podszywanie się pod osobę zajmującą określoną pozycję społeczną, by wykorzystać z nią związane uprawnienia,
b) **pretexting** (tworzenie pretekstu) – kreowanie sytuacji, która usprawiedliwia nawiązanie kontaktu zawodowego lub prywatnego.

Ataki oparte na socjotechnice stanowią poważne zagrożenie ze względu na ich skryty charakter, który sprawia, że ich wykrycie jest wyjątkowo trudne. Często osoba będąca celem takiego ataku nie zdaje sobie sprawy, że została zmanipulowana do wykonania pewnych działań. Celem tych działań manipulacyjnych jest często uzyskanie dostępu do informacji, uznawanych za jedne z najbardziej wartościowych aktywów w środowisku biznesowym[289]. Ataki te są szczególnie skuteczne w dużych organizacjach z wieloma oddziałami, gdzie komunikacja wewnętrzna może być ograniczona, co utrudnia identyfikację wszystkich pracowników. W takich warunkach manipulator może łatwo podawać się za pracownika innego działu. Fundamentalnym elementem, który zwiększa podatność na tego typu ataki, jest brak świadomości na temat zagrożeń, co dotyczy zarówno dużych, jak i małych firm. Może to

[287] Por. R. B. Cialdini, *Wywieranie wpływu na ludzi. Teoria i praktyka*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2012.
[288] Ibidem.
[289] K. Malinowski, *Inwigilacja elektroniczna i bezpośrednia. Część 2*, Wydawnictwo Spyshop Expert Sp. z o. o., Poznań 2017, s. 197,

obejmować przypadki udostępniania poufnych danych w Internecie, niewystarczających systemów kontroli, czy też braku wiedzy o tym, które informacje powinny zostać zachowane wyłącznie w obrębie organizacji[290].

W dziedzinie socjotechniki obserwuje się różnorodność metod ataków, które mogą być dostosowywane, ulepszane lub łączone w zależności od specyficznych potrzeb. Większość tych metod opiera się na szeroko rozpoznawalnych i często wykorzystywanych strategiach. Poniżej przedstawiono kilka przykładów:

a) **kradzież urządzeń mobilnych** – to jedna z najstarszych metod ataku, która zyskuje na znaczeniu wraz ze wzrostem popularności urządzeń przenośnych. Efektywność tego typu ataku wzrasta w środowiskach korporacyjnych adoptujących politykę BYOD (Bring Your Own Device),
b) **shoulder-surfing** – jest to jedna z najbardziej podstawowych technik ataku, polegająca na obserwacji aktywności fizycznej użytkownika i jego urządzenia w celu uzyskania dostępu do prywatnych danych. Atakujący może obserwować ekran, klawiaturę lub ruchy rąk użytkownika,
c) **monitorowanie sieci** – analiza ruchu sieciowego pozwala zidentyfikować usługi, z których użytkownicy korzystają najczęściej. Pozwala to atakującemu na zrozumienie zabezpieczeń danej usługi i zaplanowanie potencjalnego ataku,
d) **digital dumpster diving** – postępujący rozwój technologiczny skraca czas życia urządzeń elektronicznych, co prowadzi do sytuacji, w której wycofane z użytku urządzenia, pozostawione na składowiskach elektrośmieci, mogą zawierać w swojej pamięci prywatne i poufne informacje[291].

Udział w procesie socjotechnicznym często odbywa się nieświadomie, bez znajomości faktu manipulacji przez osoby poddawane wpływom oraz bez rozumienia, że są one obiektem działań wpływowych ze strony autorytetów. Zatem działania socjotechniczne są niezamierzone z perspektywy manipulowanych jednostek, gdyż osoby posiadające wpływ na społeczeństwo eksploatują istniejące w nim relacje, utrwalając lub kreując nowe struktury społeczne lub wykorzystując znajomość procesów przyczynowo-skutkowych zachodzących w społeczeństwie.

Taka perspektywa na efektywność, przewidywalność i świadomość wpływu w kontekście socjotechnicznym napotyka istotne ograniczenia. Wynika to z faktu, iż chociaż jesteśmy świadomi występowania danego procesu i obserwujemy jego skutki, zrozumienie jego

[290] Ibidem, s. 198-199.
[291] M. Nycz, B. Michno, R. Mlicki, *Badanie efektywności ataków socjotechnicznych w jednostkach samorządu terytorialnego*, W: *Innowacyjna Gmina. Informatyka w jednostkach samorządu terytorialnego* (red.) M. Hajder. Wydawnictwo Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie, Rzeszów 2014, s. 147-148.

mechanizmów oraz identyfikacja kluczowych inicjatorów staje się zadaniem wyjątkowo złożonym.

Na podstawie raportu o stanie cyberbezpieczeństwa w 2022 r., w ramach kategorii socjotechniki zespół CSIRT GOV zidentyfikował ogółem 1 053 zdarzenia tej metody ataku, zgłoszonej przez podmioty prywatne i publiczne, odnotowując jednocześnie wzrost liczby incydentów w porównaniu do roku 2021, kiedy to zaobserwowano 904 przypadki[292].

Szantaż definiuje się jako powszechnie stosowaną strategię wpływania na jednostki, polegającą na postawieniu osoby przed dylematem: spełnienie wszelkich postulatów strony szantażującej lub ryzyko ujawnienia kompromitujących informacji[293]. Procedura organizacji i realizacji szantażu obejmuje szereg etapów:

a) identyfikację obszarów podatnych na wpływ w przypadku danej osoby,
b) selekcję konkretnej treści służącej za podstawę szantażu,
c) określenie osób, które zdaniem poszkodowanego, nie powinny mieć dostępu do dyskredytujących go danych,
d) dobór oraz przygotowanie materiału kompromitującego, niezależnie czy jest on istniejący, czy zostanie stworzony na potrzeby sytuacji,
e) wyznaczenie strategii i metodologii szantażu,
f) planowanie i koordynowanie działań mających na celu podważenie determinacji dotkniętej osoby,
g) wybór optymalnego czasu i miejsca na przeprowadzenie kluczowego elementu szantażu[294].

Identyfikacja obszarów podatnych na wpływ w przypadku danej osoby polega na dokonaniu konstatacji, iż każdy element, który jest dla jednostki cenny i którego nagła utrata budzi obawy (takie jak kariera, status społeczny, uczucia, dobrostan potomstwa, przedsiębiorczość, poparcie i uznanie ze strony określonych osób, integralność fizyczna, w tym bezpieczeństwo bliskich, oraz stabilność materialna), konstytuuje obszar jej indywidualnej podatności. W procesie identyfikacji tych aspektów niezbędne jest:

a) zdefiniowanie kluczowych motywacji, zwyczajów, aspiracji, pragnień oraz afiliacji badanego podmiotu, a także dokonanie oceny jego cech psychicznych, etycznych i charakterologicznych (takich jak skłonność do uległości, przewidywalność, skłonność do niekonwencjonalnych reakcji, zdolność do zastosowania strategii, wytrwałość, skłonność do działania pod wpływem impulsu, ambicje),

[292] *Raport o stanie bezpieczeństwa w cyberprzestrzeni*, Zespół CSIRT GOV, Warszawa 2023, s. 14.
[293] *Metody i formy pracy operacyjnej…,* op. cit., s. 110.
[294] Ibidem.

b) rozważenie, w jakim zakresie dana sytuacja może potencjalnie wpłynąć na zwiększenie wrażliwości osoby (na przykład, oczekując na awans zawodowy, jednostka może okazać się bardziej podatna na wpływ kompromitujących informacji, niż w okresie, gdy nie ma takiej możliwości)[295].

Selekcja konkretnej treści służącej za podstawę szantażu polega na dokładnej analizie zgromadzonych informacji oraz ocenie własnych zasobów do uzyskania (lub stworzenia) wymaganych dowodów, można podejść do organizacji strategii szantażu. Strategia ta może wykorzystywać różnorodne elementy, takie jak: materiały dyskredytujące mogące zaszkodzić karierze zawodowej lub działalności gospodarczej; informacje kompromitujące, które mogą pogorszyć relacje z kluczowymi osobami; fakty skandaliczne z potencjałem zniszczenia życia osobistego; materiały szkalujące dotyczące osób bliskich celu szantażu, z potencjałem niszczenia ich egzystencji; dane autentyczne lub sfabrykowane o charakterze kryminalnym. Zazwyczaj uderzenie w jedną dziedzinę życia powoduje reperkusje w innych sferach. Przykładowo, kompromitacja w sferze zawodowej może skutkować pogorszeniem relacji z istotnymi jednostkami lub destabilizacją życia rodzinnego.

Przy formułowaniu strategii szantażu kluczowe jest precyzyjne zidentyfikowanie osób, których zdaniem zainteresowanego, informacje kompromitujące powinny pozostać przed nimi ukryte za wszelką cenę (np. kierownictwo w miejscu pracy, partnerzy biznesowi, postacie publiczne, dziennikarze specjalizujący się w aferach, małżonek, przyjaciele oraz antagoniści, potencjalni przeciwnicy, przedstawiciele organów ścigania, służb specjalnych). Należy podkreślić zagrożenie udostępnieniem tych informacji właśnie tym podmiotom[296].

Dobór oraz przygotowanie materiału kompromitującego polegają na uzyskaniu lub sfabrykowaniu materiałów dźwiękowych i wizualnych, diagramów i zdjęć, kopii kluczowych dokumentów, świadectw od konkretnych osób, w taki sposób, aby zapobiec pojawieniu się ewentualnych wątpliwości u osoby będącej w zainteresowaniu. Zręcznie spreparowane dowody są konstruowane przez wyjęcie oryginalnych wypowiedzi i działań obiektu z kontekstu i nadanie im specjalnej interpretacji, która przesuwa narrację w preferowanym kierunku; sprytnie wykreowane dowody prezentują materiał w najbardziej korzystnym świetle, zwłaszcza gdy w dotychczasowym zachowaniu osoby docelowej brakuje oczywistych punktów zaczepienia, lub gdy brak czasu (lub możliwości) na szczegółowe zbadanie jej przeszłości[297].

Wyznaczenie strategii i metodologii szantażu polega na zademonstrowaniu powagi i udokumentowanie materiału co przekłada się bezpośrednio na przekonanie osoby będącej

[295] Ibidem, s. 111.
[296] Ibidem, s. 112.
[297] Ibidem, s. 112-113.

w zainteresowaniu do determinacji szantażysty do wykorzystania tego materiału w przypadku próby oporu. Następnie należy uzmysłowić osobie szantażowanej, że informacja, którą dysponuje szantażysta zostanie potraktowana poważnie przez jej otoczenie. W celu spotęgowania efektu, osoba szantażowana jest również informowana o realnych skutkach pochopnej odmowy oraz o tym, w jaki sposób mogłaby próbować się obronić i dlaczego jest to pozbawione sensu. Na koniec należy włączyć bodziec czasu, który wywiera dodatkową presję na osobę szantażowaną[298].

Planowanie i koordynowanie działań mających na celu podważenie determinacji dotkniętej osoby polega na doprowadzeniu osoby będącej w zainteresowaniu do stanu maksymalnej uległości. W tym celu można zastosować nękanie osoby szantażowanej częstymi telefonami, anonimami lub spotkaniami bezpośrednimi. Ponadto, zastosować można rozpowszechnianie fałszywych lub sfabrykowanych informacji w otoczeniu osoby szantażowanej tak aby możliwie dotkliwie umniejszyć jej wizerunek[299].

Wybór optymalnego czasu i miejsca na przeprowadzenie kluczowego elementu szantażu polega na przeprowadzaniu całej czynności podczas krótkotrwałego obniżenia siły woli osoby szantażowanej oraz w przypadku, gdy osoba chce za wszelką cenę uniknąć kompromitacji. Miejsce przeprowadzenia szantażu powinno zapewniać brak obecności osób postronnych oraz brak jakiegokolwiek wsparcia psychologicznego dla osoby szantażowanej.

Czynności związane z **pozyskaniem pracownika** rozpoczynają się od tzw. opracowania kandydata. Poprzedzone jest to typowaniem potencjalnych kandydatów według kryteriów związanych z możliwością dotarcia do osób lub obiektów współpracujących lub należących do przedsiębiorstwa będącego w zainteresowaniu oraz możliwości realizacji stawianych zadań. Wytypowany pracownik powinien:

a) posiadać wiedzę na temat przedsiębiorstwa pozostającego w zainteresowaniu i posiadać możliwość zdobywania w nim informacji lub realną perspektywę dotarcia do określonych osób lub obiektów,
b) być przydatny do wykonywana określonych zadań, w szczególności obejmujących zdobywania informacji o kadrze zarządzającej, osobach zajmujących kluczowe stanowiska, mechanizmach regulujących funkcjonowanie przedsiębiorstwa, miejscach przebywania osób posiadających kluczowe informacje,
c) posiadać predyspozycje psychiczne do wykonywania zadań oraz utrzymania faktu współpracy w ścisłej tajemnicy,

[298] Ibidem, s. 113.
[299] Ibidem, s. 114.

d) posiadać łatwość w nawiązywaniu kontaktów oraz umiejętność szybkiego opracowania i analizy uzyskiwanych informacji[300].

Samo wytypowanie kandydata powinno odbywać się w oparciu o personel zatrudniony w przedsiębiorstwie będącym w zainteresowaniu lub w oparciu o osoby pośrednio lub bezpośrednio z nim współpracujące.

Kolejnym etapem, następującym po wytypowaniu pracownika i jego opracowaniu, jest przygotowanie i przeprowadzenie rozmowy, podczas której wytypowanej osobie zostanie zaoferowana współpraca. Rozmowa ta powinna być poprzedzona odpowiednim i umiejętnym doborem motywu pozyskania wytypowanego pracownika, czyli wykorzystaniem jego negatywnych cech charakteru lub sytuacji zawodowo-personalnej. Motywem pozyskania, według Tadeusza Hanauska, mogą być następujące obszary:

a) zainteresowania materialne kandydata,
b) obawa przed ujawnieniem materiałów kompromitujących kandydata,
c) obawa przed ujawnieniem materiałów obciążających kandydata,
d) dążenie do bezkonfliktowego wykonywania swoich obowiązków,
e) niskie pobudki, np. zazdrość, zawiść, chęć zemsty, eliminacja konkurencji,
f) chęć odegrania w określonym środowisku decydującej roli, nawet anonimowo,
g) poczucie krzywdy kandydata ze strony określonego środowiska,
h) negatywne nastawienie kandydata do określonego środowiska,
i) inne, kompleksowe układy motywacyjne[301].

Według Bolesława Piaseckiego, motywy pozyskania sprowadzały się do angielskiego akronimu *MICE*, gdzie M oznacza *Money* – pieniądze, I oznacza *Ideology* – ideologię, C oznacza *Coercion* – przymus, a E oznacza *Ego* lub *Excitment* – ego lub ekscytacja[302].
Natomiast, według Krzysztofa Horosiewicza, motywy pozyskania można podzielić na te ułatwiające oraz te, które mogą utrudnić lub uniemożliwić pozyskanie[303]. Motywy ułatwiające, określa jako:

a) niskie pobudki kandydata – zazdrość, zawiść, chciwość, żądza władzy, chęć zemsty, eliminacja konkurencji,
b) pozytywne uczucia kandydata – np. chęć niesienia pomocy bliskiej osobie (ochrona),

[300] Na podstawie *Wybrane elementy taktyki werbowania i współpracy z osobowymi źródłami informacji*, Wydawnictwo WSPol, Szczytno 2019, s. 13 oraz F. Musiał, *Teoria pracy operacyjnej…,* op. cit, s. 97.
[301] T. Hanausek, *Zarys taktyki kryminalistycznej*, Dom Wydawniczy ABC, Warszawa 1994, s. 46-48.
[302] B. Piasecki, *Kontrwywiad – atak i obrona*, Wydawnictwo LTW, Łomianki 2021, s. 193.
[303] Na podstawie K. Horosiewicz, *Przedsięwzięcia werbunkowe,* „Przegląd Policyjny" 2012, nr 4 (108), s. 217-218.

c) negatywne nastawienie do określonego środowiska w ogóle lub do określonych jego części,
d) względy ambicjonalne, np. chęć zdetronizowania obecnego kierownictwa działu, zespołu itd.,
e) poczucie krzywdy, zawód wobec oczekiwań w stosunku do środowiska,
f) różne zobowiązania i inne motywacje[304].

Motywy, które mogą utrudnić lub uniemożliwić pozyskanie zostały opisane w sposób następujący:

a) brak perspektywy osiągnięcia własnych, ukrytych celów oraz obawa o utratę źródła własnych dochodów,
b) awersja do prowadzenia działań przeciwko swojemu pracodawcy lub kolegom z pracy.
c) obawa o dekonspirację,
d) nieustalone w toku opracowania nastawienie do występowania przeciwko przedsiębiorstwu będącemu w zainteresowaniu[305].

Na potrzeby pozyskania należały przyjąć odpowiednią strategię uzależnioną od motywu podjęcia współpracy kandydata oraz celu, do osiągnięcia którego jest on pozyskiwany. Analiza literatury przedmiotu i zaadaptowanie jej do realiów nieuczciwej konkurencji biznesowej, pozwoliła na wskazanie czterech głównych sposobów pozyskania:

a) jednorazowy – gdy zgoda na współpracę uzyskiwana jest podczas jednego spotkania. Ten sposób może być zastosowany wyłącznie w przypadku, gdy dokonane rozpoznanie kandydata daje niemalże pewność by w oparciu o dobrany motyw i skuteczną argumentację pozyskać rozmówcę do współpracy,
b) stopniowy – gdy zgoda na podjęcie współpracy wymaga odbycia kilku spotkań z kandydatem lub zależy od przyzwyczajenia kandydata do osoby, dla której zdobywać ma informacje. Podczas kolejnych spotkań z kandydatem, osoba prowadząca rozmowy musi przyzwyczaić kandydata do kontaktów, kształtować pozytywny stosunek do wykonywania potencjalnych zadań oraz w konsekwencji doprowadzić do *przełamania* kandydata i wyrażenia zgody na współpracę,
c) dokonywany pozornie dla innego celu – gdy kandydat nie ma oporów co do faktu samej współpracy, jednak przeszkodę stanowi cel pozyskania. Wobec czego osoba prowadząca rozmowę musi zapewnić rozmówcę, iż będzie zdobywał informacje w celu pozornie zupełnie niezwiązanym z jego miejscem zatrudnienia lub środowiskiem biznesowym w którym działa. Na dalszym etapie współpracy, kandydat jest stopniowo

[304] K. Horosiewicz, *Wybrane elementy taktyki…*, dz. cyt., s. 19-20.
[305] Ibidem.

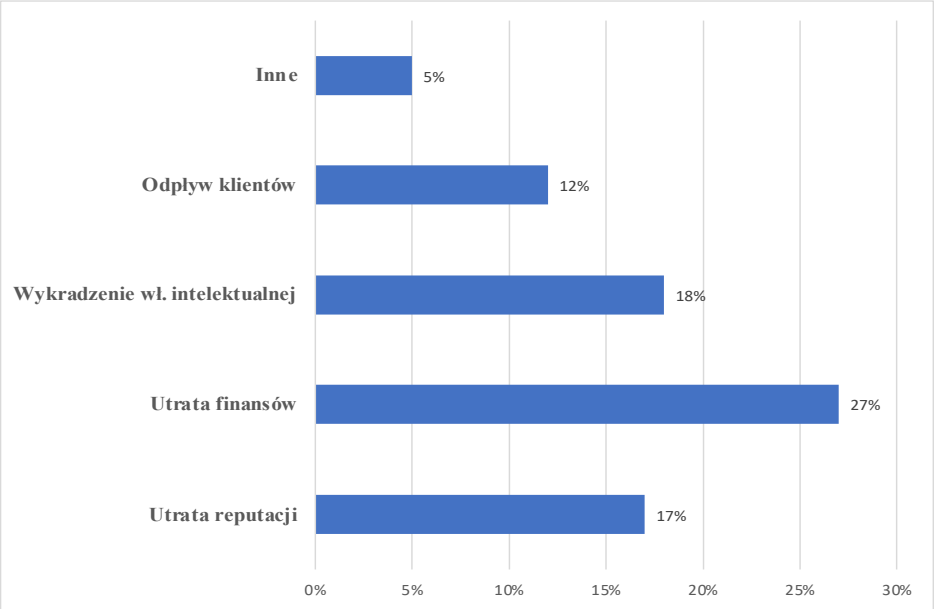
wprowadzany w faktyczny obszar zainteresowań i adekwatnie wdrażany w realizację zadań,

d) pod *obcą flagą* – gdy kandydat nie ma oporów co do faktu samej współpracy, jednak przeszkodę stanowi instytucja, z którą współpracę ma nawiązać (np. konkurencyjne przedsiębiorstwo, grupa przestępcza). W takim przypadku, osoba prowadząca rozmowę, wytwarza u kandydata przekonanie, iż współpracuje z zupełnie inną instytucją niż w rzeczywistości[306].

Pozyskanego pracownika traktuje się jako tzw. *insider'a*, czyli osobę, która dysponuje bezpośrednią wiedzą o przedsiębiorstwie będącym w zainteresowaniu. Taki pracownik nie musi być od razu osobą posiadającą szeroki dostęp do informacji oraz przydzielone szerokie uprawnienia do systemów komputerowych. W myśl zasady *po nitce do kłębka*, przedsiębiorstwo będące w zainteresowaniu grupy przestępczej lub konkurencyjnej organizacji otacza się takimi pozyskanymi pracownikami, aby uzyskać możliwie najszerszą wiedzą dotyczącą interesujących obszarów działalności[307].

Zagrożenia wewnętrzne stanowią rosnące wyzwanie dla organizacji, co potwierdzają dane z raportu przedsiębiorstwa Verizon[308], według których między 2018 a 2020 rokiem globalnie odnotowano wzrost takich zdarzeń o 47%. Wewnętrzni sprawcy są odpowiedzialni za 22% incydentów związanych z bezpieczeństwem w przedsiębiorstwach, przy czym sektory finansowy i opieki zdrowotnej są szczególnie narażone. Raport Instytutu Ponemon[309] wskazuje, że w 2020 roku 13,86% wewnętrznych zagrożeń było spowodowanych przez złośliwych pracowników działających na szkodę organizacji, a 24,75% miało na celu wykradzenie poufnych danych w ramach szpiegostwa biznesowego. Procentowy udział poszczególnych rodzajów strat z 2019 roku prezentuje poniższy wykres przedstawiony na wykresie nr 1.

[306] K. Horosiewicz, *Wybrane elementy taktyki…*, dz. cyt., s. 31-35.
[307] U. Inayat, M. Farzan, S. Mahmood, M. F. Zia, S. Hussain, F. Pallonetto, *Insider threat mitigation: Systematic literature review*, Ain Shams Engineering Journal 2024, https://doi.org/10.1016/j.asej.2024.103068, s. 3 i 6.
[308] *Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report*, Verizon, https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report [dostęp 04.04.2024 r.].
[309] *2020 Cost of Insider Threats Global Report*, Ponemon Institute, https://www.proofpoint.com/sites/default/files/observeit/2020/02/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf [dostęp 04.04.2024 r.].



Wykres 1 Efekty działalności insiderów w 2019 r. w USA i Wielkiej Brytanii
Źródło: opracowanie własne na podstawie Egress, Insider Data Breach Survey 2019, https://scoop-cms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmatters-insider-threat-research-report-a4-uk-digital.pdf [dostęp 04.04.2024 r.].

Najliczniejszą grupę stanowili jednak pracownicy działający przez nieuwagę, którzy przyczynili się do 61,39% wszystkich przypadków zagrożeń. Ten sam raport oszacował również, że w Stanach Zjednoczonych, w przedsiębiorstwach zatrudniających do 75 tys. osób, w latach 2018-2020 straty finansowe wzrosły o 31%, z 8,76 do 11,45 miliona dolarów. Poza stratami finansowymi, działania wewnętrzne powodują także inne szkody, w tym utratę reputacji, znaczny odpływ klientów oraz wykradzenie własności intelektualnej.

W niniejszym podrozdziale scharakteryzowano specyfikę zarządzania bezpieczeństwem w przedsiębiorstwach sektora ICT w kontekście zagrożeń związanych z operacyjnym pozyskiwaniem informacji. Przedstawiono koncepcję analizy operacyjnej jako metody umożliwiającej potencjalnym adwersarzom identyfikację słabych punktów w zabezpieczeniach firm. W podrozdziale wyjaśniono, jak analiza ta, polegająca na systematycznym zbieraniu i analizowaniu informacji z otwartych źródeł (OSINT), może wspierać działania konkurencji w uzyskiwaniu przewagi konkurencyjnej poprzez uzyskanie dostępu do danych, zasobów ludzkich oraz informacji o strategiach i wizerunku przedsiębiorstwa. Omówiono także ryzyka związane z metodami socjotechnicznymi, obserwacją oraz wykorzystaniem "insiderów", czyli pracowników organizacji angażujących się w działania szpiegowskie. Poruszono również zagrożenia wynikające z aktywności wewnętrznej, które mogą znacząco wpływać na bezpieczeństwo przedsiębiorstw poprzez ujawnianie poufnych danych i kradzież własności intelektualnej.

Hipoteza szczegółowa: *szpiegostwo korporacyjne stawia przed zarządzaniem bezpieczeństwem przedsiębiorstwa konieczność przeciwdziałania środkom i metodom dostępu do danych oraz pozyskiwania informacji w celu zdobycia przewagi konkurencyjnej*, znajduje potwierdzenie w kilku aspektach omawianego podrozdziału:

a) środki i metody dostępu do danych – potwierdzono, że jednym z głównych wyzwań stojących przed przedsiębiorstwami ICT jest przeciwdziałanie różnorodnym metodom nieautoryzowanego dostępu do danych, w tym poprzez analizy operacyjne, socjotechnikę, a także pozyskiwanie pracowników ("insiderów") do działań na szkodę organizacji,
b) pozyskiwanie informacji dla przewagi konkurencyjnej – opisane działania szpiegowskie, takie jak zbieranie informacji poprzez OSINT i obserwację, są bezpośrednio nakierowane na zdobycie przewagi rynkowej przez poznanie strategii i zasobów konkurencyjnych organizacji. Przedsiębiorstwa muszą zatem aktywnie monitorować i zabezpieczać swoje informacje, aby ograniczyć możliwość ich wycieku do konkurentów.

Podsumowując, tekst ten częściowo potwierdza kluczowe elementy hipotezy szczegółowej, wskazując na konieczność wdrażania zaawansowanych środków ochrony oraz zarządzania ryzykiem zewnętrznym i wewnętrznym w obszarze bezpieczeństwa informacji.

3.4 Współczesne wyzwania stawiane zarządzaniu bezpieczeństwem informacji w organizacjach sektora ICT wynikające z rozwoju technologicznego

Phishing (ang. *password harvesting fishing* – łowienie haseł) jest formą oszustwa komputerowego, polegającą na pozyskiwaniu poufnych danych, takich jak hasła do kont bankowych czy numery kart kredytowych. Oszuści, udając zaufane instytucje lub organizacje, mają na celu zdobycie danych umożliwiających dostęp do zasobów finansowych lub innych wrażliwych informacji ofiar. W ramach tego przestępstwa, sprawcy często przygotowują wiadomości e-mail, które na pierwszy rzut oka wydają się być autentyczne, imitując wygląd i treść komunikatów od renomowanych instytucji[310]. Odbiorcy są zachęcani do kliknięcia w załączony link lub otwarcie pliku, co przekierowuje ich na fałszywą stronę internetową. Strona ta, naśladująca rzeczywistą witrynę banku czy instytucji, prosi użytkowników o podanie swoich danych logowania, takich jak login, hasło czy numer PIN. Dostęp do tych informacji

[310] J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Rozprawa doktorska, Uniwersytet w Białymstoku, Białystok 2017, s. 341.

pozwala przestępcom na wykorzystanie środków finansowych ofiar lub uzyskanie dostępu do innych poufnych danych, które posiadają[311].

Zastosowanie złośliwego oprogramowania przez cyberprzestępców w obszarze bankowości elektronicznej i pozyskiwania poufnych danych może prowadzić do różnorodnych negatywnych konsekwencji, w tym:

a) zmiany numeru konta odbiorcy oraz kwoty transakcji bezpośrednio przed jej autoryzacją,
b) modyfikacji bieżącego salda konta,
c) alteracji danych w historii transakcji,
d) wyświetlenia okna internetowego wymagającego wprowadzenia kodów jednorazowych w celu weryfikacji lub aktywacji funkcji bezpieczeństwa,
e) pojawienia się prośby o podanie numeru telefonu oraz modelu urządzenia w nowo otwartym oknie przeglądarki,
f) pokazania monitu z prośbą o zwrot środków z rzekomo błędnego lub podejrzanego przelewu,
g) wyświetlenia żądania wykonania przelewu testowego jako część procedury weryfikacyjnej nowych funkcji bezpieczeństwa[312].

Cyberprzestępcy do realizacji przestępstw phishingowych wykorzystują specjalistyczne oprogramowanie złośliwe, które może mieć charakter zarówno aktywny, jak i bierny. Aktywne formy obejmują wyskakujące okna dialogowe, podczas gdy bierne to keyloggery rejestrujące wprowadzane informacje[313]. Zgodnie z analizą dokonaną przez Jerzego Kosińskiego, główne cechy charakterystyczne takiego złośliwego oprogramowania obejmują:

a) funkcje samoobrony, w ramach których złośliwe oprogramowanie dezaktywuje programy antywirusowe oraz blokuje aktualizacje oprogramowania, modyfikuje działanie firewalli,
b) możliwość zdalnego zarządzania, w tym instalację aplikacji umożliwiających zdalny dostęp do zainfekowanego komputera i przekierowywanie ruchu sieciowego na serwer pośredniczący,
c) kradzież danych identyfikacyjnych, takich jak hasła, identyfikatory użytkownika, adresy e-mail czy certyfikaty SSL[314].

[311] A. Kiedrowicz-Wywiał, *Pharming i jego penalizacja*, „Prokuratura i Prawo" 2011, nr 6, s. 24-25.
[312] J. Worona, *Cyberprzestrzeń a prawo…,* op. cit., s. 342.
[313] Ibidem.
[314] J. Kosiński, *Cyberprzestępczość*, W: W. Jasiński (red.), *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, Szczytno 2013, s. 475.

Fałszywe strony internetowe, wykorzystywane przez przestępców, naśladują oryginalne witryny bankowe z zachowaniem ich graficznego wyglądu, co może wprowadzić użytkowników w błąd. Cyberprzestępcy natychmiastowo wykorzystują zdobyte w ten sposób informacje.

W kontekście cyberbezpieczeństwa, obok tradycyjnego phishingu istotne jest wyróżnienie bardziej niebezpiecznej formy tego ataku, znanego jako spear phishing. Ten typ ataku jest celowo skierowany na indywidualne osoby lub instytucje[315]. Zamiast rozsyłania ogólnych e-maili do losowych użytkowników sieci Internet, przestępcy dokonują starannego wyboru ofiar[316]. Odbiorcy, którzy otrzymują wiadomość pozornie autentyczną, mogą błędnie uznać ją za komunikat od nadawcy takiego jak przełożony, administrator systemu, partner biznesowy lub przedstawiciel współpracującej instytucji. W rzeczywistości jest to jednak wiadomość fałszywa, mająca na celu wyłudzenie poufnych informacji, takich jak szczegóły dotyczące przedsiębiorstwa czy dane dostępowe do systemów. Ataki typu spear phishing często poprzedza kompleksowa analiza i rozpoznanie celu przez cyberprzestępców, stanowiąc początek bardziej skomplikowanych działań mających na celu ominięcie zabezpieczeń. Warto pamiętać, że tego typu ataki są głównie przeprowadzane w celach szpiegostwa biznesowego i kradzieży poufnych danych, podczas gdy standardowe ataki phishingowe zazwyczaj mają na celu oszustwa finansowe lub kradzież tożsamości, skierowane do szerokiej grupy odbiorców[317].

Oprócz spear phishingu, istotnym zagrożeniem jest również whaling (ang. *whale* – wieloryb, polowanie na tzw. *grubą rybę*), będący formą ataku phishingowego[318] skierowaną na wyższe kadry kierownicze przedsiębiorstw czy instytucji[319]. Przestępcy w tym przypadku poświęcają znaczne zasoby czasu na analizę profilu wybranej ofiary, podobnie jak w spear phishingu, aby ustalić optymalny moment i sposób na uzyskanie dostępu do danych logowania lub autoryzacji. Tego rodzaju ataki niosą ze sobą wysokie ryzyko, gdyż osoby na stanowiskach kierowniczych mają dostęp do szerokiego zakresu poufnych danych dotyczących organizacji, w której pracują. Dodatkowo, wyróżnić można vishing, czyli phishing głosowy, który odbywa się za pośrednictwem rozmów telefonicznych. Metoda ta ma na celu wyłudzenie poufnych

[315] M. Tuz, *Wpływ cyberzagrożeń na funkcjonowanie organizacji*, Przegląd Policyjny 2023/151(3), s. 26.
[316] M. Mozgawa, *Phishing w ujęciu prawnokarnym* W: *Współczesne oblicza prawa karnego, prawa wykroczeń, kryminologii i polityki kryminalnej. Księga jubileuszowa dedykowana Profesor Violetcie Konarskiej-Wrzosek* (red.) J. C. Bojarski, N. Daśko, J. Lachowski, T. Oczkowski, A. Ziółkowska, Wydawnictwo: Wolters Kluwer Polska, Warszawa 2023, s. 641-642.
[317] Ibidem.
[318] M. Matacz, W. Vodičková, *Zjawisko phisingu w Polsce*, De Securitate Et Defensione. O Bezpieczeństwie I Obronności, 9 (1) 2023, https://doi.org/10.34739/dsd.2023.01.09, s. 116.
[319] *What is Phishing?*, CISCO, https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html [dostęp 15.04.2024 r.].

informacji, takich jak dane dostępowe lub autoryzacyjne, poprzez oszukańcze manipulacje rozmówcę[320].

W 2022 roku najczęściej raportowanym rodzajem incydentów cybernetycznych były te związane z oszustwami komputerowymi, w tym przede wszystkim phishingiem. Według danych CERT Polska, zarejestrowano 25 625 przypadków phishingu, co odpowiada 64% wszystkich zgłoszonych incydentów w tym roku. Liczba zgłoszeń związanych z phishingiem także była znacząca, osiągając poziom 82 830. Najczęściej wykorzystywanym wizerunkiem w atakach phishingowych była firma kurierska InPost, z 5 119 zarejestrowanymi przypadkami. Wysokie miejsce w statystykach zajęły również incydenty związane z platformą mediów społecznościowych Facebook, która odnotowała 4 370 incydentów oraz serwis ogłoszeniowy Vinted z 2 926 zgłoszeniami[321].

Rosnąca zależność od sieci Internet w zarządzaniu informacjami i trendu ku elektronicznej wymianie wrażliwych danych, spoofing stanowi rosnące zagrożenie dla zasobów cyfrowych[322]. **Spoofing**, czyli rodzaj działalności cyberprzestępczej, polega na podszyciu się pod inną osobę lub instytucję przez sfałszowanie informacji nadawcy, co może prowadzić do nieuprawnionego uzyskania dostępu do informacji osobistych, przejęcia środków finansowych, rozprzestrzeniania złośliwego oprogramowania lub kradzieży danych[323]. Według definicji przygotowanej przez Ministerstwo Cyfryzacji, Spoofing to rodzaj ataku, w którym przestępcy podszywają się pod banki, instytucje i urzędy państwowe, przedsiębiorstwa, a nawet osoby fizyczne w celu wyłudzenia od swoich ofiar danych lub pieniędzy. Dzięki wykorzystaniu różnych technik, oszuści mogą podszyć się pod wybrany adres e-mail, numer telefonu, a nawet adres IP i w nieuczciwy sposób osiągnąć swoje cele[324].

Spoofing wiadomości e-mail, będący najczęstszym typem spoofingu, charakteryzuje się trudno wykrywalnymi emailami z fałszywym poczuciem pilności. Oznaki takich maili to m.in. niepoprawna gramatyka, błędy ortograficzne, niewłaściwie skonstruowane zdania i frazy czy nieprawidłowe adresy URL i błędnie napisane adresy nadawcy[325].

---

[320] Ibidem.

[321] *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu*. NASK-PIB/CERT Polska, https://cert.pl/uploads/docs/Raport_CP_2022.pdf [dostęp 15.04.2024 r.], s. 36.

[322] A. Khan, K. M. Malik, J. Ryan, M. Saravanan, *Battling voice spoofing: a review, comparative analysis, and generalizability evaluation of state-of-the-art voice spoofing counter measures*, Artificial Intelligence Review Vol. 56 (2023), https://doi.org/10.1007/s10462-023-10539-8, s. 3 i 6.

[323] *What Is Spoofing?*, CISCO, https://www.cisco.com/c/en/us/products/security/email-security/what-is-spoofing.html?dtid=osscdc000283 [dostęp 15.04.2024 r.].

[324] *Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?*, Ministerstwo Cyfryzacji, https://www.gov.pl/web/cyfryzacja/czym-jest-spoofing--jak-go-rozpoznac-i-nie-dac-sie-nabrac [dostęp 15.04.2024 r.].

[325] Ibidem.

Obrona przed spoofingiem obejmuje wielowarstwowe podejście do zabezpieczeń poczty elektronicznej, które powinno obejmować solidną ochronę przed phishingiem, spoofingiem, kompromitacją poczty biznesowej i innymi cyberzagrożeniami[326]. Środki obronne powinny umożliwiać wykrywanie, blokowanie i usuwanie zagrożeń dotyczących zarówno poczty przychodzącej, jak i wychodzącej. Warto szukać rozwiązań takich jak:

a) inteligencja zagrożeń klasy światowej umożliwiająca szybkie działanie wobec wykrytych zagrożeń,
b) wieloczynnikowa autentykacja chroniąca przed kradzieżą danych uwierzytelniających,
c) ochrona przed phishingiem zatrzymująca zagrożenia związane z oszustwami,
d) autoryzacja DMARC oraz środki egzekwujące chroniące reputację marki,
e) ochrona przed złośliwym oprogramowaniem rozpoznająca ryzykowne pliki w załącznikach oraz zapewniająca bezpieczeństwo w izolowanym środowisku (sandboxing),
f) szkolenie użytkowników końcowych, aby ciągle poszerzać i wdrażać wiedzę na temat ryzyka cyberbezpieczeństwa.

Istnieją również inne typy spoofingu, takie jak smishing (wykorzystanie wiadomości SMS), spoofing identyfikatora dzwoniącego, spoofing URL, spoofing adresów IP i spoofing DNS. Wszystkie te metody mają na celu podszywanie się pod inne systemy lub osoby w celu uzyskania nieuprawnionych korzyści, często prowadząc do poważnych konsekwencji, takich jak kradzież tożsamości, oszustwa finansowe i kompromitacja bezpieczeństwa sieci.

Aby skutecznie bronić się przed atakami spoofingowymi, organizacje i użytkownicy indywidualni powinni być świadomi różnorodnych form spoofingu i podejmować odpowiednie środki ochronne. Obejmuje to edukację o technikach i oznakach ostrzegawczych spoofingu, aktualizację oprogramowania i zabezpieczeń oraz implementację solidnych protokołów bezpieczeństwa, w tym regularne oceny podatności na zagrożenia.

Spoofing stanowi wyzwanie dla instytucji finansowych i inwestorów, mając wpływ na zaufanie do systemu finansowego i przejrzystość rynku. Ta zwodnicza praktyka rozciąga się daleko poza bezpośrednie straty finansowe, erodując zaufanie do systemów finansowych i utrudniając transparentność rynkową. Spoofing może generować znaczącą niestabilność rynkową, prowadząc do strat inwestycyjnych i wprowadzając zakłócenia w funkcjonowanie rynków finansowych[327]. Spoofing jest nie tylko wyzwaniem dla pojedynczych inwestorów, ale

[326] K. Radoš, M. Brkic, D. Begušic, *Recent Advances on Jamming and Spoofing Detection in GNSS*, Sensors 2024, 24, 4210, https://doi.org/10.3390/s24134210, s. 10-12.
[327] V. Dalko, B. Michael, M. Wang, *Spoofing: effective market power building through perception alignment*, Studies in Economics and Finance Vol. 37 No. 3 (2020), https://doi.org/10.1108/SEF-09-2019-0346, s. 506-507.

ma także szersze konsekwencje dla regulatorów oraz całości ekonomii, potencjalnie prowadząc do zmniejszenia wzrostu gospodarczego oraz hamowania rozwoju biznesu i przemysłu[328].

W celu przeciwdziałania spoofingowi, instytucje finansowe oraz regulatorzy powinni wdrożyć skuteczne mechanizmy nadzoru i egzekwowania przepisów, w tym zwiększone monitorowanie aktywności handlowych i surowsze kary za spoofing, aby przywrócić zaufanie do systemu finansowego i zagwarantować przejrzystość rynku. Wprowadzenie surowszych sankcji dla sprawców spoofingu przesyła jasny komunikat, że manipulacje rynkowe nie będą tolerowane, co w efekcie powinno ograniczyć przyszłe incydenty spoofingu[329].

Organizacje i dostawcy usług muszą wdrożyć wytrzymałe protokoły bezpieczeństwa oraz regularnie przeprowadzać oceny podatności, aby identyfikować i minimalizować potencjalne słabości, które mogłyby zostać wykorzystane w atakach typu spoofing. Jest to niezbędne dla ochrony integralności systemów finansowych oraz ograniczenia negatywnych skutków finansowych spoofingu. Poprzez dostosowanie się do nowoczesnych technik nadzoru, edukację uczestników rynku o ryzyku związanym ze spoofingiem oraz współpracę z globalnymi organami regulacyjnymi, sektor finansowy może utrzymać krok wyprzedzając oszustów i zabezpieczać stabilność oraz wiarygodność systemu finansowego.

Nowa ustawa anty-spoofingowa i anty-smishingowa[330], przyjęta po roku debat i prac, wprowadza zintegrowane środki do walki z tymi formami oszustwa. Ustawa nakłada na telekomy obowiązek stosowania technologii wykrywających i blokujących spoofing oraz smishing, a także tworzy wykazy numerów banków i innych instytucji ułatwiające identyfikację oszustów. CSIRT NASK otrzymało zadanie monitorowania smishingu oraz prowadzenia wykazów nadpisów używanych przez podmioty publiczne, które pomogą w eliminowaniu oszustw. Ponadto, ustawa określa szczegółowe obowiązki dla przedsiębiorców sektora technologii informacyjno-komunikacyjnych, w tym blokowanie połączeń i wiadomości społecznościowych zgodnie z wykrytymi wzorcami nadużyć. Zawarte są również przepisy karne dla naruszeń oraz mechanizmy obronne dla dostawców usług email. Główne założenia ustawy:

a) **walka z nadużyciami w komunikacji elektronicznej –** ustawa definiuje i proponuje walkę ze zjawiskiem spoofing'u i smishing'u poprzez zintegrowane podejście technologiczne i regulacyjne,

[328] Por. D. Deb., A. K. Jain, *Look locally infer globally: A generalizable face anti-spoofing approach*, IEEE Transactions on Information Forensics and Security, 16 (2020), s. 1143-1148.
[329] Na podstawie *What Is Spoofing…*, op. cit. oraz *Czym jest spoofing…,* op. cit.
[330] Ustawa z dnia 28 lipca 2023 r. *o zwalczaniu nadużyć w komunikacji elektronicznej* (Dz.U. 2023 poz. 1703).

b) **obowiązki dla telekomów i CSIRT NASK –** telekomy mają obowiązek wykorzystania technologii do blokowania oszustw, a CSIRT NASK ma monitorować i edukować w zakresie smishing'u,
c) **wykazy i rejestracje –** tworzenie i utrzymanie wykazów numerów oraz nadpisów ma pomóc w łatwiejszej identyfikacji i blokadzie podejrzanych działań,
d) **przepisy karne i ochrona przed nadużyciami –** ustawa wprowadza kary pieniężne i możliwości karania za nieprzestrzeganie nowych przepisów, jak również zawiera mechanizmy ochronne dla operatorów i użytkowników końcowych[331].

Ustawa reprezentuje kompleksowy atak na problemy związane z cyberbezpieczeństwem i socjotechniką, wprowadzając zarówno prewencyjne, jak i pociągające do odpowiedzialności rozwiązania mające na celu ochronę użytkowników i usług telekomunikacyjnych w Polsce.

Spyware (*software szpiegujący*) w kontekście zarządzania systemami informacyjnymi, jest uznawany za jedno z największych zagrożeń dla integralności i poufności danych w strukturach korporacyjnych. Jego istotą jest nieautoryzowane zbieranie informacji o działaniach użytkowników oraz przetwarzanych przez nich danych. Ingeruje to w prywatność osób i stanowi realne niebezpieczeństwo dla bezpieczeństwa danych przedsiębiorstw, co podkreśla konieczność wnikliwego poznania charakterystyki oraz metod przeciwdziałania[332].

Spyware zakorzenia się w systemach komputerowych, często wykorzystując luki w zabezpieczeniach lub instalując się razem z innym, pozornie legalnym oprogramowaniem[333]. Wskazana aplikacja lub jej fragmenty kodu działają w ukryciu, rejestrując każdą akcję użytkownika – od naciśnięć klawiszy, przez dane wprowadzane w przeglądarkach internetowych, aż po zmiany w konfiguracji systemu oraz treści rozmów elektronicznych[334].

Przestępcy internetowi używają spyware jako narzędzia do pozyskiwania poufnych danych korporacyjnych, w tym informacji finansowych, danych osobowych pracowników, a nawet praw autorskich i innych wartości niematerialnych. Przykładowo, wykorzystują inżynierię społeczną i phishing, aby nakłonić użytkownika do uruchomienia zainfekowanego

---

[331] N. Bochyńska, *To koniec smishingu i spoofingu? Zobacz, co się zmieni*, Cyberdefence24.pl, https://cyberdefence24.pl/polityka-i-prawo/wchodzi-w-zycie-wazna-ustawa-o-smishingu-i-spoofingu-zobacz-co-sie-zmieni {dostęp 15.04.2024 r.] oraz M. Maj, *Koniec ze scamami przez telefon? Rusza wykaz DNO a w życie wchodzi ustawa antyspoofingowa,* Niebezpieczenik.pl, https://niebezpiecznik.pl/post/rusza-dno-czyli-ustawa-anty-spoofingowa/ [dostęp 15.04.2024 r.].

[332] D. H. Kwak, D. M. Kizzier, E. Jung, *Spyware Knowledge in Anti-Spyware Program Adoption: Effects on Risk, Trust, and Intention to Use*, 2011 44th Hawaii International Conference on System Sciences, Kauai, HI, USA, 2011, doi: 10.1109/HICSS.2011.382, s. 1-3.

[333] M. Naser, H. Bazar, H. Abdel-Jaber, *Mobile Spyware Identification and Categorization: A Systematic Review*, Informatica 47 (2023), https://doi.org/10.31449/inf.v47i8.4881, s. 48 i 50.

[334] C. Onwubiko and A. P. Lenaghan, *Managing Security Threats and Vulnerabilities for Small to Medium Enterprises,* 2007 IEEE Intelligence and Security Informatics, New Brunswick, NJ, USA, 2007, doi: 10.1109/ISI.2007.379479, s. 244-249.

załącznika. Takie działania mogą prowadzić do znaczących strat finansowych i naruszeń regulacji ochrony danych, jak również mogą stanowić wstęp do dalszych, bardziej złożonych ataków cybernetycznych, takich jak ransomware (ang. *ransom* – okup i *software* – oprogramowanie)[335].

Strategie obronne przed spyware muszą być kompleksowe, obejmując zarówno techniczne aspekty bezpieczeństwa, jak i edukację pracowników. Obejmują one regularne aktualizacje oprogramowania, stosowanie narzędzi antyspyware, implementację wielopoziomowych strategii uwierzytelniania, a także przeprowadzanie regularnych audytów bezpieczeństwa i testów penetracyjnych. Szczególnie istotne w obliczu ewolucji zagrożeń są szkolenia personelu, mające na celu podnoszenie świadomości na temat metod działania spyware oraz sposobów rozpoznawania potencjalnych prób infekcji[336].

W świetle bieżących trendów i przewidywań, przyszłość spyware związana jest z rozwojem technologii sztucznej inteligencji, której zadaniem będzie wykrywanie i blokowanie tego typu oprogramowania[337]. Wzrost liczby ataków na urządzenia mobilne i Internet Rzeczy (IoT) wymusza na przedsiębiorstwach ciągłe dostosowywanie swoich strategii bezpieczeństwa, szczególnie w kontekście zwiększonego ryzyka związanego z pracą zdalną i trendem BYOD (Bring Your Own Device)[338].

Ataki z wykorzystaniem spyware stanowią wyrafinowaną formę cyberzagrożenia, której celem jest infiltracja korporacyjnych systemów informacyjnych w celu wykradzenia wrażliwych danych biznesowych i osłabienia ich struktur bezpieczeństwa. Jako przykład takich ataków można przedstawić następujące wydarzenia:

a) **FinFisher lub FinSpy –** FinFisher, znany także jako FinSpy, zyskał złą sławę w 2010 roku. Rozwinięty pod pozorem wykorzystania przez organy ścigania i wywiad, szybko stał się narzędziem, za pomocą którego rządy szpiegowały swoich obywateli. Badanie przeprowadzone przez Citizen Lab w 2015 roku ujawniło alarmujący zasięg FinFishera, identyfikując 33 prawdopodobnych rządowych użytkowników w 32 krajach oraz obecność głównego serwera FinFishera – centrum operacji szpiegowskich – w tych państwach. Liczby te szokują nie tylko z powodu ilości zaangażowanych rządów, ale również ze względu na implikacje dla prywatności i praw człowieka,

[335] Z. Li, A. Oprea, Operational *Security Log Analytics for Enterprise Breach Detection*, 2016 IEEE Cybersecurity Development (SecDev), Boston, MA, USA, 2016, doi: 10.1109/SecDev.2016.015, s. 15-19.
[336] H. Xu, Y. Zhou, C. Gao, Y. Kang, M. R. Lyu, *SpyAware: Investigating the privacy leakage signatures in app execution traces*, 2015 IEEE 26th International Symposium on Software Reliability Engineering (ISSRE), Gaithersbury, MD, USA, 2015, doi: 10.1109/ISSRE.2015.7381828, s. 348-352.
[337] Ibidem, s. 353-355.
[338] S. N. Swamy, D. Jadhav, N. Kulkarni, *Security threats in the application layer in IOT applications*, 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, doi: 10.1109/I-SMAC.2017.8058395, s. 477-480.

b) **Regin –** oprogramowanie, które pojawiło się na początku lat 2010, odkrywa historię globalnego cyber-szpiegostwa o szczególnym rozkładzie geograficznym. Dane ze Społeczności Broadcom wykazały, że spośród komputerów na całym świecie zainfekowanych przez Regin, aż 28 procent znajdowało się w Rosji, a 24 procent w Arabii Saudyjskiej, dodatkowo Meksyk i Irlandia stanowiły po 9 procent infekcji. Dane te nie tylko podkreślają szeroki wpływ Regin, ale również sugerują strategiczne ukierunkowanie na konkretne regiony, co pozostaje przedmiotem spekulacji i debaty w kręgach cyberbezpieczeństwa,

c) **DarkHotel –** w krajobrazie cyfrowego szpiegostwa DarkHotel wyróżnia się jako szczególnie podstępny przykład. Po raz pierwszy zidentyfikowany w 2014 roku, ten szpiegujący software specjalizował się w celowaniu w wysokiej rangi osoby w luksusowych hotelach. Metoda działania DarkHotel była zarówno pomysłowa, jak i niepokojąca: wykorzystywała sieci Wi-Fi hoteli do infiltracji urządzeń celowych gości, często wysokich rangą wykonawców lub urzędników rządowych, umożliwiając DarkHotel dyskretne zbieranie wrażliwych informacji przez długi czas.

d) **Pegasus –** Pegaz, nazwa, która budzi niepokój w świecie spyware'u, napotykamy na przerażający przykład możliwości technologii nadzoru. Pegaz, który zdobył notoryczność w połowie lat 2010, został opracowany rzekomo w celu śledzenia przestępców i terrorystów, jednak jego zastosowanie szybko przeszło na kontrowersyjne terytoria. Raport z udziałem Laboratorium Bezpieczeństwa Amnesty International i Citizen Lab ujawnił głęboko niepokojące statystyki: próby włamań lub udane włamania na 37 telefonów komórkowych należących do osób o wysokim profilu. Zaawansowanie Pegaza pozwoliło mu potajemnie infiltrować smartfony, przekształcając je w urządzenia szpiegowskie bez wiedzy właścicieli. Szczególne kontrowersje program budził w Polsce, po ujawnieniu inwigilacji polityków i urzędników państwowych[339],

e) **Havex** lub **Dragonfly** – w połowie lat 2010 krajobraz cyberbezpieczeństwa był świadkiem pojawienia się szczególnie ukierunkowanego spyware: Havex, znany również jako Dragonfly. Ta zaawansowana kampania cyber-szpiegowska wyróżniała się skupieniem na systemach sterowania przemysłowego. To, co wyróżnia Dragonfly, to szerokie i strategiczne ukierunkowanie. Eksperci z Dragos.com szacują, że kampania Dragonfly wpłynęła na ponad 2000 witryn. Liczby te są nie tylko świadectwem skali kampanii, ale także jej precyzji. Strony te nie zostały wybrane przypadkowo; zostały

[339] N. Loba, *O "Pegazie", czyli fakty zamiast mitu*, Infosecurity24.pl, https://infosecurity24.pl/sluzby-specjalne/o-pegazie-czyli-fakty-zamiast-mitu-opinia [dostęp 15.04.2024 r.].

starannie wyselekcjonowane ze względu na ich znaczenie w sektorach krytycznej infrastruktury. Strategia ta podkreśla zmianę w taktykach cyber-szpiegostwa - od zbierania danych do potencjalnego zakłócania niezbędnych usług. Oprogramowanie Havex zostało zaprojektowane do infiltracji i badania tych systemów, przygotowując grunt pod możliwe przyszłe zakłócenia. Wpływ Dragonfly wykracza poza zwykłą kradzież danych, stanowiąc znaczące zagrożenie dla bezpieczeństwa operacyjnego istotnych usług i branż[340].

W konkluzji, zrozumienie działania i skutków ataku spyware, wraz ze stosowaniem skutecznych metod obronnych, jest niezbędne do ochrony przedsiębiorstwa przed nieautoryzowanym dostępem i potencjalnymi szkodami. Zapewnienie bezpieczeństwa informacyjnego wymaga stałej czujności oraz adaptacji do dynamicznie zmieniającego się środowiska cybernetycznego.

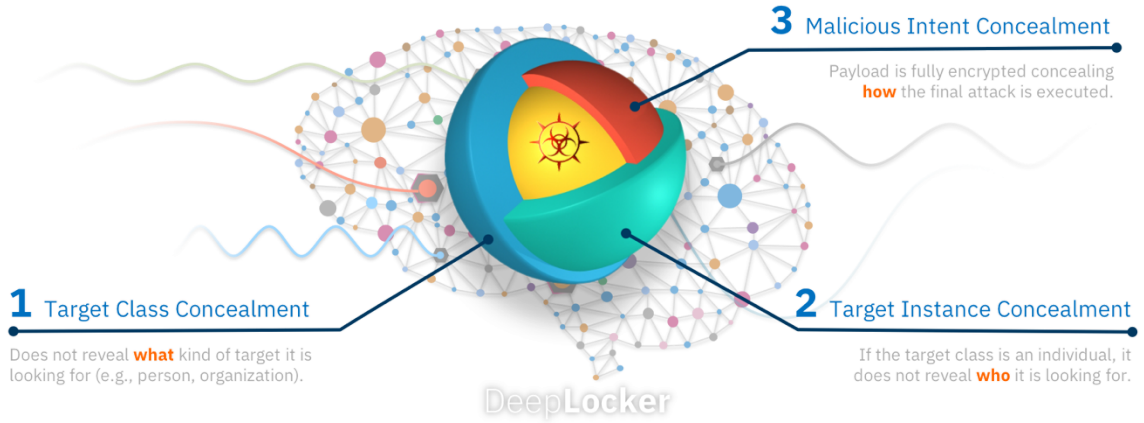
Sztuczna inteligencja (ang. *Artificial Intelligence, AI*) wraz z powiązanym uczeniem maszynowym (ang. *Machine Learning, ML*) stanowią kluczowy problem współczesnej zarządzania: ich zastosowanie w procesie podejmowania decyzji dotyczących osób. Obserwuje się trend utraty zrozumienia dla tej technologii oraz malejącą kontrolę nad jej konsekwencjami przez osoby niezwiązane bezpośrednio z jej rozwojem[341]. W konsekwencji, zarządzanie danymi statystycznymi, a szczególnie uczenie maszynowe, staje się centralnym wyzwaniem dla bezpieczeństwa organizacji[342]. Kluczowe staje się pytanie o odpowiedzialność firm za wykorzystywanie i dystrybucję danych, oraz konsekwencje tych działań. Ta problematyka jest ściśle związana z kwestią niezależnych audytów oraz stosowaniem adekwatnych regulacji prawnych. Przyszły rozwój tych obszarów będzie miał istotny wpływ na bezpieczeństwo przedsiębiorstw.

Należy także podkreślić postępy w dziedzinie głębokiego uczenia (ang. *Deep Learning, DL*), które stanowi specjalistyczną gałąź uczenia maszynowego. Koncentruje się ono na projektowaniu sieci neuronowych, mających na celu usprawnienie technologii rozpoznawania mowy i przetwarzania języka ludzkiego[343]. Innowacyjność cyberprzestępców nie zna granic, a rozwój technologii sztucznej inteligencji oferuje im możliwości do kreowania nowych,

[340] T. Moes, *Spyware Examples (2024): The 5 Worst Attacks of All Time*, SoftwareLab.org, https://softwarelab.org/blog/spyware-examples/ [dostęp 15.04.2024 r.].
[341] P. Herman, *Ochrona zasobów informatycznych przed szpiegostwem gospodarczym*, W: *Ochrona przedsiębiorstwa przed szpiegostwem gospodarczym. Prawne i praktyczne aspekty zapewnienia bezpieczeństwa aktywów przedsiębiorcy* (red.) P. Herman, P. Łabuz, T. Safjański, Wydawnictwo Difin, Warszawa 2021, s. 175.
[342] J. P. Bharadiya, *A Comparative Study of Business Intelligence and Artificial Intelligence with Big Data Analytics*, American Journal of Artificial Intelligence 2023 7(1), doi: 10.11648/j.ajai.20230701.14, s. 29.
[343] N. Mungoli, *Scalable, Distributed AI Frameworks: Leveraging Cloud Computing for Enhanced Deep Learning Performance and Efficiency*, Computer Science 2023, https://doi.org/10.48550/arXiv.2304.13738, s. 3 i 7.

bardziej zaawansowanych cyberataków[344]. Wykorzystują oni oprogramowanie oparte na uczeniu maszynowym (ML) oraz głębokim uczeniu (DL) do zwiększania częstotliwości i skomplikowania ataków. Projektowane są także nowe warianty złośliwego oprogramowania, których celem jest modyfikacja struktury w sposób umożliwiający uniknięcie wykrycia[345].

Jednym z nowo powstałych złośliwych oprogramowań, które wkrótce może być powszechnie wykorzystywane przez cyberprzestępców, jest DeepLocker[346]. To zaawansowane narzędzie opiera się na modelu sztucznej inteligencji, skrywając swoje zamiary aż do momentu dotarcia do określonej ofiary. Ujawnia swoje złośliwe funkcje tylko wtedy, gdy model AI rozpozna cel na podstawie czynników takich jak rozpoznawanie twarzy, geolokalizacja czy identyfikacja głosu. Cechy tego oprogramowania zostały przedstawione na rysunku nr 21.



Rysunek 21 DeepLocker - ukrycie zapewniane przez sztuczną inteligencję
Źródło: M. P. Stoecklin, J. Jang, D. Kirat, DeepLocker: How AI Can Power…, op. cit.

Głównym zadaniem tego oprogramowania jest uniknięcie wykrycia przez programy antywirusowe poprzez ukrywanie się w powszechnie używanych aplikacjach, na przykład w narzędziach do wideokonferencji[347]. Charakterystyczną cechą DeepLocker jest trudność w wykryciu i neutralizacji tego rodzaju zagrożenia. Zastosowanie technologii głębokiego uczenia (DL) umożliwia uaktywnienie złośliwej zawartości wyłącznie w momencie identyfikacji celu[348].

Wracając do omawianego wcześniej zjawiska phishingu, w kontekście AI istnieją zestawy narzędzi, które ułatwiają tworzenie materiałów wykorzystywanych w atakach

[344] P. Herman, *Ochrona zasobów informatycznych…*, op. cit., s. 176.
[345] A. A. Mughal, *Building and Securing the Modern Security Operations Center (SOC)*, International Journal of Business Intelligence and Big Data Analytics, 5(1) 2022, s. 15 i 19.
[346] M. P. Stoecklin, J. Jang, D. Kirat, *DeepLocker: How AI Can Power a Stealthy New Breed of Malware*, SecurityIntelligence, https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/ [dostęp 15.04.2024 r.].
[347] P. Herman, *Ochrona zasobów informatycznych…*, op. cit.
[348] M. P. Stoecklin, J. Jang, D. Kirat, *DeepLocker: How AI Can Power…,* op. cit.

phishingowych. Te zestawy wymagają od operatorów-botów wybrania kontekstu i redagowania treści dialogu. Jednakże, dzięki nowoczesnym i przyszłym postępom w rozwoju chatbotów, sama sztuczna inteligencja będzie mogła generować dialogi i uczyć się na podstawie interakcji, aby stać się bardziej skuteczną w inżynierii społecznej[349]. Jest to krok dalej niż efekt Elizy, w którym AI pełni rolę psychoterapeuty. Eliza, program komputerowy, zadawała pytania użytkownikom i przekształcała ich odpowiedzi w pytania, tworząc wrażenie głębszego zgłębiania problemu[350]. Zwykle kończyło się to na tym, że osoba wierzyła, iż Eliza doskonale rozumie jej problem, mimo że był on zbyt skomplikowany, aby Eliza mogła go pojąć. AI wykorzystujące efekt Elizy uczą się z ludzkich zachowań i korzystają z tych społecznych wzorców jako szablonu, aby lepiej nauczyć się zachowywać jak człowiek. Taki rodzaj AI jest szczególnie skuteczny w inżynierii społecznej i dzięki uczeniu maszynowemu będzie ewoluować, stając się coraz bardziej efektywny.

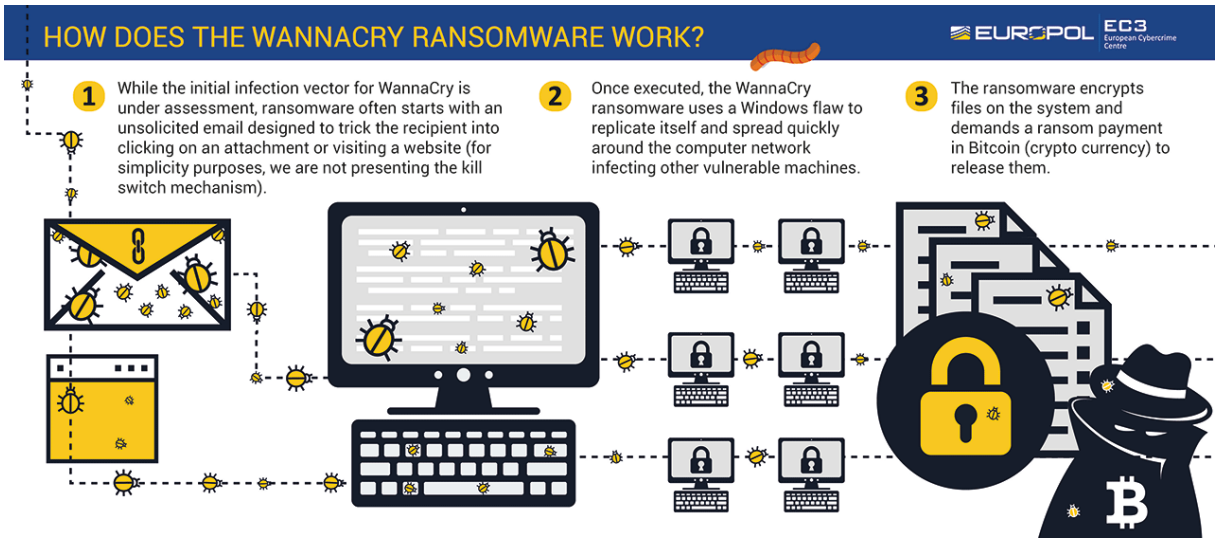
Jedną z głównych metod rozprzestrzeniania złośliwego oprogramowania są ataki phishingowe, które polegają na wysyłaniu fałszywych wiadomości pozornie pochodzących od legalnych i zaufanych nadawców. Wiadomości te mają na celu oszukanie odbiorców, aby ujawnili osobiste lub wrażliwe informacje firmowe, takie jak hasło do konta, dane logowania czy numery kart kredytowych. Wiadomości mogą zachęcać odbiorcę do odwiedzenia strony internetowej w celu aktualizacji lub weryfikacji danych osobowych, podając link, który zainstaluje złośliwe oprogramowanie na komputerze użytkownika lub otworzy załącznik e-mail, który uczyni to samo. Phishing jest jedną z najłatwiejszych form ataków cybernetycznych, a sztuczna inteligencja może znacząco zwiększyć efektywność i łatwość jego implementacji. Stanowi to zagrożenie zarówno dla firm, jak i osób prywatnych. Program AI, prosty jak chatbot, po odpowiednim rozwoju, może zdobyć informacje od osoby i działać jako wirtualny phisher[351].

Sztuczna inteligencja posiada potencjał do intensyfikacji zarówno zagrożeń, jak i mechanizmów obronnych w cyberbezpieczeństwie. Najlepiej ilustruje to model wyścigu zbrojeń w obszarze AI. W miarę jak AI zwiększa efektywność ataku, tak samo obrona wykorzystuje AI do autonomicznego łatania/ochrony przed danym atakiem[352]. Przykładem tego jest oprogramowanie typu ransomware, gdzie ostatnie badania wykazują stały spadek jego

[349] R. Alabdan, *Phishing Attacks Survey: Types, Vectors, and Technical Approaches*, Future Internet 12, no. 10 (2020), https://doi.org/10.3390/fi12100168, s. 3-8.
[350] D. Pierce, *From Eliza to ChatGPT: why people spent 60 years building chatbots*, TheVerge.com, https://www.theverge.com/24054603/chatbot-chatgpt-eliza-history-ai-assistants-video [dostęp 15.04.2024 r.].
[351] E. Zhu, Y. Ju, Z. Chen, F. Liu, X. Fang, *An Artificial Neural Network phishing detection model based on Decision Tree and Optimal Features*, Applied Soft Computing Journal 95 (2020), s. 5-7.
[352] M. Bega, *The New Arms Race Between China and the US: A Comparative Analysis of Ai-Powered Military and Economic Pursuits*, EUROPOLITY, vol. 17, no. 2, 2023, DOI: 10.25019/europolity.2023.17.2.3, s. 81.

rozpowszechnienia i efektywności[353]. Złośliwe oprogramowanie oparte na AI stanowi potencjalny, ostateczny scenariusz, w którym bardzo prosta AI może być wykorzystana do przeprowadzenia bardzo prostego ataku. W miarę wzrostu złożoności ataku, musi również wzrosnąć złożoność AI stosowanej do obrony. Na szczycie tego hipotetycznego wyścigu zbrojeń jedyną opłacalną metodą dla złośliwego oprogramowania byłaby walka AI kontra AI, gdzie każda 'strona' stara się przechytrzyć przeciwnika. Dodatkowym elementem tego trendu byłoby wykorzystanie AI opartej na uczeniu nadzorowanym, aby zwiększyć szybkość i efektywność cyberbezpieczeństwa. Badania pokazały, że AI już przewyższa ludzi w grach z wykorzystaniem nadzorowanego uczenia się, co niewątpliwie ma miejsce w cyberbezpieczeństwie, traktowanym jako gra w kotka i myszkę o wysokie stawki[354].

Badacze AI przedstawiają nieuchronną przyszłość wzbogaconą o sztuczną inteligencję jako utopię, gdzie ludzie są wyzwoleni od monotonnej pracy, jednak rzadko porusza się temat jej negatywnych aspektów. Pierwsze udane zastosowanie AI miało miejsce w grach, szczególnie w szachach, gdzie algorytm wykorzystywał heurystyki do wybierania najlepszego możliwego ruchu na podstawie potencjalnych przyszłych stanów planszy. Dotychczas AI była stosowana głównie w najprostszych atakach. Przykładem z 2015 roku jest atak „WannaCry[355]". Jego przebieg został przedstawiony na rysunku nr 22.



Rysunek 22 Schemat działania ataku WannaCry

Źródło: WannaCry Ransomware, Europol, https://www.europol.europa.eu/wannacry-ransomware [dostęp 16.04.2024 r.].

[353] N. Kaloudi, J. Li, *The AI-Based Cyber Threat Landscape: A Survey*, https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2642553/%28withoutACM%29AIsurvey+copy.pdf?sequence=1 [dostęp 15.04.2024 r.], s. 1-2.

[354] Ibidem, s. 3-5.

[355] Vide: M. Cunningham-Dickie, *Are we ready for the next WannaCry?*, Computer Fraud & SecurityVol. 2023, No. 9, https://doi.org/10.12968/S1361-3723(23)70041-9.

W kontekście analizy pierwotnego wektora inicjującego infekcję programem WannaCry, identyfikuje się, że oprogramowanie typu ransomware z reguły inicjuje swoje działanie poprzez rozesłanie niezaproszonych komunikatów elektronicznych, które mają na celu manipulację adresata poprzez indukowanie do kliknięcia w załącznik lub wejście na zainfekowaną stronę internetową. Należy podkreślić, że w prezentacji pominięto mechanizm tzw. „kill switch", który służy jako środek bezpieczeństwa.

Po aktywacji, szkodliwe oprogramowanie WannaCry eksploatuje słabość systemu operacyjnego Windows do replikacji własnego kodu i jego dystrybucji w obrębie sieci komputerowej przedsiębiorstwa, prowadząc do zainfekowania kolejnych systemów wrażliwych na określony wektor ataku.

Ransomware inicjuje proces szyfrowania danych zapisanych na zainfekowanym systemie i formułuje żądanie wypłaty okupu, wyrażonego w kryptowalucie Bitcoin, za odblokowanie dostępu do zaszyfrowanych danych[356].

Sztuczna inteligencja nie była przyczyną tego ransomware, lecz była używana do przeszukiwania portfeli bitcoinowych w celu lokalizowania okupów płaconych przez ofiary, co jest zadaniem niezoptymalizowanym dla algorytmu nieopartego na uczeniu się[357]. W miarę jak AI staje się bardziej zaawansowana i rozpowszechniona, tak samo rośnie jej zastosowanie w cyberprzestępczości. Na szczęście AI w kontekście cyberbezpieczeństwa jest jeszcze młodą dziedziną. Rok 2016 oznaczał pierwszą konferencję IEEE (ang. *Institute of Electrical and Electronics Engineers*) na ten temat, a ośrodki badawcze nadal są rzadkością. Może więc minąć jeszcze kilka lat, zanim ataki cybernetyczne oparte na AI zaczną stanowić aktywne zagrożenie[358], jednakże organizacje biznesowe powinny przygotowywać i rozwijać swoje systemy bezpieczeństwa w kontekście ataków z wykorzystaniem złośliwych aplikacji i narzędzi przez cyberprzestępców.

W niniejszym podrozdziale omówiono współczesne wyzwania w zarządzaniu bezpieczeństwem organizacji sektora ICT, wynikające z dynamicznego rozwoju technologicznego. Przedstawiono szczegółowo różnorodne formy ataków cybernetycznych, takich jak phishing, spear phishing, whaling, vishing, a także bardziej zaawansowane techniki, jak spoofing i spyware. Opisano metody działania cyberprzestępców, którzy wykorzystują socjotechnikę oraz złośliwe oprogramowanie do pozyskiwania danych finansowych, poufnych

[356] A. Połowin, *Cyberzagrożenia w internecie –analiza przypadków*, Cybersecurity and Law Issue 2/2024 vol. 12, DOI: https://doi.org/10.35467/cal/188562, s. 124 i 126.
[357] B. Guembe, A. Azeta, S. Misra, V. Chukwudi Osamor, L. Fernandez-Sanz, V. Pospelova, *The Emerging Threat of Ai-driven Cyber Attacks: A Review*, Applied Artificial Intelligence, 36:1 (2022), https://www.tandfonline.com/doi/epdf/10.1080/08839514.2022.2037254?needAccess=true [dostęp 15.04.2024 r.].
[358] Ibidem.

informacji firmowych oraz kompromitujących materiałów. Zwrócono uwagę na rozwój oprogramowania złośliwego, takiego jak ransomware (np. WannaCry) oraz spyware (np. Pegasus i DarkHotel), które infiltrują systemy, powodując znaczące straty. Rozważania te podkreślają potrzebę adaptacji i wdrażania nowych technologii, takich jak sztuczna inteligencja (AI) i uczenie maszynowe, które wspierają zarówno strony atakujące, jak i obronne.

Hipoteza szczegółowa: *szpiegostwo korporacyjne stawia przed zarządzaniem bezpieczeństwem przedsiębiorstwa konieczność przeciwdziałania środkom i metodom dostępu do danych oraz pozyskiwania informacji w celu zdobycia przewagi konkurencyjnej*, znajduje potwierdzenie w kilku aspektach omawianego podrozdziału:

a) środki i metody dostępu do danych – potwierdzono konieczność przeciwdziałania zaawansowanym środkom dostępu do danych, w tym phishingowi, spoofingowi, spyware i ransomware. Organizacje muszą wdrażać strategie ochrony przed różnorodnymi metodami nieautoryzowanego dostępu do informacji, w szczególności poprzez rozwój zabezpieczeń cyfrowych oraz edukację pracowników,
b) pozyskiwanie informacji w celu zdobycia przewagi konkurencyjnej – scharakteryzowano w jaki sposób, działania cyberprzestępcze, zwłaszcza te ukierunkowane na wysoką kadrę zarządzającą, mogą prowadzić do wycieku kluczowych danych, które mogą być wykorzystane do uzyskania przewagi konkurencyjnej. W szczególności spear phishing oraz whaling są przykładami, które pokazują, jak złośliwe oprogramowanie i socjotechnika są stosowane w celu zdobycia strategicznych informacji.

Podsumowując, niniejszy podrozdział częściowo potwierdza hipotezę roboczą wykazując, że przedsiębiorstwa muszą przeciwdziałać złożonym technikom dostępu do danych, które rozwijają się wraz z postępem technologicznym, aby ochronić swoje zasoby informacyjne przed zagrożeniami związanymi ze szpiegostwem korporacyjnym.

Rozdział 4.METODYKA BADAŃ WŁASNYCH

4.1 Zakres przedmiotowy, podmiotowy, przestrzenny i czasowy badań

Przedmiotem badań niniejszej dysertacji jest analiza zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych (ICT), ze szczególnym uwzględnieniem wpływu szpiegostwa korporacyjnego na postrzeganie zagrożeń przez pracowników. Sektor technologii informacyjno-komunikacyjnych (ICT) obejmuje szeroki zakres technologii i usług związanych z gromadzeniem, przetwarzaniem, przechowywaniem oraz przesyłaniem informacji. Do kluczowych obszarów ICT należą między innymi telekomunikacja, infrastruktura chmurowa, technologie mobilne, bezpieczeństwo danych oraz rozwój oprogramowania. Sektor ten dynamicznie się rozwija, odgrywając istotną rolę w cyfrowej transformacji przedsiębiorstw oraz gospodarek na całym świecie, z rosnącym naciskiem na cyfrową transformację sektora publicznego i prywatnego.

Sektor technologii informacyjno-komunikacyjnych (ICT) odgrywa kluczową rolę w kształtowaniu współczesnej gospodarki cyfrowej. ICT obejmuje szeroki zakres działalności związanych z przetwarzaniem, przechowywaniem i transmisją informacji, w tym rozwój oprogramowania, usług internetowych, sprzętu komputerowego oraz telekomunikacji[359]. W dobie globalizacji i postępującej cyfryzacji, znaczenie sektora ICT stale rośnie, wpływając na transformację modeli biznesowych i struktur organizacyjnych przedsiębiorstw.

Sektor ICT zajmuje się tworzeniem i wdrażaniem innowacyjnych rozwiązań technologicznych, które wpływają na efektywność procesów biznesowych, komunikację międzyludzką oraz dostęp do informacji. Kluczowe obszary działalności obejmują rozwój oprogramowania, usługi chmurowe, technologie mobilne, analizę big data oraz sztuczną inteligencję. Organizacje z tego sektora dostarczają narzędzia umożliwiające automatyzację procesów, integrację systemów oraz optymalizację zarządzania informacją[360].

Wśród głównych szans dla sektora ICT należy wymienić rosnące zapotrzebowanie na cyfryzację w różnych sektorach gospodarki. Pandemia COVID-19 przyspieszyła procesy digitalizacji, zwiększając popyt na rozwiązania zdalnej pracy, e-commerce oraz telemedycynę. Rozwój Internetu Rzeczy (IoT) otwiera nowe możliwości integracji urządzeń i systemów,

[359] A. Brzozowska, D. Bubel, L. Nekrasenko, *Organisation Management in the Digital Economy: Globalization Challenges*, CRC Press, Boca Raton 2022, s. 3-4.
[360] T. Lis, A. Ptak, *ICT a Efektywność Zarządzania Informacją w Przedsiębiorstwie*, W: *Technologie informacyjno-komunikacyjne w zarządzaniu, logistyce i turystyce. Wybrane zagadnienia* (red.) L. Kiełtyka, K. Smoląg, Wydawnictwo TNOiK "Dom Organizatora" w Toruniu, Toruń 2022, s. 82-83.

umożliwiając tworzenie inteligentnych miast i infrastruktury. Ponadto, wzrost zainteresowania technologiami blockchain i kryptowalutami stwarza nowe obszary inwestycji i innowacji.

Mimo licznych szans, sektor ICT stoi przed wieloma wyzwaniami. Jednym z nich jest szybkie tempo zmian technologicznych, które wymaga ciągłego inwestowania w badania i rozwój oraz podnoszenia kwalifikacji pracowników. Deficyt wykwalifikowanej kadry w sektorze ICT staje się coraz bardziej odczuwalny. Ponadto, kwestia bezpieczeństwa cybernetycznego nabiera na znaczeniu ze względu na rosnącą liczbę cyberataków i zagrożeń związanych z prywatnością danych. Regulacje prawne i etyczne dotyczące sztucznej inteligencji i przetwarzania danych osobowych stanowią istotne wyzwanie dla firm działających w tym sektorze.

Główne kierunki rozwoju sektora ICT obejmują dalszą integrację sztucznej inteligencji w procesach biznesowych, rozwój technologii 5G[361] i przygotowanie do wdrożenia sieci 6G, a także intensyfikację wykorzystania technologii chmurowych[362] i edge computing. Wzrasta również znaczenie technologii kwantowych, które mogą zrewolucjonizować przetwarzanie danych i bezpieczeństwo informacji. Ponadto, rośnie nacisk na zrównoważony rozwój i ekologiczne rozwiązania w ICT, co wpływa na strategie firm w zakresie efektywności energetycznej i redukcji śladu węglowego.

Dla nauk o zarządzaniu i jakości, sektor ICT stanowi istotny obszar badań ze względu na wpływ technologii na struktury organizacyjne, modele biznesowe i procesy decyzyjne. Implementacja nowych technologii wymaga adaptacji strategii zarządzania oraz uwzględnienia aspektów jakościowych w dostarczaniu usług i produktów ICT. Organizacje muszą integrować nowe technologie z istniejącymi procesami, dbając o ciągłe doskonalenie i innowacyjność.

Sektor ICT jest kluczowym elementem współczesnej gospodarki, oferującym liczne innowacje i rozwiązania zwiększające efektywność różnych sektorów[363]. W obliczu dynamicznych zmian technologicznych, sektor ten musi sprostać wyzwaniom związanym z bezpieczeństwem, regulacjami i szybkością adaptacji do nowych technologii[364]. Dla zarządzania i jakości istotne jest zrozumienie wpływu ICT na organizacje oraz wykorzystanie tych technologii do osiągania przewagi konkurencyjnej[365].

---

[361] S. Ghaemi, *Powering the Distant Future: 5G and Machine Learning at the Edge*, Unite.ai, https://www.unite.ai/powering-the-distant-future-5g-and-machine-learning-at-the-edge/ [dostęp 13.11.2024 r.].
[362] A. Bitkowska, M. Szymborski, *Cyfryzacja przedsiębiorstw z perspektywy procesowo-projektowej*, W: *Wykorzystanie technik informacyjnych w zarządzaniu* (red.) Leszek Kiełtyka, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2023, s. 198.
[363] OECD, *Embracing the Technology Frontier*, OECD Digital Economy Outlook 2024 (Volume 1), DOI: https://doi.org/10.1787/a1689dc5-en, s. 11.
[364] J. Tomczyk, Technologiczni giganci inwestują w Edge Computing, MITSloan, https://mitsmr.pl/b/technologiczni-giganci-inwestuja-w-edge-computing/PelOIcy3P [dostęp 13.11.2024 r.].
[365] S. Zuboff, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, Public Affairs, Nowy Jork 2019, s. 242.

Celem nadrzędnym jest weryfikacja hipotezy głównej, zgodnie z którą skuteczne zarządzanie bezpieczeństwem powinno uwzględniać różnice w percepcji zagrożeń związanych ze szpiegostwem korporacyjnym wśród pracowników. Badania odnoszą się do głównych obszarów związanych z zarządzaniem bezpieczeństwem, takich jak: wdrażanie procesów decyzyjnych, stosowanie norm bezpieczeństwa informacji oraz strategie ochrony przed metodami dostępu i pozyskiwania danych stosowanymi przez konkurencję.

Podmiotem badań były przedsiębiorstwa z sektora technologii informacyjno-komunikacyjnych, spełniające określone kryteria kwalifikacyjne. Do badania wybrano sześć dużych przedsiębiorstw działających na terytorium Polski, posiadających co najmniej 5-letni staż na rynku oraz specjalizujących się w innowacyjnych rozwiązaniach w zakresie ICT. Wybór ten był podyktowany potrzebą uzyskania reprezentatywnych wyników dotyczących dużych przedsiębiorstw, które prowadzą działalność w sektorze narażonym na ryzyko szpiegostwa korporacyjnego. Próba badawcza obejmowała zarówno osoby odpowiedzialne za zarządzanie bezpieczeństwem, jak i pracowników na różnych szczeblach organizacji, co pozwoliło uzyskać wszechstronny obraz postrzegania zagrożeń oraz stosowanych praktyk zarządzania bezpieczeństwem.

Zakres przestrzenny badań obejmował Rzeczpospolitą Polską, przy czym analizowano przedsiębiorstwa operujące w polskim sektorze ICT. Uwzględnienie polskich przedsiębiorstw umożliwiło skoncentrowanie się na lokalnym kontekście regulacyjnym i specyfice rynku ICT, z uwzględnieniem regulacji i wymogów związanych z ochroną danych, takich jak GDPR, oraz innych przepisów obowiązujących w Polsce.

Badania zostały przeprowadzone w okresie od czerwca 2022 roku do listopada 2024 roku i obejmowały pięć głównych etapów:

- **Etap I (czerwiec 2022 r. – wrzesień 2023 r.)** – przegląd i analiza dostępnej literatury poświęconej poruszanemu zagadnieniu. Biorąc pod uwagę fakt, iż temat podjęty w dysertacji stanowi pewne *novum* i nie był szerzej podejmowany przez badaczy naukowych, należy zaznaczyć, iż dostępna literatura na ten temat jest ograniczona. Napotkane trudności badawcze, takie jak brak ustalonych punktów odniesienia dla analizy, ograniczenia w dostępie do literatury oraz luka badawcza dotyczącą szpiegostwa korporacyjnego, skłoniły do przeprowadzenia badań empirycznych. Badania te, stanowiące kolejne etapy metodycznej procedury, mają na celu wypełnienie luki w dostępnych danych i umożliwienie dalszej analizy,
- **Etap II (wrzesień 2022 r. – marzec 2023 r.)** – polegał na przeprowadzeniu wywiadów eksperckich z osobami odpowiedzialnymi za bezpieczeństwo w sześciu przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych, wybranych na

podstawie precyzyjnie określonych kryteriów. Przeprowadzone wywiady miały na celu głębokie zrozumienie i weryfikację postawionych hipotez badawczych, a także ocenę, jak teoria przekłada się na praktyczne dylematy w kontekście bezpieczeństwa przedsiębiorstwa. Wywiad ekspercki został zrealizowany z udziałem dwunastu specjalistów ds. bezpieczeństwa przedsiębiorstw, wybranych z grona pracowników zatrudnionych bezpośrednio przez wyselekcjonowane przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych. Takie podejście umożliwiło uzyskanie bezpośrednich i szczegółowych informacji (nieobjętych tajemnicą przedsiębiorstwa) na temat aktualnych wyzwań i praktyk w zakresie zabezpieczeń w sektorze technologii informacyjno-komunikacyjnych,

- **Etap III (listopad 2023 r. – marzec 2024 r.)** – wykorzystano kwestionariusz ankiety, który stanowi załącznik nr 2 do niniejszej dysertacji. Ankieta, zatytułowana „*Problematyka Szpiegostwa Korporacyjnego w Przedsiębiorstwie Sektora Technologii Informacyjno-Komunikacyjnych*", była adresowana do personelu na różnych poziomach hierarchicznych, od kierownictwa do pracowników biurowych i dotyczyła takich aspektów jak rozumienie szpiegostwa korporacyjnego, procedury reagowania na incydenty, szkolenia oraz zaangażowanie instytucji państwowych w tę kwestie. Struktura ankiety, składająca się z 18 pytań zamkniętych według skali Likerta, zapewniała spójność i możliwość porównania odpowiedzi respondentów,
- **Etap IV (wrzesień – październik 2024)** – przeprowadzono własne badanie empiryczne przy wykorzystaniu metod statystycznych, których finalnym efektem było przygotowanie modelu zarządzania bezpieczeństwem przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych. Model uwzględniał kluczowe obszary wskazane przez ekspertów oraz obszary wskazane przez pracowników wyselekcjonowanych przedsiębiorstw sektora ICT,
- **Etap V (październik – listopad 2024**) – kontynuowanie własnego badania empirycznego przy wykorzystaniu metody symulacji komputerowej, której efekt finalny stanowi przygotowanie 9 wariantów wdrożenia uprzednio przygotowanego modelu zarządzania bezpieczeństwem wraz z proponowanymi rozwiązaniami w zakresie monitorowania i ewaluacji skuteczności wdrożenia oraz optymalizacji modelu w oparciu o wyniki wdrożenia.

Badania podjęte w ramach niniejszej dysertacji dostarczają nowej, interdyscyplinarnej wiedzy na temat zarządzania bezpieczeństwem w sektorze technologii informacyjno-komunikacyjnych (ICT), ukazując zarówno teoretyczne podstawy, jak i praktyczne implikacje związane z identyfikacją, oceną oraz przeciwdziałaniem zagrożeniom wynikającym ze

szpiegostwa korporacyjnego. Szczególny nacisk położono na analizę specyfiki tych zagrożeń w dynamicznie zmieniającym się środowisku technologicznym oraz na wykorzystanie nowoczesnych strategii zarządzania bezpieczeństwem.

4.2 Założenia badawcze i uwagi metodyczne

Chcąc zweryfikować postawione hipotezy badawcze (zarówno hipotezę główną jak i hipotezy szczegółowe) oraz zrealizować główny cel rozprawy doktorskiej, przeprowadzono ściśle określoną procedurę empiryczną w pełni zgodną z założeniami metodologicznymi z zakresu prowadzenia badań naukowych.

W dysertacji sformułowano następujący główny problem badawczy: jakie wyzwania dla zarządzania bezpieczeństwem informacji w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych wynikają ze zróżnicowanego postrzegania przez pracowników zagrożeń ze strony szpiegostwa korporacyjnego?

Wśród szczegółowych problemów badawczych należy wymienić kilka zagadnień sformułowanych w formie pytań:

P1: Jaką rolę i znaczenie odgrywa bezpieczeństwo w zarządzaniu przedsiębiorstwem sektora technologii informacyjno-komunikacyjnych?

P2: Jakie przesłanki i wyzwania wpływają na implementację zarządzania bezpieczeństwem informacyjnym w organizacji?

P3: W jaki sposób zagrożenia wynikające ze szpiegostwa korporacyjnego wpływają na zarządzanie bezpieczeństwem przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych?

P4: W jaki sposób można ocenić poziom świadomości pracowników na temat zagrożeń wynikających ze szpiegostwa korporacyjnego oraz skuteczność zarządzania bezpieczeństwem?

P5: Jaka jest zależność pomiędzy poziomem świadomości pracowników a skutecznością zarządzania bezpieczeństwem w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych?

P5.1: Czy postrzeganie problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych zależy od miejsca zatrudnienia?

P5.2: Czy postrzeganie problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych zależy od wieku badanych osób?

P5.3: Czy postrzeganie problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych zależy od stażu pracy?

P5.4: Czy postrzeganie problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych zależy od wykształcenia badanych osób?

P5.5: Czy postrzeganie problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych zależy od zajmowanego stanowiska służbowego?

P5.6: W jaki sposób postrzegane przez pracowników skuteczność procedur ochrony, edukacja w zakresie zagrożeń oraz środki prawne wpływają na ich ocenę ryzyka szpiegostwa korporacyjnego w organizacji?

P5.7: Czy szkolenia i świadomość pracowników są mediatorem wpływu skuteczności zabezpieczeń organizacyjnych na postrzegane ryzyko szpiegowskie?

P5.8: Czy szkolenia i świadomość, i regulacje prawne wpływają na postrzeganie zagrożenia szpiegostwem?

Głównym celem niniejszej pracy jest opracowanie modelu zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych, który uwzględnia zróżnicowane postrzeganie zagrożeń wynikających ze szpiegostwa korporacyjnego przez pracowników, w celu zwiększenia ochrony danych i tajemnicy przedsiębiorstwa. Osiągnięcie założonego celu, wymusiło określenie następujących celów szczegółowych:

C1: Identyfikacja roli i znaczenia bezpieczeństwa w zarządzaniu przedsiębiorstwem,

C2: Zidentyfikowanie przesłanek oraz wyzwań związanych z wdrażaniem zarządzania bezpieczeństwem informacji w organizacji,

C3: Ustalenie, jakie wyzwania dla zarządzania bezpieczeństwem przedsiębiorstw sektora technologii informacyjno-komunikacyjnych stwarza szpiegostwo korporacyjne,

C4: Diagnoza zależności między poziomem świadomości pracowników a skutecznością zarządzania bezpieczeństwem w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych.

Uprzednio zdefiniowany problem badawczy wymagał sformułowania hipotezy głównej, zgodnie z którą zarządzanie bezpieczeństwem informacji przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych powinno uwzględniać różnice w postrzeganiu przez pracowników zagrożeń wynikających ze szpiegostwa korporacyjnego.

Odpowiednio do szczegółowych problemów badawczych, sformułowano następujące hipotezy szczegółowe:

H1: Racjonalne zarządzanie bezpieczeństwem, w tym wdrażanie odpowiednich procesów decyzyjnych oraz strategii identyfikacji i minimalizacji ryzyka, warunkuje ciągłość działania organizacji oraz zabezpieczenie jej kluczowych zasobów.

H2: Stosowanie odpowiednich standardów i norm w zarządzaniu bezpieczeństwem informacji, pozwala na skuteczne rozpoznawanie zagrożeń, kształtując poziom ochrony danych oraz tajemnicy przedsiębiorstwa.

H3: Szpiegostwo korporacyjne stawia przed zarządzaniem bezpieczeństwem przedsiębiorstwa konieczność przeciwdziałania środkom i metodom dostępu do danych oraz pozyskiwania informacji w celu zdobycia przewagi konkurencyjnej.

H4: Skuteczne zarządzanie bezpieczeństwem przedsiębiorstw sektora technologii informacyjno-komunikacyjnych wymaga uwzględnienia sposobu, w jaki pracownicy postrzegają szpiegostwo korporacyjne:

H4.1: Postrzeganie problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych zależy od miejsca zatrudnienia.

H4.2: Postrzeganie problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych zależy od wieku badanych osób.

H4.3: Postrzeganie problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych zależy od stażu pracy.

H4.4: Postrzeganie problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych zależy od wykształcenia badanych osób.

H4.5: Postrzeganie problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych zależy od zajmowanego stanowiska służbowego.

H4.6: Postrzegane przez pracowników skuteczność procedur ochrony, edukacja w zakresie zagrożeń oraz środki prawne wpływają na ich ocenę ryzyka szpiegostwa korporacyjnego w organizacji.

H4.7: Szkolenia i świadomość pracowników są mediatorem wpływu skuteczności zabezpieczeń organizacyjnych na postrzegane ryzyko szpiegowskie.

H4.8: Szkolenia, świadomość zagrożeń i regulacje prawne wpływają na postrzeganie zagrożenia szpiegostwem.

Procedurę badawczą rozpoczęto od zrealizowania pierwszego etapu, w ramach którego dokonano szczegółowego przeglądu, a następnie analizy literatury poświęconej poruszanej tematyce. Na jej podstawie opracowano trzynaście pytania w ramach wywiadu eksperckiego, które posłużyły do przeprowadzenia rozmów z 12 specjalistami z zakresu bezpieczeństwa

zatrudnionymi w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych. Wyniki uzyskane na podstawie przeprowadzonego wywiadu pozwoliły na przygotowanie kwestionariusza ankiety, składającego się z 18 pytań z odpowiedziami przygotowanymi według skali Likerta, dotyczących aktualnego stanu wiedzy badanych na temat bezpieczeństwa przedsiębiorstwa, w którym są zatrudnieni.

Wyniki uzyskane w ramach przeprowadzonego badania kwestionariuszowego zostały poddane weryfikacji, przy wykorzystaniu metody statystycznej. Przeprowadzone badania, pozwoliły na przygotowanie modelu zarządzania bezpieczeństwem przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych.

Ostatnim etapem badań, było przeprowadzenie symulacji komputerowej, która miała na celu wskazanie optymalnego wariantu wdrożenia modelu zarządzania bezpieczeństwem w oparciu o kluczowe wskaźniki, które uzyskano podczas badań.

4.3 Kryteria i dobór obiektów badawczych

Realizacja II i III etapu prowadzonych badań, poprzedzona została wytypowaniem określonej próby badawczej, którą stanowili pracownicy wyselekcjonowanych przedsiębiorstw, na podstawie ściśle określonych kryteriów. Wskazane kryteria przedstawiają się w sposób następujący:

a) profil przedsiębiorstwa – sektor technologii informacyjno-komunikacyjnych,
b) zasięg prowadzonej działalności – Rzeczypospolita Polska,
c) status przedsiębiorstwa – przedsiębiorstwo duże,
d) okres funkcjonowania na rynku – co najmniej 5 lat,
e) charakter prowadzonej działalności – usługi informacyjno-komunikacyjne oraz innowacyjne rozwiązania w tym zakresie.

Na podstawie wskazanych powyżej kryteriów, do badania wytypowano następujące przedsiębiorstwa, które na dzień 31.12.2023 r. zatrudniały następującą liczbę pracowników, przedstawioną w tabeli nr 16.

Tabela 16 Liczba pracowników zatrudniana przez wybrane przedsiębiorstwa sektora ICT

Przedsiębiorstwo sektora ICT	Ilość pracowników
Orange Polska S. A.	9500
T-Mobile Polska S. A.	3700
P4 Sp. z o. o. (Play)	4000
Polkomtel Sp. z o. o. (Plus)	3000

Przedsiębiorstwo sektora ICT	Ilość pracowników
Netia S. A.	2000
Vectra S. A.	1260
Suma	23460

Źródło: opracowanie własne.

W ramach przeprowadzonego badania jakościowego dotyczącego bezpieczeństwa przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych w kontekście szpiegostwa korporacyjnego, od czerwca 2022 r. do listopada 2023 r., przeprowadzono wywiady eksperckie z 12 specjalistami w tej dziedzinie zatrudnionymi w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych prowadzących swoją działalność na terytorium RP. Celem tych wywiadów było zgromadzenie głębokiej wiedzy i praktycznych spostrzeżeń na temat aktualnych wyzwań, najlepszych praktyk oraz przyszłych trendów w zakresie zapewnienia ochrony przed zagrożeniami związanymi ze szpiegostwem korporacyjnym (załącznik nr 1).

Eksperci, z którymi przeprowadzono wywiadu, reprezentują szerokie spektrum doświadczeń i perspektyw, obejmujące różnorodne aspekty bezpieczeństwa, takie jak cyberbezpieczeństwo, zarządzanie ryzykiem, ochrona fizyczna, a także polityki i procedury związane z bezpieczeństwem. Ich doświadczenie zawodowe oraz kompleksową znajomość tematu pozwoliły na uzyskanie cennych i różnorodnych opinii, które stanowią fundament wniosków zrealizowanego procesu badawczego.

Następnie, od listopada 2023 r. do marca 2024 r. przeprowadzono badanie ankietowe, wykorzystując kwestionariusz ankiety pt. „Problematyka Szpiegostwa Korporacyjnego w Przedsiębiorstwie Sektora Technologii Informacyjno-Komunikacyjnych" (załącznik nr 2). Badanie to miało miejsce w sześciu celowo wybranych przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych, zgodnie z kryteriami wskazanymi w poniższej treści.

Biorąc pod uwagę liczbę pracowników zatrudnianych przez poszczególne podmioty, wykorzystano następujący wzór, celem oszacowania liczby osób zatrudnionych w centrali każdego przedsiębiorstwa.

$$N = \frac{T \cdot (Pc + P\omega)}{Ec \cdot F}$$

Opis:

N – szacowana liczba osób zatrudnionych w centrali przedsiębiorstwa,

T – całkowita liczba pracowników w przedsiębiorstwie,

$\mathbf{P_c}$ – procentowy udział funkcji centralnych w strukturze zatrudnienia,

$\mathbf{P_w}$ – procentowy udział wsparcia operacyjnego, realizowanego w centrali,

$\mathbf{E_c}$ – efektywność struktury centrali, wyrażona jako stosunek liczby zadań przypadających na jednego pracownika centrali (współczynnik efektywności),

F – współczynnik fluktuacji, uwzględniający tymczasowe wakaty oraz dynamikę zatrudnienia.

Całkowita liczba pracowników jest to podstawowa wartość, która określa pełne zatrudnienie w organizacji (centrala + oddziały regionalne + zewnętrzne podmioty). Procentowy udział funkcji centralnych zależny jest od specyfiki działalności przedsiębiorstwa, natomiast typowe wartości to 5–15% w przedsiębiorstwach produkcyjnych oraz 20–30% w sektorze usług. Procentowy udział wsparcia operacyjnego uwzględnia jednostki wspierające operacje (IT, HR, marketing), które mogą być centralizowane, natomiast typowe wartości to 10–20%. Efektywność struktury centrali wskazuje na produktywność pracowników centrali, natomiast typowe wartości to 0.8–1.2. Współczynnik fluktuacji uwzględnia rotację pracowników oraz ewentualne wakaty, a typowe wartości wynoszą 1.0–1.1.

Zatem na podstawie powyższego wzoru, dokonano oszacowania liczby pracowników centrali dla poszczególnych przedsiębiorstw. Wskazane wyliczenia kształtują się w sposób następujący: Orange – 2262, T-Mobile – 881, Play – 952, Plus – 714, Netia – 476, Vectra – 300. Sumarycznie, liczba pracowników zatrudnionych w centrali wszystkich przedsiębiorstw wynosi 5585.

Wielkość próby została ustalona na podstawie poniższych założeń:

a) wielkość badanej populacji stanowiło 5 tys. osób;
b) poziom ufności założono na poziomie 95%;
c) wielkość frakcji wyniosła 0,5;
d) błąd maksymalny wynosi 5%.

Wobec powyższego, podjęto dalsze czynności do obliczenia reprezentatywnej próby badawczej. W tym celu uwzględniono niżej wymienione parametry:

a) wielkość populacji (**N**) – liczba osób w całej populacji, spośród których wybierana jest próba,
b) poziom ufności (**z**) – określa, jak pewni chcemy być wyniku (95% ≈ 1,96),
c) maksymalny błąd szacunku (**E**) – dopuszczalna różnica między wynikiem próby, a rzeczywistością w populacji (5% = 0,05),
d) proporcja sukcesu (**p**) – zakładany odsetek osób w populacji, które mają daną cechę (jeśli brak danych, przyjmuje się 50%, czyli p=0,5).

Celem wyznaczenia reprezentatywnej wielkości próby badawczej zastosowano następujący ciąg logiczny wyznaczania właściwej formuły matematycznej. Rozpoczęto od wyznaczenia wzoru oraz wyliczenia próby dla dużej populacji, gdzie N>10,000.

$$N = \frac{z^2 \cdot p \cdot (1-p)}{E^2}$$

$$n_0 = \frac{1{,}96^2 \cdot 0{,}5 \cdot (1-0{,}5)}{0{,}5^2} = \frac{3{,}8416 \cdot 0{,}25}{0{,}0025} = 384{,}16$$

Następnie, uwzględniając, iż uzyskana we wstępnym szacowaniu populacja wyniosła 5 tys. (N≤10,000), zastosowano korektę.

$$N = \frac{N \cdot z^2 \cdot p \cdot (1-p)}{E^2 \cdot (N-1) + z^2 \cdot p \cdot (1-p)}$$

$$N = \frac{10000 \cdot 384{,}16}{0{,}0025 \cdot 9{,}999 + 384{,}16} = \frac{3{,}841{,}600}{25 + 384{,}16} \approx 370$$

Na podstawie przedstawionej formuły matematycznej, reprezentatywna wielkość próby została wyliczona na 370 osób.

Kwestionariusz ankiety w formie interaktywnego formularza udostępniono 600 osobom, natomiast odpowiedzi udzieliło 466 osób. Kwestionariusz wypełniło ponad 78% respondentów. Główny wpływ na powyższy wynik miały takie czynniki jak m. in. brak czasu spowodowany ilością obowiązków służbowych, brak zainteresowania ze strony respondentów oraz brak bezpośredniej gratyfikacji za udzielenie odpowiedzi.

Następnie, od września do października 2024 r. przeprowadzono własne badanie empiryczne przy wykorzystaniu metod statystycznych, których finalnym efektem było przygotowanie modelu zarządzania bezpieczeństwem przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych. Model uwzględniał kluczowe obszary wskazane przez ekspertów oraz obszary wskazane przez pracowników wyselekcjonowanych przedsiębiorstw sektora ICT.

Ostatnim elementem, realizowanym od października do listopada 2024 r. było kontynuowanie własnego badania empirycznego przy wykorzystaniu metody symulacji komputerowej, której efekt finalny stanowi przygotowanie 9 wariantów wdrożenia uprzednio przygotowanego modelu zarządzania bezpieczeństwem wraz z proponowanymi rozwiązaniami w zakresie monitorowania i ewaluacji skuteczności wdrożenia oraz optymalizacji modelu w oparciu o wyniki wdrożenia.

4.4 Metody, techniki i narzędzia badawcze

Pierwszą zastosowaną metodą badawczą była metoda przeglądu literatury przedmiotu. Głównym celem tej metody w przypadku poniższej dysertacji było zidentyfikowanie głównych pojęć oraz źródeł i rodzajów dostępnych dowodów w danym obszarze badawczym (zmapowanie literatury), identyfikacja luk w istniejącej literaturze, co może prowadzić do sformułowania tematów przyszłych badań oraz wskazania obszarów wymagających dalszej eksploracji oraz zrozumienie natury i rozmiaru dowodów badawczych, co pozwala na lepsze kształtowanie polityki i praktyki w danym obszarze[366].

Badania własne rozpoczęto od przeglądu literatury przedmiotu w trzech głównych obszarach tematycznych: zarządzania bezpieczeństwem, zarządzania bezpieczeństwem informacji oraz szpiegostwa korporacyjnego. Powyższe spowodowane było zidentyfikowaniem luki badawczej, dotyczącej relacji i powiązań zachodzących pomiędzy dwoma pierwszymi obszarami tematycznymi, a szpiegostwem korporacyjnym.

Na podstawie dokonanego przeglądu dostępnej literatury w poszczególnych wskazanych obszarach, przygotowano 13 pytań dotyczących istotnych obszarów działalności przedsiębiorstwa w zakresie bezpieczeństwa. Wskazane pytania zostały opracowane na potrzeby przeprowadzenia wywiadów eksperckich, które stanowiły kolejny etap własnych badań empirycznych. Wywiad ekspercki jest jedną z kluczowych metod badawczych w naukach o zarządzaniu i jakości, umożliwiającą uzyskanie kompleksowych informacji od specjalistów w danej dziedzinie[367]. Ta metoda badawcza opiera się na specyficznej formie dialogu, w którym kluczową rolę odgrywa interakcja między badaczem a respondentem, co pozwala na wspólne tworzenie wiedzy. Wywiad nie jest jedynie prostą wymianą zdań, lecz precyzyjnie zaplanowanym procesem, w którym badacz jako ekspert merytoryczny, koncentruje się na eksploracji opinii, przekonań i doświadczeń respondentów w kontekście założonych celów badawczych. Charakter pytań w wywiadzie może być ustrukturalizowany, półustrukturalizowany lub swobodny, w zależności od przyjętego podejścia, co wpływa na sposób gromadzenia danych i głębokość uzyskiwanych odpowiedzi. Szczególną cechą wywiadu eksperckiego jest możliwość zgłębiania kluczowych aspektów tematu oraz uwzględnienie zarówno poziomu faktograficznego, jak i subiektywnego znaczenia wypowiedzi. Metoda ta, stanowiąca często uzupełnienie innych technik badawczych, pozwala na uchwycenie perspektywy eksperta, a tym samym dostarczenie cennych danych do analizy

[366] M. Ćwiklicki, *Metodyka przeglądu zakresu literatury*, W: *Współczesne zarządzanie – koncepcje i wyzwania* (red.) A. Sopińska, A. Modliński, Wydawnictwo SGH, Warszawa 2020, s. 6 i 12.
[367] Ł. Sułkowski, R. Lenart-Gasiniec, *Epistemologia, metodologia i metody badań w naukach o zarządzaniu i jakości,* Społeczna Akademia Nauk, Łódź 2021, s. 367.

i interpretacji zjawisk badanych w kontekście naukowym. W tym przypadku, wyniki uzyskane na podstawie rozmów przeprowadzonych ze specjalistami zatrudnionymi w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych, pozwoliły na przygotowanie kwestionariusza ankiety, dotyczącego kluczowych obszarów zarządzania bezpieczeństwem w przedsiębiorstwie – szkolenia, postrzegania zagrożeń oraz regulacji prawnych.

Wybór metody wywiadu eksperckiego w zrealizowanym badaniu nie był przypadkowy i został dokonany z kilku istotnych powodów, które mają szczególne znaczenie w kontekście nauk o zarządzaniu i jakości:

a) kompleksowa analiza i nadanie kontekstu: wywiad ekspercki pozwala na uzyskanie szczegółowych informacji oraz zrozumienie kontekstu, w jakim funkcjonują przedsiębiorstwa. Eksperci mogą dostarczyć nie tylko faktów, ale również wniosków wynikających z ich bogatego doświadczenia i wiedzy praktycznej,
b) identyfikacja najlepszych praktyk: w dziedzinie zarządzania i jakości, szczególnie ważne jest poznanie sprawdzonych metod i strategii, które przyniosły sukces w praktyce. Eksperci mogą wskazać konkretne rozwiązania, które z powodzeniem zastosowano w różnych firmach i sektorach,
c) adaptacja do dynamicznych zmian: szybko zmieniające się środowisko biznesowe i technologiczne wymaga ciągłej adaptacji strategii zarządzania i bezpieczeństwa. Eksperci są na bieżąco z najnowszymi trendami i innowacjami, co pozwala na bardziej aktualne i precyzyjne wnioski,
d) różnorodność perspektyw: rozmowy z ekspertami z różnych branż i dziedzin pozwalają na zebranie szerokiego spektrum opinii i doświadczeń. Dzięki temu nasze badanie uwzględnia różnorodne aspekty bezpieczeństwa przedsiębiorstw, co przekłada się na bardziej kompleksowe i wszechstronne wnioski,
e) walidacja teoretycznych modeli: wywiady z ekspertami umożliwiają skonfrontowanie teoretycznych modeli zarządzania i jakości z rzeczywistością biznesową, co pozwala na weryfikację i udoskonalenie istniejących teorii oraz praktyk zarządzania.

Badanie ankietowe oparte na skali Likerta stanowi jedną z kluczowych metod badawczych w podejściu nomotetycznym, które koncentruje się na identyfikacji ogólnych prawidłowości i weryfikacji hipotez[368]. Skala Likerta, będąca popularnym narzędziem w badaniach ilościowych, umożliwia pomiar opinii, postaw oraz percepcji respondentów poprzez zastosowanie stopniowanych odpowiedzi odzwierciedlających poziom zgody lub

[368] J. Apanowicz, *Metodologia nauk*, Wydawnictwo TNOiK „Dom Organizatora", Toruń 2003, s. 86.

sprzeciwu wobec danego twierdzenia[369]. Tego typu badania, charakteryzujące się ustrukturalizowaną formą i powtarzalnym układem pytań, pozwalają na zebranie danych ilościowych, które następnie mogą być poddane statystycznej analizie. W kontekście braku aktywnej interakcji między badaczem a respondentem, metoda ta zapewnia standaryzację i obiektywizm, umożliwiając badaczowi uzyskanie miarodajnych informacji na temat szerokiej próby badanych. Dzięki temu ankiety oparte na skali Likerta są szczególnie użyteczne w badaniach społecznych i psychologicznych, gdzie analiza ludzkich postaw i zachowań wymaga ujęcia ilościowego z wykorzystaniem rzetelnych narzędzi pomiarowych.

Następnie, celem weryfikacji postawionych hipotez badawczych została zastosowana metoda statystyczna, w postaci testu chi-kwadrat[370]. Wskazana metoda odnosi się do techniki analizy danych używanej do weryfikacji hipotez badawczych. W szczególności test chi-kwadrat służy do badania zależności między zmiennymi nominalnymi lub porządkowymi (np. w tabelach kontyngencji) oraz do sprawdzania zgodności rozkładu empirycznego z teoretycznym (test zgodności). W badaniach społecznych jest szeroko stosowany do analizy relacji między cechami jakościowymi, co pozwala na wnioskowanie o ich statystycznej istotności.

Kolejnym etapem procedury badawczej było zastosowanie metod analizy mediacji, regresji i ścieżkowej, które zostały opracowane w pakiecie SPSS AMOS[371]. Pakiet AMOS (Analysis of Moment Structures) w programie SPSS to narzędzie do przeprowadzania analizy ścieżkowej oraz modelowania równań strukturalnych (SEM)[372]. Jest używany głównie w analizach statystycznych i badaniach naukowych, gdzie istotne jest modelowanie skomplikowanych zależności między zmiennymi. SEM umożliwia jednoczesne analizowanie wielu zależności między zmiennymi obserwowalnymi i ukrytymi (latentnymi), co jest przydatne w badaniach społecznych, psychologii, zarządzaniu, ekonomii oraz wielu innych. Przed opracowaniem modelu SEM wykonano analizę struktury czynnikowej (konfirmacyjną CFI)[373], co pomaga sprawdzić, czy dane empiryczne są zgodne z założonym modelem teoretycznym. Umożliwiło to weryfikację czy zestaw zmiennych mierzy określony konstrukt zgodnie z przyjętym modelem. Efektem finalnym tego etapu było stworzenie proponowanego

[369] P. Tarka, *Własności 5- i 7-stopniowej skali Likerta w kontekście normalizacji zmiennych metodą Kaufmana i Rousseeuwa*, W: *Taksonomia 25 Klasyfikacja i analiza danych –teoria i zastosowania* (red.) K. Jajuga, M. Walesiak, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu nr 385 (2015), s. 287-288.
[370] A. Agresti, *Statistical Methods for the Social Sciences* (5th ed.). Pearson, Boston 2018, s. 230.
[371] B. M. Byrne, *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming* (3rd ed.), Routledge, New York 2016, s. 16.
[372] R. B. Kline, *Principles and Practice of Structural Equation Modeling* (4th ed.), Guilford Press, New York 2015, s. 7-16.
[373] T. A. Brown, *Confirmatory Factor Analysis for Applied Research* (2nd ed.), Guilford Press, New York 2015, s. 1-3.

modelu zarządzania bezpieczeństwem przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych.

Ostatnim etapem procedury badawczej było wykorzystanie metody symulacji komputerowej, która miała na celu sprawdzenie działania proponowanego modelu zarządzania bezpieczeństwem. Symulacja komputerowa, będąca specyficzną metodą badawczą, łączy elementy obserwacji i eksperymentu, co pozwala na precyzyjne modelowanie zjawisk i procesów. Jej istota polega na tworzeniu modeli odzwierciedlających rzeczywistość oraz przeprowadzaniu eksperymentów poprzez manipulację zmiennymi niezależnymi, aby zbadać reakcje zmiennych zależnych. W porównaniu z klasycznymi metodami, symulacja znajduje się na styku badań analitycznych, polegających na budowaniu formalnych modeli matematycznych oraz eksperymentów z systemami rzeczywistymi, co czyni ją elastycznym narzędziem do analizy złożonych systemów. W kontekście modeli społeczno-gospodarczych szczególnie widoczna jest jej różnorodność technik i podejść, co umożliwia adaptację metody do zróżnicowanych celów badawczych. Dzięki tej wszechstronności symulacja jest wykorzystywana zarówno do testowania hipotez, jak i prognozowania oraz wspierania procesów decyzyjnych, co podkreśla jej interdyscyplinarny charakter[374]. Ponadto, wykorzystano następujące narzędzia: drzewa decyzyjne (decision trees) wspomagające identyfikację kluczowych czynników determinujących skuteczność wdrożenia[375], las losowy (random forest) w celu analizy trendów oraz hierarchizacji zmiennych wpływających na efektywność w różnych scenariuszach[376], oraz regresję logistyczną (logistic regression) – służąca prognozowaniu prawdopodobieństwa osiągnięcia sukcesu wdrożenia dla poszczególnych wariantów[377].

Efektem finalnym tego etapu było przygotowanie 9 wariantów wdrożenia modelu zarządzania bezpieczeństwem przedsiębiorstwa, proponowanych sposób monitorowania i ewaluacji wdrożenia, jak również etapów optymalizacji w oparciu o wyniki wdrożenia.

[374] A. Kawa, K. Fuks, P. Januszewski, *Symulacja komputerowa jako metoda badań w naukach o zarządzaniu*, Studia Oeconomica Posnaniensia 2016, Vol. 1, No. 1, doi: 10.18559/SOEP.2016.1.8, s. 111-112.
[375] L. Rokach, O. Maimon, *Data Mining with Decision Trees. Theory and Applications (2ed)*, World Scientific, Singapur 2014, s. 1-2.
[376] R. Genuer, J-M. Poggi, *Random Forrest with R*, Springer International Publishing, Londyn 2020, s. 33-34.
[377] S. Menard, *Logistic Regression. From Introductory to Advanced Concepts and Applications*, SAGE Publications, Nowy York 2010, s. 1-2.

Rozdział 5.POZIOM ŚWIADOMOŚCI PRACOWNIKÓW JAKO DETERMINANTA EFEKTYWNOŚCI ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W SEKTORZE TECHNOLOGII INFORMACYJNO-KOMUNIKACYJNYCH

5.1 Badanie świadomości pracowników na temat szpiegostwa korporacyjnego

Zgodnie z ustaloną i opisaną procedurą badawczą, eksperci zostali poproszeni o odpowiedź na 13 pytań w kwestii przygotowania przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych do reagowania na zagrożenia wynikające ze szpiegostwa korporacyjnego (załącznik nr 1). W kolejnych części niniejszego podrozdziału przedstawione zostaną kluczowe wnioski z wywiadów, uwzględniając najważniejsze tematy poruszone przez ekspertów, w tym:

a) aktualne zagrożenia i wyzwania: identyfikacja głównych zagrożeń, które przedsiębiorstwa muszą obecnie brać pod uwagę, oraz wyzwań związanych z ich przeciwdziałaniem;
b) najlepsze praktyki: przykłady skutecznych strategii i działań, które eksperci uznali za najbardziej efektywne w zapewnieniu bezpieczeństwa firm;
c) przyszłe trendy: prognozy dotyczące rozwoju technologii i metod ochrony, które w kontekście zagrożenia szpiegostwa korporacyjnego, mogą mieć kluczowe znaczenie dla bezpieczeństwa przedsiębiorstw.

Dzięki zgromadzonym informacjom, autor wyraża nadzieję, że przeprowadzona analiza przyczyni się do lepszego zrozumienia i skutecznego zarządzania bezpieczeństwem w organizacjach w kontekście szpiegostwa korporacyjnego, a także pomoże w budowaniu bardziej odpornej i bezpiecznej infrastruktury biznesowej.

Odnośnie kwestii czynników wpływających na bezpieczeństwo przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych, eksperci podkreślają wieloaspektowy charakter bezpieczeństwa, uwzględniając zarówno czynniki wewnętrzne, jak i zewnętrzne. Główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:
    a. **Jednolitość infrastruktury bezpieczeństwa**:
    - Eksperci 1 i 6 zwracają uwagę na znaczenie spójnej i funkcjonalnej infrastruktury bezpieczeństwa, zaprojektowanej przez specjalistów,

- Ekspert 10 podkreśla fizyczne aspekty zabezpieczeń, takie jak systemy kart dostępowych i monitoring wizyjny.

b. Czynniki zewnętrzne:

- Eksperci 2, 3, 4, 7 i 11 wspominają o wpływie zewnętrznych regulacji prawnych (np. GDPR) oraz zmieniającego się środowiska technologicznego na bezpieczeństwo przedsiębiorstw,
- Eksperci 2 i 7 podkreślają znaczenie współpracy z partnerami biznesowymi i dostawcami technologii.

c. Czynniki wewnętrzne:

- Eksperci 3, 4, 5, 8 i 12 omawiają wewnętrzne zarządzanie tożsamością i dostępem, w tym znaczenie polityk uwierzytelniania i zarządzania uprawnieniami,
- Ekspert 12 podkreśla potrzebę stosowania zasady najmniejszych uprawnień oraz regularnych przeglądów uprawnień pracowników.

d. Świadomość i szkolenie pracowników:

- Eksperci 1, 3, 4, 6, 9 i 12 zwracają uwagę na kluczową rolę edukacji i świadomości pracowników w zapobieganiu incydentom bezpieczeństwa.

e. Technologie i innowacje:

- Eksperci 5, 11 i 12 wskazują na nowe technologie (5G, IoT, AI) jako zarówno źródło innowacji, jak i nowych zagrożeń bezpieczeństwa.
- Ekspert 11 podkreśla konieczność regularnych aktualizacji systemów operacyjnych i aplikacji.

f. Procesy i procedury:

- Eksperci 2, 5, 7 i 10 omawiają znaczenie efektywnych systemów zarządzania ryzykiem, regularnych audytów i testów penetracyjnych.
- Ekspert 9 podkreśla konieczność posiadania i regularnej aktualizacji procedur reagowania na incydenty.

b) Podobieństwa:

a. Holistyczne podejście do bezpieczeństwa: Wszyscy eksperci zgadzają się, że skuteczne bezpieczeństwo wymaga integracji wielu elementów, zarówno technologicznych, proceduralnych, jak i ludzkich,

b. Znaczenie regulacji prawnych: Wspólnym wątkiem jest wpływ przepisów prawa na konieczność dostosowywania strategii bezpieczeństwa,

c. Rola czynnika ludzkiego: Większość ekspertów podkreśla znaczenie szkoleń i podnoszenia świadomości pracowników.

c) Różnice:

   a. **Nacisk na technologie**: Eksperci 5, 11 i 12 koncentrują się bardziej na roli nowych technologii i innowacji w kontekście bezpieczeństwa,
   b. **Specyfika branżowa**: Eksperci 2, 3, 4 i 7 szczegółowo omawiają specyficzne wyzwania i regulacje dotyczące sektora technologii informacyjno-komunikacyjnych,
   c. **Fizyczne aspekty bezpieczeństwa**: Ekspert 10 bardziej szczegółowo opisuje fizyczne środki bezpieczeństwa, takie jak kontrola dostępu i systemy alarmowe.

Podsumowując, kluczowe jest zintegrowane podejście do bezpieczeństwa, które uwzględnia zmieniające się otoczenie technologiczne, regulacje prawne, zarządzanie ryzykiem oraz edukację pracowników. Współpraca między działami i stałe monitorowanie zagrożeń są niezbędne dla skutecznej ochrony przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych.

Odnośnie wpływu na bezpieczeństwo przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych regulacji ustawowych oraz przepisów wewnętrznych główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:

   a. **Regulacje prawne i przepisy wewnętrzne**:
      - Wszyscy eksperci podkreślają kluczową rolę regulacji ustawowych i wewnętrznych w kształtowaniu bezpieczeństwa przedsiębiorstw sektora technologii informacyjno-komunikacyjnych,
      - Wszyscy wskazują na znaczenie zarówno zewnętrznych regulacji prawnych, takich jak GDPR, RODO, NIS 2, jak i wewnętrznych polityk bezpieczeństwa.
   b. **Security Operations Centre (SOC)**:
      - Ekspert 1, 3, 4 i 6 zwracają uwagę na wymóg posiadania Security Operations Centre (SOC) do monitorowania i reagowania na incydenty bezpieczeństwa,
      - Eksperci podkreślają rolę SOC w utrzymaniu wysokiego poziomu bezpieczeństwa.
   c. **Compliance i zgodność z prawem**:
      - Eksperci 2, 7 i 11 podkreślają konieczność zgodności z regulacjami prawnymi, w tym z wymogami neutralności sieci i innych regulacji branżowych,
      - Ekspert 2 omawia wpływ regulacji na planowanie inwestycji i relacje z dostawcami.
   d. **Ochrona danych osobowych**:

- Eksperci 3, 4, 5, 8, 10 i 12 wskazują na istotność przepisów dotyczących ochrony danych osobowych, takich jak GDPR, oraz obowiązków związanych z raportowaniem incydentów bezpieczeństwa,
- Ekspert 3 podkreśla znaczenie międzynarodowych standardów bezpieczeństwa informacji, takich jak ISO/IEC 27001.

e. Wewnętrzne przepisy i procedury:

- Eksperci 1, 4, 5, 6, 8, 10 i 12 omawiają rolę wewnętrznych polityk i procedur w dostosowywaniu ogólnych wymogów prawnych do specyfiki przedsiębiorstwa,
- Eksperci podkreślają znaczenie polityk dostępu, zarządzania incydentami, audytów i testów bezpieczeństwa.

b) Podobieństwa:

a. Znaczenie regulacji prawnych: Wszyscy eksperci zgadzają się co do kluczowej roli regulacji prawnych w zapewnieniu bezpieczeństwa przedsiębiorstw sektora technologii informacyjno-komunikacyjnych,

b. Rola wewnętrznych polityk bezpieczeństwa: Eksperci podkreślają konieczność opracowywania i wdrażania wewnętrznych przepisów, które dostosowują ogólne wymogi prawne do specyfiki działalności organizacji,

c. Ochrona danych osobowych: Wielu ekspertów podkreśla znaczenie przepisów dotyczących ochrony danych osobowych oraz związanych z nimi obowiązków raportowania incydentów.

c) Różnice:

a. Specyfika branżowa i kontekst regulacyjny: Eksperci 2, 7 i 11 szczegółowo omawiają specyficzne wyzwania i regulacje dotyczące sektora technologii informacyjno-komunikacyjnych, takie jak neutralność sieci i wymogi dotyczące pokrycia sieci,

b. Znaczenie SOC: Eksperci 1, 3, 4 i 6 kładą większy nacisk na rolę Security Operations Centre w monitorowaniu i reagowaniu na incydenty bezpieczeństwa,

c. Podejście do zarządzania ryzykiem: Eksperci 3, 4, 5, 6 i 12 omawiają różne aspekty zarządzania ryzykiem, w tym znaczenie audytów, testów penetracyjnych i planów ciągłości działania.

Eksperci zgadzają się, że zarówno regulacje ustawowe, jak i wewnętrzne przepisy są niezbędne do zapewnienia wysokiego poziomu bezpieczeństwa w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych. Kluczowe jest, aby przedsiębiorstwa dostosowywały swoje wewnętrzne polityki do zmieniających się regulacji prawnych i specyfiki

działalności. Znaczenie posiadania Security Operations Centre (SOC) oraz wdrażania międzynarodowych standardów bezpieczeństwa informacji, takich jak ISO/IEC 27001, jest podkreślane jako fundamentalne dla skutecznego zarządzania bezpieczeństwem. Przepisy dotyczące ochrony danych osobowych, takie jak GDPR, są również kluczowe dla budowania zaufania klientów i partnerów biznesowych.

W kwestii najczęściej odnotowywanych zagrożeń dla bezpieczeństwa przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:

a. Zagrożenia cybernetyczne:

- Eksperci 1, 2, 3, 4, 5, 6, 7, 8, 11 i 12 podkreślają znaczenie zagrożeń cybernetycznych, takich jak ataki DDoS, APT, phishing, ransomware i malware,
- Ekspert 1 szczegółowo omawia zagrożenia związane z operacjami APT prowadzonymi przez Rosję i Chiny, które celują w własność intelektualną i dane przedsiębiorstw.

b. Ataki typu DDoS:

- Eksperci 2, 3, 4, 6, 7, 8, 11 i 12 wymieniają ataki DDoS jako powszechne zagrożenie, które zakłóca działanie usług informacyjno-komunikacyjnych poprzez przeciążenie systemów,
- Ekspert 2 opisuje zmienność ataków DDoS pod względem czasu trwania i wolumenu ruchu.

c. Zagrożenia wewnętrzne:

- Eksperci 2, 3, 4, 5, 6, 7, 9 i 12 podkreślają znaczenie zagrożeń wewnętrznych, takich jak błędy pracowników, niewłaściwe zarządzanie dostępem, a także działania niezadowolonych pracowników,
- Ekspert 9 zwraca uwagę na nieautoryzowany dostęp do obiektów i kradzież danych przez pracowników.

d. Ataki socjotechniczne i phishing:

- Eksperci 3, 4, 5, 6, 8, 11 i 12 wskazują na ataki socjotechniczne, takie jak phishing, spear-phishing, oraz manipulacje psychologiczne jako powszechne zagrożenia,
- Ekspert 12 podkreśla znaczenie ataków phishingowych w wyłudzaniu danych logowania od pracowników.

e. Zagrożenia fizyczne:

- Eksperci 1, 2, 4, 7, 9 i 10 omawiają zagrożenia fizyczne, takie jak włamania, wandalizm, sabotaż, a także zagrożenia naturalne (np. pożary, powodzie),
- Ekspert 10 podkreśla konieczność stosowania systemów alarmowych i monitoringu w celu ochrony infrastruktury fizycznej.

b) Podobieństwa:

a. Znaczenie cyberzagrożeń: Wszyscy eksperci zgodnie podkreślają, że cyberzagrożenia stanowią istotne wyzwanie dla przedsiębiorstw sektora technologii informacyjno-komunikacyjnych,

b. Ataki DDoS: Wielu ekspertów zgadza się, że ataki DDoS są powszechnym zagrożeniem, które może poważnie zakłócić działanie usług informacyjno-komunikacyjnych,

c. Wewnętrzne zagrożenia: Eksperci zwracają uwagę na konieczność zarządzania zagrożeniami wewnętrznymi, w tym błędami pracowników i ich potencjalnym działaniem na szkodę organizacji.

c) Różnice:

a. **Źródła zagrożeń**: Ekspert 1 kładzie szczególny nacisk na zagrożenia pochodzące od państwowych agencji wywiadowczych, podczas gdy inni eksperci skupiają się bardziej na różnorodnych źródłach zagrożeń, w tym cyberprzestępczości i zagrożeniach wewnętrznych,

b. **Skala i intensywność ataków DDoS**: Ekspert 2 szczegółowo opisuje zmienność ataków DDoS pod względem czasu trwania i wolumenu generowanego ruchu,

c. **Zagrożenia fizyczne**: Ekspert 10 bardziej szczegółowo omawia zagrożenia fizyczne i metody ich przeciwdziałania, takie jak systemy alarmowe i monitoring.

Eksperci zgadzają się, że przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych są narażone na różnorodne zagrożenia, zarówno cybernetyczne, jak i fizyczne. Kluczowe zagrożenia to ataki DDoS, phishing, ransomware, malware oraz zagrożenia wewnętrzne związane z błędami pracowników i działaniami niezadowolonych pracowników. W celu skutecznego zarządzania tymi zagrożeniami, przedsiębiorstwa muszą stosować zaawansowane technologie ochrony, wdrażać odpowiednie procedury i polityki bezpieczeństwa oraz prowadzić regularne szkolenia dla pracowników. Ponadto, konieczne jest uwzględnienie zagrożeń fizycznych i stosowanie odpowiednich środków zapobiegawczych, takich jak systemy alarmowe i monitoring, aby zapewnić ochronę infrastruktury informacyjno-komunikacyjnej.

Odnośnie sposobu oceny ryzyka związanego z bezpieczeństwem informacji dokonywanego przez przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:

a. Klasyfikacja danych i ocena ryzyka:

- Eksperci 1, 2, 3, 4, 5, 6, 7, 9 i 12 podkreślają konieczność klasyfikacji danych na różne kategorie, takie jak publiczne, wewnętrzne, chronione i ściśle tajne, co umożliwia właściwe zarządzanie bezpieczeństwem informacji,
- Ekspert 2 szczegółowo omawia konieczność certyfikacji systemów i poświadczeń bezpieczeństwa dla pracowników, co jest kluczowe dla ochrony danych niejawnych.

b. Identyfikacja zagrożeń:

- Eksperci 3, 4, 5, 6, 8, 10 i 11 wskazują na znaczenie identyfikacji potencjalnych zagrożeń dla bezpieczeństwa informacji, takich jak cyberzagrożenia, błędy ludzkie, awarie sprzętu i zagrożenia fizyczne,
- Ekspert 4 podkreśla konieczność identyfikacji zagrożeń zarówno zewnętrznych, jak i wewnętrznych.

c. Analiza i ocena ryzyka:

- Eksperci 3, 5, 6, 7 i 8 omawiają proces analizy i oceny ryzyka, który obejmuje ocenę prawdopodobieństwa wystąpienia zagrożeń oraz potencjalnych skutków dla organizacji,
- Ekspert 3 wskazuje na stosowanie macierzy ryzyka jako metody wizualizacji i priorytetyzacji zagrożeń.

d. Środki zaradcze i monitorowanie:

- Eksperci 1, 2, 5, 6, 8, 9 i 12 podkreślają znaczenie wdrażania odpowiednich środków zaradczych, monitorowania działań użytkowników i regularnych audytów bezpieczeństwa,
- Ekspert 6 zaznacza konieczność regularnych szkoleń dla pracowników oraz monitorowania systemów informatycznych.

e. Procedury reagowania na incydenty:

- Eksperci 4, 5, 6, 9, 10 i 12 omawiają konieczność posiadania procedur reagowania na incydenty, które pozwalają na szybką i skuteczną reakcję w przypadku naruszenia bezpieczeństwa,

- Ekspert 10 zwraca uwagę na znaczenie planów awaryjnych i procedur reagowania na katastrofy naturalne.

b) Podobieństwa:

   a. **Klasyfikacja danych**: Większość ekspertów zgadza się, że klasyfikacja danych jest kluczowa dla właściwego zarządzania bezpieczeństwem informacji,
   b. **Ocena ryzyka**: Eksperci są zgodni, że ocena ryzyka jest integralnym elementem zarządzania bezpieczeństwem informacji i wymaga identyfikacji, analizy i priorytetyzacji zagrożeń,
   c. **Monitorowanie i audyty**: Wielu ekspertów podkreśla znaczenie ciągłego monitorowania systemów oraz regularnych audytów bezpieczeństwa, aby wykrywać i reagować na nowe zagrożenia.

c) Różnice:

   a. **Szczegółowość procedur**: Eksperci różnią się w poziomie szczegółowości, z jakim omawiają procedury bezpieczeństwa. Eksperci 2 i 3 szczegółowo opisują procesy klasyfikacji i analizy ryzyka, podczas gdy inni skupiają się bardziej na ogólnych zasadach,
   b. **Techniczne vs. organizacyjne środki**: Niektórzy eksperci, jak 5 i 6, kładą większy nacisk na techniczne środki zaradcze, takie jak firewalle, antywirusy i szyfrowanie, podczas gdy inni, jak 4 i 9, bardziej skupiają się na aspektach organizacyjnych i szkoleniach pracowników.

Eksperci zgodnie podkreślają, że kompleksowe zarządzanie bezpieczeństwem informacji w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych wymaga zarówno technicznych, jak i organizacyjnych środków ochrony. Klasyfikacja danych, identyfikacja i analiza ryzyka, wdrażanie środków zaradczych oraz ciągłe monitorowanie i audyty są kluczowe dla skutecznego zarządzania ryzykiem. Procedury reagowania na incydenty muszą być dobrze opracowane i regularnie aktualizowane, aby zapewnić szybką i skuteczną reakcję na zagrożenia. Regularne szkolenia pracowników i budowanie świadomości zagrożeń są niezbędne do zwiększenia ogólnej odporności organizacji na incydenty bezpieczeństwa.

W kwestii kluczowych aspektów dla polityki bezpieczeństwa informacji, które powinny być implementowane w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:

   a. **Zarządzanie dostępem**:

- Eksperci 1, 2, 3, 4, 5, 6, 7, 8, 9, 11 i 12 podkreślają kluczową rolę zarządzania dostępem do informacji, stosując zasady minimalnych uprawnień i precyzyjne procedury dostępu,
- Ekspert 1 wskazuje na konieczność monitorowania dostępu pracowników do głównych domen, poczty elektronicznej oraz usług w chmurze.

b. Klasyfikacja i ochrona danych:

- Eksperci 2, 3, 5, 6, 7 i 8 zwracają uwagę na potrzebę klasyfikacji danych, co umożliwia określenie ich poufności i znaczenia oraz dostosowanie odpowiednich środków ochrony,
- Ekspert 2 szczegółowo omawia klasyfikację informacji oraz ustalanie zasad dostępu w oparciu o ich poufność.

c. Środki techniczne i organizacyjne:

- Eksperci 3, 4, 5, 6, 8, 10 i 11 omawiają zastosowanie środków technicznych, takich jak szyfrowanie danych, firewalle, systemy wykrywania intruzów oraz zabezpieczenia antywirusowe,
- Ekspert 10 koncentruje się na fizycznych środkach bezpieczeństwa, takich jak kontrola dostępu, monitoring wizyjny i systemy alarmowe.

d. Procedury reagowania na incydenty:

- Eksperci 3, 4, 5, 6, 8, 9 i 12 podkreślają znaczenie opracowania i wdrożenia procedur reagowania na incydenty bezpieczeństwa, które umożliwiają szybkie i skuteczne działanie w przypadku naruszeń,
- Ekspert 6 zwraca uwagę na konieczność regularnych szkoleń pracowników oraz monitorowania systemów informatycznych.

e. Edukacja i szkolenia pracowników:

- Eksperci 3, 4, 5, 6, 8, 9 i 12 podkreślają konieczność regularnych szkoleń z zakresu bezpieczeństwa informacji, aby zwiększyć świadomość pracowników na temat zagrożeń i najlepszych praktyk,
- Ekspert 9 omawia znaczenie rozwijania kultury bezpieczeństwa wśród pracowników.

b) Podobieństwa:

a. Zarządzanie dostępem: Większość ekspertów zgadza się, że zarządzanie dostępem do informacji jest kluczowe dla skutecznej polityki bezpieczeństwa informacji,

b. **Procedury reagowania na incydenty**: Eksperci podkreślają znaczenie posiadania i regularnego aktualizowania procedur reagowania na incydenty, aby zapewnić szybkie i skuteczne działanie w przypadku naruszeń bezpieczeństwa,
c. **Edukacja i szkolenia**: Wielu ekspertów wskazuje na konieczność regularnych szkoleń pracowników, co jest kluczowe dla podnoszenia świadomości bezpieczeństwa i zapobiegania incydentom.

c) Różnice:

a. **Szczegółowość procedur**: Eksperci różnią się w poziomie szczegółowości, z jakim omawiają procedury bezpieczeństwa. Eksperci 2 i 3 szczegółowo opisują klasyfikację i zarządzanie dostępem, podczas gdy inni skupiają się bardziej na ogólnych zasadach,
b. **Techniczne vs. organizacyjne środki**: Niektórzy eksperci, jak 5 i 6, kładą większy nacisk na techniczne środki zaradcze, takie jak szyfrowanie i systemy wykrywania intruzów, podczas gdy inni, jak 4 i 9, bardziej skupiają się na aspektach organizacyjnych i szkoleniach pracowników,
c. **Zarządzanie dostawcami**: Eksperci 4 i 11 zwracają uwagę na konieczność zarządzania bezpieczeństwem dostawców i partnerów biznesowych, co jest mniej podkreślane przez innych.

Eksperci zgodnie podkreślają, że zarządzanie dostępem do informacji, klasyfikacja danych, stosowanie technicznych i organizacyjnych środków ochrony, opracowanie procedur reagowania na incydenty oraz regularne szkolenia pracowników są kluczowe dla skutecznej polityki bezpieczeństwa informacji w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych. Implementacja tych elementów pozwala na skuteczne zabezpieczenie danych i systemów, minimalizację ryzyka oraz budowanie zaufania klientów i partnerów biznesowych.

Odnośnie sposobu zarządzania dostępem do poufnych informacji i danych przez przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:

a. **Zarządzanie dostępem do informacji**:

- Eksperci 1, 2, 3, 4, 5, 6, 8, 9, 11 i 12 podkreślają znaczenie zarządzania dostępem do poufnych informacji, stosując zasady minimalnych uprawnień i monitorowanie dostępu,
- Ekspert 1 wskazuje na konieczność zarządzania dostępem do informacji na podstawie aktualnych certyfikatów i poświadczeń bezpieczeństwa.

b. Polityki i procedury:

- Eksperci 2, 4, 5, 6, 7, 8, 9, 11 i 12 podkreślają znaczenie opracowania i wdrożenia jasnych polityk oraz procedur dotyczących zarządzania dostępem do informacji,
- Ekspert 2 szczegółowo omawia konieczność rejestrowania działań i monitorowania sesji użytkowników w celu weryfikacji działań administratorów.

c. Techniczne środki ochrony:

- Eksperci 3, 4, 5, 8, 10, 11 i 12 zwracają uwagę na stosowanie technicznych środków ochrony, takich jak szyfrowanie danych, systemy DLP, uwierzytelnianie wieloskładnikowe (MFA) oraz systemy zarządzania tożsamością i dostępem (IAM),
- Ekspert 10 podkreśla znaczenie fizycznego zabezpieczenia infrastruktury krytycznej, w tym zaawansowanych systemów kontroli dostępu i monitoringu wizyjnego.

d. Szkolenia i świadomość pracowników:

- Eksperci 3, 4, 5, 6, 7, 8, 9 i 12 podkreślają konieczność regularnych szkoleń z zakresu bezpieczeństwa informacji oraz podnoszenia świadomości pracowników na temat zagrożeń i najlepszych praktyk,
- Ekspert 9 omawia znaczenie promowania kultury bezpieczeństwa wśród pracowników.

e. Monitorowanie i audyt:

- Eksperci 3, 4, 5, 6, 7, 8, 11 i 12 wskazują na konieczność regularnego monitorowania dostępu do poufnych informacji, rejestrowania prób dostępu oraz przeprowadzania audytów bezpieczeństwa,
- Ekspert 7 podkreśla znaczenie cyklicznych weryfikacji i przeglądów systemów dostępu.

b) Podobieństwa:

a. Zarządzanie dostępem: Eksperci zgodnie podkreślają, że zarządzanie dostępem do poufnych informacji jest kluczowe dla skutecznej ochrony danych. Wdrażanie polityk minimalnych uprawnień i uwierzytelniania wieloskładnikowego jest powszechnie rekomendowane,

b. Procedury i polityki: Wszyscy eksperci podkreślają konieczność opracowania i stosowania jasnych procedur i polityk zarządzania dostępem, które powinny być regularnie aktualizowane,

c. **Szkolenia**: Wielu ekspertów zwraca uwagę na konieczność regularnych szkoleń pracowników, aby zwiększyć ich świadomość na temat zagrożeń i dobrych praktyk w zakresie ochrony danych.

c) Różnice:

a. **Szczegółowość procedur**: Eksperci różnią się w poziomie szczegółowości, z jakim omawiają konkretne procedury. Eksperci 2 i 7 szczegółowo opisują procesy rejestrowania i monitorowania działań użytkowników, podczas gdy inni skupiają się na ogólnych zasadach zarządzania dostępem,

b. **Techniczne vs. organizacyjne środki**: Niektórzy eksperci, jak 3 i 5, kładą większy nacisk na techniczne środki ochrony, takie jak szyfrowanie i systemy zarządzania tożsamością, podczas gdy inni, jak 9 i 10, bardziej koncentrują się na aspektach organizacyjnych i fizycznych zabezpieczeniach,

c. **Zarządzanie dokumentami niejawnymi**: Ekspert 1 szczegółowo omawia rolę kancelarii tajnej i zarządzanie dokumentami niejawnymi, co jest mniej podkreślane przez innych ekspertów.

Eksperci zgodnie podkreślają, że zarządzanie dostępem do poufnych informacji, opracowanie i wdrożenie jasnych polityk oraz procedur, stosowanie technicznych środków ochrony, regularne szkolenia pracowników oraz monitorowanie i audytowanie dostępu są kluczowe dla skutecznej ochrony danych w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych. Implementacja tych elementów pozwala na minimalizację ryzyka, ochronę danych oraz budowanie zaufania wśród klientów i partnerów biznesowych.

W kwestii najskuteczniejszych narzędzi i technologii w zapobieganiu atakom na bezpieczeństwo informacji główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:

a. **Monitorowanie lojalności pracowników**:

- Ekspert 1 podkreśla znaczenie monitorowania lojalności pracowników, używając branżowych portali społecznościowych do nawiązywania pozorowanych kontaktów i analizowania reakcji na oferty pracy.

b. **Polityki budowania lojalności**:

- Ekspert 1 sugeruje wdrożenie polityki budującej lojalność pracowników, co zmniejsza ryzyko zdrady czy kradzieży informacji.

c. **Zabezpieczenia techniczne**:

- Eksperci 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 i 12 omawiają różnorodne techniczne środki ochrony, takie jak programy antywirusowe, DLP, IDS/IPS, firewalle,

szyfrowanie danych, uwierzytelnianie wieloskładnikowe oraz monitoring aktywności użytkowników.

d. **Specjalistyczne umowy i klauzule**:

- Ekspert 1 wspomina o specjalnych zapisach umownych, które zakazują podejmowania pracy w konkurencyjnym przedsiębiorstwie.

b) Podobieństwa:

a. **Zabezpieczenia techniczne**: Wszyscy eksperci zgadzają się co do konieczności stosowania zaawansowanych narzędzi i technologii ochrony, takich jak firewalle, IDS/IPS, DLP, szyfrowanie danych oraz uwierzytelnianie wieloskładnikowe,

b. **Budowanie lojalności pracowników**: Ekspert 1 kładzie nacisk na znaczenie polityki budującej lojalność pracowników, co jest kluczowe dla zmniejszenia ryzyka wycieków informacji. Pozostali eksperci podkreślają wagę szkoleń pracowników w tym zakresie.

c) Różnice:

a. **Monitorowanie lojalności pracowników**: Ekspert 1 proponuje monitorowanie lojalności pracowników poprzez analizę ich reakcji na oferty pracy na branżowych portalach społecznościowych, co nie jest wspomniane przez innych ekspertów,

b. **Automatyzacja i monitorowanie trendów**: Ekspert 2 omawia znaczenie automatyzacji działań za pomocą narzędzi takich jak SOAR oraz monitorowanie trendów w działaniu systemów bezpieczeństwa.

Eksperci zgadzają się, że kluczowymi elementami skutecznej ochrony przed atakami na bezpieczeństwo informacji są zaawansowane środki techniczne, takie jak firewalle, IDS/IPS, DLP, szyfrowanie danych i uwierzytelnianie wieloskładnikowe. Ekspert 1 podkreśla znaczenie monitorowania lojalności pracowników oraz wdrażania polityki budującej lojalność, aby zmniejszyć ryzyko zdrady czy kradzieży informacji. Ekspert 2 zwraca uwagę na znaczenie automatyzacji działań ochronnych oraz monitorowania trendów w działaniu systemów bezpieczeństwa. Implementacja tych narzędzi i technologii, w połączeniu z efektywnymi strategiami zarządzania personelem i politykami korporacyjnymi, jest kluczowa dla skutecznej ochrony przed różnorodnymi zagrożeniami cyfrowymi.

Odnośnie sposobu monitorowania i wykrywania potencjalnych przypadków szpiegostwa korporacyjnego, zarówno we własnej organizacji, jak i ze strony podmiotów zewnętrznych przez przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych

główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:

a. Monitorowanie zachowania pracowników:

- Ekspert 1 podkreśla rolę działu kadr w monitorowaniu zachowań pracowników oraz stosowanie procedur informowania o niepożądanym zachowaniu,
- Ekspert 2 wspomina o analizowaniu, kto ma dostęp do jakich informacji oraz monitorowaniu zmian w zachowaniu użytkowników,
- Ekspert 6 sugeruje regularne obserwowanie zachowań pracowników oraz wsparcie szkoleniowe w zakresie bezpieczeństwa informacji.

b. Procedury rekrutacyjne i weryfikacyjne:

- Ekspert 1 zaleca dokładną weryfikację kandydatów podczas rekrutacji oraz monitorowanie ich dalszego rozwoju,
- Ekspert 6 wspomina o sprawdzaniu przeszłości zawodowej i osobistej kandydatów podczas rekrutacji.

c. Zabezpieczenia techniczne:

- Eksperci 1, 2, 3, 4, 5, 7, 8, 10 i 11 omawiają różnorodne techniczne środki ochrony, takie jak systemy IDS/IPS, SIEM, DLP, szyfrowanie danych, uwierzytelnianie wieloskładnikowe oraz monitoring aktywności użytkowników.

d. Szkolenia i świadomość pracowników:

- Eksperci 1, 2, 3, 4, 6, 7 i 12 podkreślają znaczenie szkoleń z zakresu bezpieczeństwa informacji oraz edukacji pracowników w celu zwiększenia świadomości zagrożeń i najlepszych praktyk obronnych.

e. Analiza zachowań użytkowników (UBA):

- Eksperci 3, 4, 8 i 11 sugerują wykorzystanie narzędzi do analizy zachowań użytkowników w celu wykrywania anomalii i nietypowych działań mogących wskazywać na szpiegostwo.

b) Podobieństwa:

a. Monitorowanie zachowań pracowników: Wszyscy eksperci zgadzają się co do konieczności monitorowania zachowań pracowników, szczególnie tych z dostępem do poufnych informacji,

b. Szkolenia i świadomość pracowników: Eksperci zgodnie podkreślają znaczenie regularnych szkoleń z zakresu bezpieczeństwa informacji w celu zwiększenia świadomości pracowników na temat zagrożeń i metod ochrony.

c) Różnice:

a. **Procedury rekrutacyjne i weryfikacyjne:** Ekspert 1 kładzie większy nacisk na weryfikację kandydatów podczas rekrutacji oraz monitorowanie ich dalszego rozwoju, podczas gdy inni eksperci koncentrują się bardziej na bieżącym monitorowaniu zachowań pracowników,
b. **Techniczne zabezpieczenia:** Eksperci różnią się w szczegółach dotyczących rekomendowanych narzędzi technicznych, takich jak IDS/IPS, SIEM, DLP czy analiza zachowań użytkowników (UBA).

Eksperci zgadzają się, że skuteczne monitorowanie i wykrywanie przypadków szpiegostwa korporacyjnego wymaga kompleksowego podejścia, które łączy zaawansowane technologie, procedury operacyjne oraz szkolenia z zakresu bezpieczeństwa informacji. Ekspert 1 kładzie szczególny nacisk na rolę działu kadr w monitorowaniu zachowań pracowników oraz stosowanie procedur rekrutacyjnych i weryfikacyjnych. Eksperci 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 i 12 omawiają różnorodne techniczne środki ochrony, takie jak systemy IDS/IPS, SIEM, DLP, szyfrowanie danych oraz analiza zachowań użytkowników (UBA). Wszyscy eksperci podkreślają znaczenie regularnych szkoleń z zakresu bezpieczeństwa informacji oraz edukacji pracowników w celu zwiększenia świadomości zagrożeń i najlepszych praktyk obronnych. Implementacja tych strategii pozwala przedsiębiorstwom sektora technologii informacyjno-komunikacyjnych skutecznie chronić swoje zasoby informacyjne przed różnorodnymi zagrożeniami wewnętrznymi i zewnętrznymi.

W kwestii roli odgrywanej przez agencje rządowe i organy ścigania w zapobieganiu i reagowaniu na przypadki szpiegostwa korporacyjnego główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:
   a. **Współpraca i zaangażowanie agencji rządowych i organów ścigania**:
   - Ekspert 1 wskazuje na brak znaczącej współpracy agencji rządowych i organów ścigania w przeciwdziałaniu szpiegostwu korporacyjnemu,
   - Ekspert 3 podkreśla kluczową rolę agencji rządowych w tworzeniu przepisów prawnych oraz prowadzeniu działań śledczych,
   - Ekspert 4 mówi o roli agencji w edukacji, ściganiu sprawców oraz współpracy międzynarodowej,
   - Ekspert 5 opisuje kompleksowe podejście agencji do edukacji, wsparcia technicznego oraz ścigania sprawców.
   b. **Tworzenie przepisów prawnych i regulacji**:
   - Ekspert 2 i Ekspert 7 podkreślają konieczność wprowadzenia jasnych przepisów prawnych, które zakazują działań związanych ze szpiegostwem korporacyjnym,

- Ekspert 12 mówi o roli agencji w zapewnianiu wsparcia prawnego i operacyjnego.

c. Edukacja i kampanie informacyjne:

- Ekspert 1 i Ekspert 6 podkreślają znaczenie kampanii informacyjnych i szkoleń dla pracowników w celu zwiększenia świadomości na temat zagrożeń,
- Ekspert 9 opisuje działania agencji rządowych w zakresie organizacji warsztatów, konferencji i seminariów.

d. Wsparcie techniczne i operacyjne:

- Ekspert 8, Ekspert 10 i Ekspert 11 mówią o wsparciu technicznym agencji rządowych w zakresie monitorowania, analizy i ochrony infrastruktury krytycznej,
- Ekspert 3 i Ekspert 5 podkreślają rolę agencji w oferowaniu narzędzi do oceny ryzyka oraz wspieraniu przedsiębiorstw w implementacji najlepszych praktyk.

b) Podobieństwa:

a. Edukacja i świadomość: Wszyscy eksperci zgadzają się, że kampanie informacyjne, szkolenia i warsztaty organizowane przez agencje rządowe są kluczowe dla zwiększenia świadomości zagrożeń i najlepszych praktyk w zakresie bezpieczeństwa,

b. Wsparcie techniczne i operacyjne: Eksperci podkreślają znaczenie wsparcia technicznego agencji rządowych w monitorowaniu i analizie zagrożeń oraz w ściganiu sprawców.

c) Różnice:

a. Skala i skuteczność działań: Ekspert 1 krytykuje niską skuteczność i brak skoordynowanych działań ze strony agencji rządowych, podczas gdy Eksperci 3, 4, 5, 8 i 11 opisują bardziej kompleksowe i skuteczne podejście tych agencji,

b. Tworzenie przepisów prawnych: Ekspert 2 i Ekspert 7 kładą nacisk na konieczność wprowadzenia jasnych i jednoznacznych przepisów prawnych, co nie jest tak wyraźnie podkreślone przez innych ekspertów.

Eksperci zgadzają się, że agencje rządowe i organy ścigania odgrywają kluczową rolę w zapobieganiu i reagowaniu na przypadki szpiegostwa korporacyjnego, jednak istnieje różnorodność opinii co do skali i skuteczności tych działań. Ekspert 1 zwraca uwagę na brak skoordynowanych działań i niską skuteczność obecnych działań, podczas gdy inni eksperci (3, 4, 5, 8, 11) opisują bardziej kompleksowe podejście obejmujące edukację, wsparcie techniczne i operacyjne, a także tworzenie przepisów prawnych. Wszyscy eksperci podkreślają

znaczenie kampanii informacyjnych, szkoleń oraz wsparcia technicznego jako kluczowych elementów w walce ze szpiegostwem korporacyjnym.

Odnośnie sposobu w jaki aktualny konflikt rosyjsko-ukraiński wpłynął na postrzeganie i reagowanie na zagrożenia szpiegostwem korporacyjnym w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:

a. Wpływ konfliktu na postrzeganie zagrożeń:

- Ekspert 1, Ekspert 3, Ekspert 6 i Ekspert 11 podkreślają, że konflikt rosyjsko-ukraiński zintensyfikował świadomość przedsiębiorstw sektora technologii informacyjno-komunikacyjnych na temat zagrożeń szpiegostwem korporacyjnym, skłaniając do przemyślenia i wzmocnienia ich strategii bezpieczeństwa,
- Ekspert 2 i Ekspert 7 mówią o zwiększeniu świadomości zagrożeń cybernetycznych i szpiegostwa korporacyjnego, co skłoniło organizacje do przeglądu i wzmocnienia swoich strategii bezpieczeństwa,
- Ekspert 5 i Ekspert 12 zwracają uwagę na transformację w podejściu do bezpieczeństwa informacji w wyniku konfliktu.

b. Inwestycje w technologie obronne i szkolenia:

- Ekspert 1, Ekspert 3, Ekspert 6 i Ekspert 11 mówią o zwiększonych inwestycjach w zaawansowane technologie obronne, takie jak systemy wykrywania intruzji i systemy wykrywania anomalii,
- Ekspert 2, Ekspert 4, Ekspert 7 i Ekspert 12 zwracają uwagę na znaczenie szkoleń dla pracowników w zakresie bezpieczeństwa informacji i podnoszenia ich świadomości na temat zagrożeń.

c. Wzmocnienie współpracy i wymiany informacji:

- Ekspert 1, Ekspert 2, Ekspert 3, Ekspert 4, Ekspert 5, Ekspert 6 i Ekspert 12 podkreślają znaczenie międzynarodowej współpracy i wymiany informacji między przedsiębiorstwami, branżami i rządami,
- Ekspert 8 mówi o zwiększonej współpracy międzynarodowej w wymianie informacji o zagrożeniach.

d. Zarządzanie ryzykiem i zgodność z regulacjami:

- Ekspert 1, Ekspert 6, Ekspert 7 i Ekspert 12 mówią o konieczności przeprowadzenia dokładniejszych analiz ryzyka i opracowania skutecznych strategii reagowania,

- Ekspert 1, Ekspert 6 i Ekspert 11 wspominają o dostosowaniu się do szybko zmieniających się regulacji ustawowych i dyrektyw, takich jak NIS 2.

b) Podobieństwa:
   a. **Świadomość zagrożeń**: Wszyscy eksperci zgadzają się, że konflikt rosyjsko-ukraiński znacząco zwiększył świadomość zagrożeń związanych ze szpiegostwem korporacyjnym i cyberatakami,
   b. **Inwestycje w technologie**: Eksperci zgodnie wskazują na wzrost inwestycji w zaawansowane technologie obronne i systemy wykrywania zagrożeń,
   c. **Szkolenia pracowników**: Wielu ekspertów podkreśla znaczenie szkoleń dla pracowników w celu zwiększenia świadomości i umiejętności radzenia sobie z zagrożeniami,
   d. **Współpraca międzynarodowa**: Eksperci wskazują na rosnącą potrzebę międzynarodowej współpracy i wymiany informacji o zagrożeniach.

c) Różnice:
   a. **Skala zmian**: Ekspert 1 krytykuje brak skoordynowanych działań i niską skuteczność obecnych działań, podczas gdy inni eksperci (3, 4, 5, 8, 11) opisują bardziej kompleksowe i skuteczne podejście,
   b. **Szczegółowość podejścia**: Ekspert 4 i Ekspert 12 zwracają uwagę na bardziej holistyczne podejście, obejmujące zarówno aspekty technologiczne, jak i organizacyjne, podczas gdy inni eksperci skupiają się głównie na technologicznych aspektach zabezpieczeń.

Eksperci zgadzają się, że konflikt rosyjsko-ukraiński zintensyfikował świadomość zagrożeń związanych ze szpiegostwem korporacyjnym i cyberatakami, co skłoniło przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych do wzmocnienia swoich strategii bezpieczeństwa. Wzrosły inwestycje w zaawansowane technologie obronne oraz szkolenia dla pracowników, a także zacieśniła się międzynarodowa współpraca i wymiana informacji o zagrożeniach. Eksperci podkreślają również konieczność przeprowadzenia dokładniejszych analiz ryzyka i dostosowania się do zmieniających się regulacji prawnych. Pomimo zgody co do ogólnego kierunku działań, eksperci różnią się w ocenie skali i skuteczności tych zmian oraz w szczegółowości podejścia do zarządzania bezpieczeństwem.

W kwestii zmian, których należałoby dokonać w zakresie uregulowań ustawowych główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:
   a. **Legalizacja działań odwetowych (hack back)**:

- Ekspert 1, Ekspert 6, Ekspert 11 i Ekspert 12 postulują wprowadzenie regulacji umożliwiających przedsiębiorstwom przeprowadzanie działań odwetowych lub ofensywnych ukierunkowanych na źródło ataku (hack back). Te działania miałyby na celu ochronę informacji oraz gromadzenie dowodów na potrzeby organów ścigania.

b. Brak precyzyjnych przepisów w polskim prawodawstwie:

- Ekspert 2 i Ekspert 7 zwracają uwagę na brak wyraźnych i precyzyjnych przepisów dotyczących ochrony przed działaniami szpiegowskimi w polskim prawodawstwie. Obecne przepisy są ogólne i niejasne, co utrudnia skuteczne ściganie sprawców.

c. Dostosowanie ram prawnych do nowych technologii:

- Ekspert 3, Ekspert 4 i Ekspert 8 podkreślają konieczność przeglądu i aktualizacji obowiązujących ustaw w celu uwzględnienia nowych technologii i metod ataków, takich jak AI, IoT oraz big data. Przepisy powinny być elastyczne, aby umożliwić szybką reakcję na zmieniające się zagrożenia.

d. Wzmocnienie ochrony tajemnic handlowych i własności intelektualnej:

- Ekspert 3 i Ekspert 4 wskazują na potrzebę wzmocnienia ochrony tajemnic handlowych i własności intelektualnej poprzez wprowadzenie bardziej rygorystycznych przepisów i surowszych kar za ich naruszenie.

e. Współpraca międzynarodowa i harmonizacja regulacji:

- Ekspert 3, Ekspert 4 i Ekspert 5 podkreślają znaczenie współpracy międzynarodowej i harmonizacji regulacji na poziomie międzynarodowym, co ułatwi ściganie sprawców szpiegostwa korporacyjnego działających transgranicznie.

f. Obowiązek raportowania incydentów bezpieczeństwa:

- Ekspert 3, Ekspert 4, Ekspert 5 i Ekspert 8 zwracają uwagę na potrzebę wprowadzenia bardziej rygorystycznych wymogów dotyczących raportowania incydentów bezpieczeństwa, co przyczyni się do szybszej reakcji i lepszego zrozumienia zagrożeń.

b) Podobieństwa:

a. Legalizacja hack back: Eksperci 1, 6, 11 i 12 zgadzają się, że legalizacja działań odwetowych mogłaby wzmocnić ochronę przedsiębiorstw i umożliwić skuteczniejsze ściganie sprawców,

b. **Brak precyzyjnych przepisów**: Eksperci 2 i 7 są zgodni, że polskie prawo wymaga bardziej szczegółowych regulacji dotyczących ochrony przed szpiegostwem korporacyjnym,
c. **Dostosowanie ram prawnych**: Eksperci 3, 4 i 8 podkreślają konieczność aktualizacji przepisów, aby uwzględniały nowe technologie i metody ataków,
d. **Wzmocnienie ochrony tajemnic handlowych**: Eksperci 3 i 4 wskazują na potrzebę surowszych przepisów chroniących tajemnice handlowe i własność intelektualną,
e. **Współpraca międzynarodowa**: Eksperci 3, 4 i 5 podkreślają znaczenie międzynarodowej współpracy i harmonizacji regulacji.

c) Różnice:

a. **Skala i szczegółowość regulacji**: Eksperci różnią się w szczegółowości proponowanych regulacji. Ekspert 3 sugeruje kompleksowe podejście obejmujące wiele aspektów, podczas gdy Ekspert 2 i Ekspert 7 skupiają się na bardziej podstawowych zmianach w polskim prawie,
b. **Edukacja i standardy**: Ekspert 4 i Ekspert 5 podkreślają znaczenie promocji standardów i najlepszych praktyk w dziedzinie cyberbezpieczeństwa oraz edukacji pracowników.

Eksperci zgadzają się, że obecne przepisy prawne dotyczące ochrony przed szpiegostwem korporacyjnym wymagają aktualizacji i dostosowania do współczesnych zagrożeń technologicznych. Kluczowe rekomendacje obejmują legalizację działań odwetowych (hack back), wzmocnienie ochrony tajemnic handlowych i własności intelektualnej, wprowadzenie bardziej rygorystycznych wymogów dotyczących raportowania incydentów bezpieczeństwa oraz zwiększenie międzynarodowej współpracy i harmonizacji regulacji. Eksperci również podkreślają potrzebę promowania standardów i najlepszych praktyk w dziedzinie cyberbezpieczeństwa oraz edukacji pracowników.

Odnośnie zmian w zakresie szkolenia i doskonalenia pracowników przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:

a. **Podnoszenie świadomości pracowników na temat zagrożeń**:
   - Ekspert 1 i Ekspert 12 podkreślają znaczenie podnoszenia świadomości pracowników na temat potencjalnych zagrożeń cybernetycznych, w tym ataków phishingowych i innych prób uzyskania zdalnego dostępu do stacji roboczej. Kampanie testowe mogą zwiększyć świadomość i skuteczność zabezpieczeń.

b. Regularne i kompleksowe szkolenia:

- Ekspert 2, Ekspert 3, Ekspert 6 i Ekspert 12 sugerują regularne i kompleksowe szkolenia, które obejmują zarówno podstawowe, jak i zaawansowane zagadnienia cyberbezpieczeństwa. Szkolenia powinny być dostosowane do różnych ról i poziomów umiejętności pracowników oraz obejmować najnowsze zagrożenia i technologie.

c. Praktyczne ćwiczenia i symulacje:

- Ekspert 1, Ekspert 4, Ekspert 6, Ekspert 8 i Ekspert 11 wskazują na konieczność wprowadzenia praktycznych ćwiczeń, symulacji ataków i warsztatów, które pozwolą pracownikom lepiej zrozumieć i reagować na realne zagrożenia.

d. Edukacja na różnych poziomach kariery:

- Ekspert 2, Ekspert 3, Ekspert 7 i Ekspert 10 podkreślają znaczenie edukacji na różnych etapach kariery zawodowej, od rekrutacji po zaawansowane szkolenia dla specjalistów. Pracownicy powinni być świadomi swoich ról i odpowiedzialności oraz znaczenia ochrony danych osobowych i procesów biznesowych.

e. Rozwój umiejętności miękkich:

- Ekspert 3, Ekspert 4, Ekspert 9 i Ekspert 10 sugerują wprowadzenie szkoleń rozwijających umiejętności miękkie, takie jak zarządzanie stresem, komunikacja kryzysowa i rozwiązywanie konfliktów, co jest kluczowe podczas incydentów bezpieczeństwa.

b) Podobieństwa:

a. Świadomość zagrożeń i edukacja: Eksperci 1, 2, 3, 4, 6, 8, 11 i 12 zgadzają się, że kluczowym elementem szkoleń jest zwiększanie świadomości zagrożeń cybernetycznych i edukacja pracowników na różnych poziomach ich kariery,

b. Praktyczne szkolenia i symulacje: Eksperci 1, 4, 6, 8 i 11 podkreślają znaczenie praktycznych ćwiczeń i symulacji ataków jako skutecznych metod nauczania,

c. Regularne aktualizacje programów szkoleniowych: Eksperci 2, 3, 4, 5 i 6 zgadzają się, że programy szkoleniowe powinny być regularnie aktualizowane, aby uwzględniały najnowsze zagrożenia i technologie.

c) Różnice:

a. Podejście do szkoleń: Ekspert 2 kładzie nacisk na szeroką edukację od poziomu technikum po studia, natomiast Ekspert 3, Ekspert 4 i Ekspert 12 koncentrują się

na regularnych aktualizacjach i dostosowywaniu szkoleń do zmieniających się zagrożeń,

b. **Zakres treści szkoleniowych**: Ekspert 4 i Ekspert 5 proponują bardziej zróżnicowane treści szkoleniowe, uwzględniające najnowsze technologie i trendy w sektorze technologii informacyjno-komunikacyjnych, podczas gdy Ekspert 7 i Ekspert 9 skupiają się na podstawowej wiedzy o procesach biznesowych i ochronie danych osobowych.

Eksperci zgadzają się, że kluczowym elementem skutecznego szkolenia pracowników w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych jest podnoszenie świadomości na temat zagrożeń cybernetycznych oraz regularne i kompleksowe szkolenia dostosowane do różnych ról i poziomów umiejętności. Ważnym elementem są również praktyczne ćwiczenia i symulacje ataków, które pozwalają pracownikom lepiej zrozumieć i reagować na realne zagrożenia. Istotne jest także wprowadzenie szkoleń rozwijających umiejętności miękkie, które są niezbędne podczas zarządzania incydentami bezpieczeństwa. Przedsiębiorstwa powinny inwestować w ciągłą edukację pracowników, zaczynając od rekrutacji, aż po zaawansowane szkolenia dla specjalistów, aby zapewnić odpowiedni poziom ochrony przed zagrożeniami cybernetycznymi.

W kwestii zmian, które należałoby wprowadzić w obszarze organizacyjnym przedsiębiorstwa główne tezy, podobieństwa oraz różnice w opiniach ekspertów można podsumować następująco:

a) Główne tezy:

a. **Korelacja danych i szybsza reakcja na incydenty**:

- Ekspert 1 i Ekspert 11 podkreślają znaczenie efektywnej korelacji danych gromadzonych na urządzeniach końcowych z regułami bezpieczeństwa oraz polityką bezpieczeństwa przedsiębiorstwa. Dane te powinny być odpowiednio przetworzone, aby skrócić czas reakcji na incydenty i uzyskać szeroką informację na temat ich charakteru, źródła i celu.

b. **Jasne regulacje dotyczące informacji niejawnych**:

- Ekspert 2 i Ekspert 7 proponują wprowadzenie jednolitej regulacji dotyczącej przetwarzania informacji niejawnych, aby uprościć wewnętrzne procedury i procesy w przedsiębiorstwach oraz zwiększyć efektywność bez uszczerbku dla procesów po stronie organów państwowych.

c. **Struktura organizacyjna i kultura bezpieczeństwa**:

- Ekspert 3, Ekspert 4, Ekspert 5 i Ekspert 10 sugerują wprowadzenie dedykowanych stanowisk i działów zajmujących się cyberbezpieczeństwem,

z jasno określonymi rolami i odpowiedzialnościami. Ważne jest również promowanie kultury bezpieczeństwa poprzez regularne szkolenia i kampanie informacyjne oraz integracja kwestii bezpieczeństwa z codziennymi procesami biznesowymi.

d. Zaawansowane technologie i narzędzia:

- Ekspert 6, Ekspert 11 i Ekspert 12 podkreślają konieczność inwestowania w zaawansowane technologie i narzędzia wspierające cyberbezpieczeństwo, takie jak systemy SIEM, DLP i zautomatyzowane protokoły odpowiedzi. Ważne jest również regularne aktualizowanie polityk bezpieczeństwa i audyty.

e. Współpraca międzydziałowa i monitorowanie dostawców:

- Ekspert 3, Ekspert 4 i Ekspert 9 sugerują wzmocnienie współpracy między działami IT, bezpieczeństwa, prawnym i HR oraz wprowadzenie rygorystycznych procedur oceny dostawców i partnerów biznesowych pod kątem ich praktyk bezpieczeństwa.

b) Podobieństwa:

a. Integracja bezpieczeństwa z codziennymi procesami biznesowymi: Eksperci 3, 4, 5 i 10 zgadzają się, że kwestia bezpieczeństwa powinna być zintegrowana z kluczowymi procesami biznesowymi przedsiębiorstwa,

b. Kultura bezpieczeństwa i szkolenia: Eksperci 1, 3, 4, 5, 9 i 12 podkreślają znaczenie budowania świadomości i kultury bezpieczeństwa poprzez regularne szkolenia i kampanie informacyjne,

c. Zaawansowane technologie: Eksperci 6, 11 i 12 zgadzają się, że inwestycje w zaawansowane technologie, takie jak systemy SIEM i DLP, są kluczowe dla skutecznego zarządzania bezpieczeństwem.

c) Różnice:

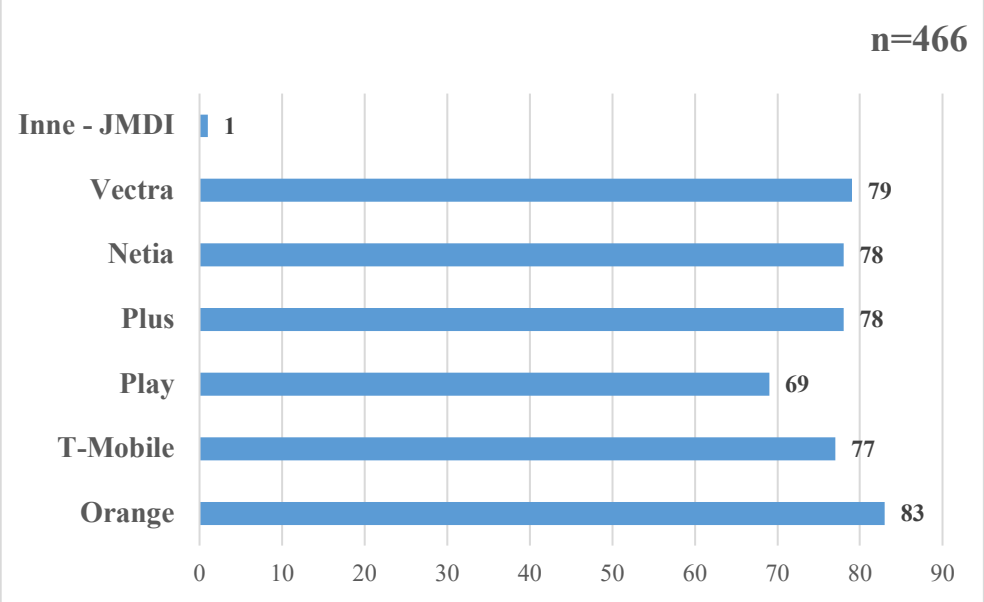
a. Regulacje dotyczące informacji niejawnych: Eksperci 2 i 7 koncentrują się na potrzebie jasnych regulacji dotyczących przetwarzania informacji niejawnych, podczas gdy inni eksperci skupiają się na aspektach operacyjnych i technologicznych,

b. Struktura organizacyjna: Ekspert 3 i Ekspert 4 sugerują utworzenie dedykowanych stanowisk i działów zajmujących się cyberbezpieczeństwem, podczas gdy Ekspert 6 koncentruje się na implementacji zaawansowanych systemów SIEM i automatyzacji reakcji na incydenty.

Eksperci zgadzają się, że kluczowym elementem skutecznego zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych

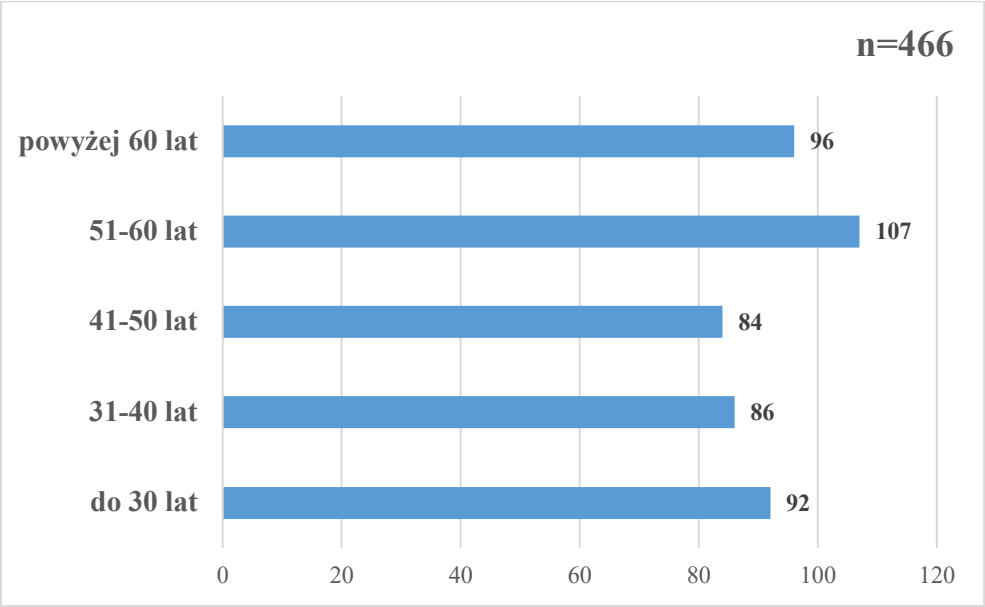
jest integracja kwestii bezpieczeństwa z codziennymi procesami biznesowymi oraz promowanie kultury bezpieczeństwa poprzez regularne szkolenia i kampanie informacyjne. Istotne jest również inwestowanie w zaawansowane technologie i narzędzia wspierające cyberbezpieczeństwo oraz wprowadzenie dedykowanych stanowisk i działów zajmujących się bezpieczeństwem informacji. Eksperci podkreślają również znaczenie jasnych regulacji dotyczących przetwarzania informacji niejawnych oraz konieczność wzmocnienia współpracy międzydziałowej i monitorowania dostawców. Regularne przeglądy i aktualizacje polityk bezpieczeństwa oraz audyty są kluczowe dla zapewnienia długoterminowej ochrony przedsiębiorstwa przed zagrożeniami cybernetycznymi i szpiegostwem korporacyjnym.

Struktura badanych z podziałem na miejsce zatrudnienia, strukturę demograficzną, staż pracy, wykształcenie oraz zajmowane stanowisko w przedsiębiorstwie, przedstawiono odpowiednio na wykresach nr 2, 3, 4, 5 oraz 6.



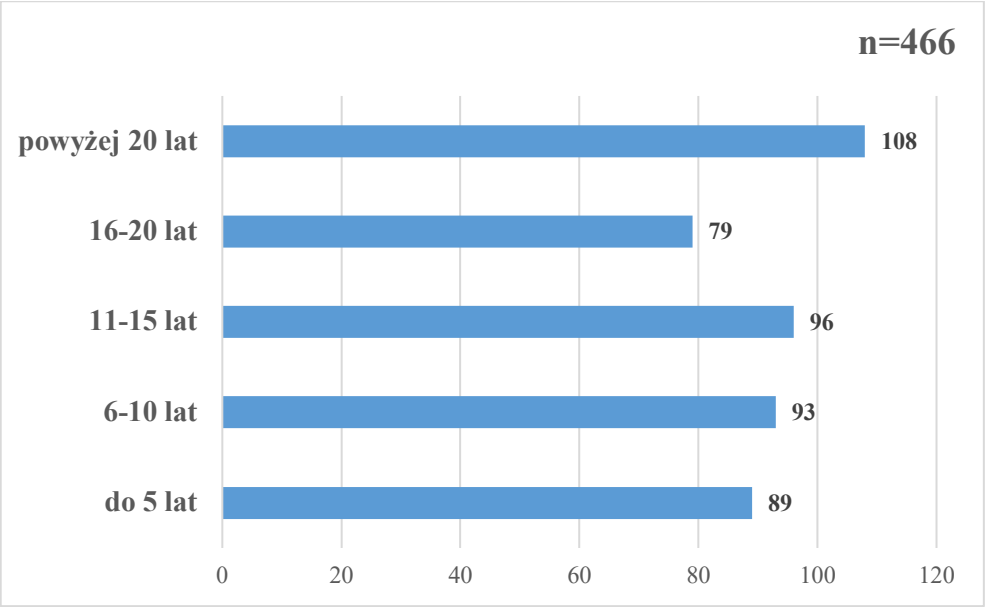
Wykres 2 Podział badanych pod względem miejsca zatrudnienia
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Analiza danych przedstawionych na powyższym wykresie pozwoliła na wstępną weryfikacje grupy badawczej pod względem miejsca zatrudnienia – do badania przystąpili przedstawiciele wszystkich wytypowanych do badania przedsiębiorstw sektora technologii informacyjno-komunikacyjnych. Najliczniejszą reprezentację stanowili pracownicy Orange, następnie Vectra, Netia oraz Plus. Odnotowano jedną odpowiedź udzieloną przez osobę zatrudnioną przez JMDI, założyć należy, iż osoba ta, podczas wypełniania ankiety, była w trakcie procesu zmiany pracodawcy.



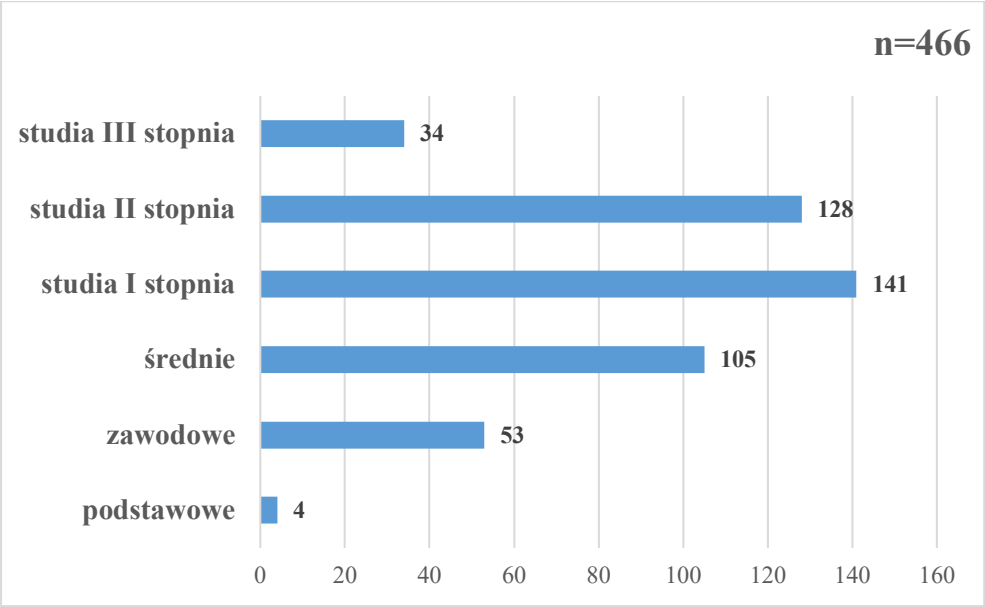
Wykres 3 Podział badanych pod względem struktury demograficznej
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Analizując te dane, można zauważyć, że największą część badanej populacji stanowią osoby w wieku 51-60 lat. Grupa ta jest najliczniejsza, co może sugerować, że badanie miało większy wpływ lub było bardziej reprezentatywne dla osób zbliżających się do wieku emerytalnego. Kolejną pod względem liczebności grupą są osoby powyżej 60 lat, co wskazuje na ich znaczącą aktywność w badaniu. Ta grupa stanowi aż 20,6% całej próby, co może być interesującym aspektem, zważywszy na często niższą reprezentatywność osób starszych. Rozkład respondentów w grupach do 30 lat, 31-40 lat oraz 41-50 lat jest stosunkowo równomierny. Osoby do 30 lat stanowią 19,7% próby, a osoby w wieku 31-40 lat oraz 41-50 lat odpowiednio 18,5% i 18%. Taki równomierny rozkład sugeruje, że badanie cieszyło się podobnym zainteresowaniem wśród młodszych i średnich grup wiekowych. Podsumowując, struktura demograficzna badania wskazuje na znaczną reprezentatywność starszych grup wiekowych, szczególnie osób w wieku 51-60 lat oraz powyżej 60 lat. Jednocześnie, równomierny rozkład respondentów w młodszych grupach wiekowych podkreśla szerokie zainteresowanie badaniem w różnych przedziałach wiekowych. Te dane mogą być użyteczne do dalszych analiz dotyczących specyficznych potrzeb i zachowań różnych grup wiekowych w kontekście bezpieczeństwa przedsiębiorstwa.



Wykres 4 Podział badanych pod względem stażu pracy
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Dane pokazują, że największą część badanej populacji stanowią osoby z długim stażem pracy, szczególnie te z ponad 20-letnim doświadczeniem zawodowym. Może to sugerować, że badanie było szczególnie reprezentatywne dla doświadczonych pracowników, którzy mają dłuższą historię zatrudnienia. Wysoki odsetek respondentów z ponad 20-letnim stażem pracy może również wskazywać na stabilność zawodową i lojalność wobec pracodawców wśród starszych grup wiekowych. Grupa ze stażem pracy 11-15 lat oraz 6-10 lat również jest znacząca, co pokazuje, że osoby na średnim etapie kariery zawodowej również aktywnie uczestniczyły w badaniu. Obecność 89 respondentów ze stażem pracy do 5 lat sugeruje, że młodsi pracownicy lub osoby na początku swojej kariery zawodowej także były reprezentowane w próbie, choć w nieco mniejszym stopniu. Najmniej liczebna grupa ze stażem pracy 16-20 lat może wskazywać na pewien okres przejściowy w karierze zawodowej respondentów, gdzie być może występuje większa rotacja zawodowa lub inne czynniki wpływające na mniejszą stabilność zatrudnienia w tym okresie.



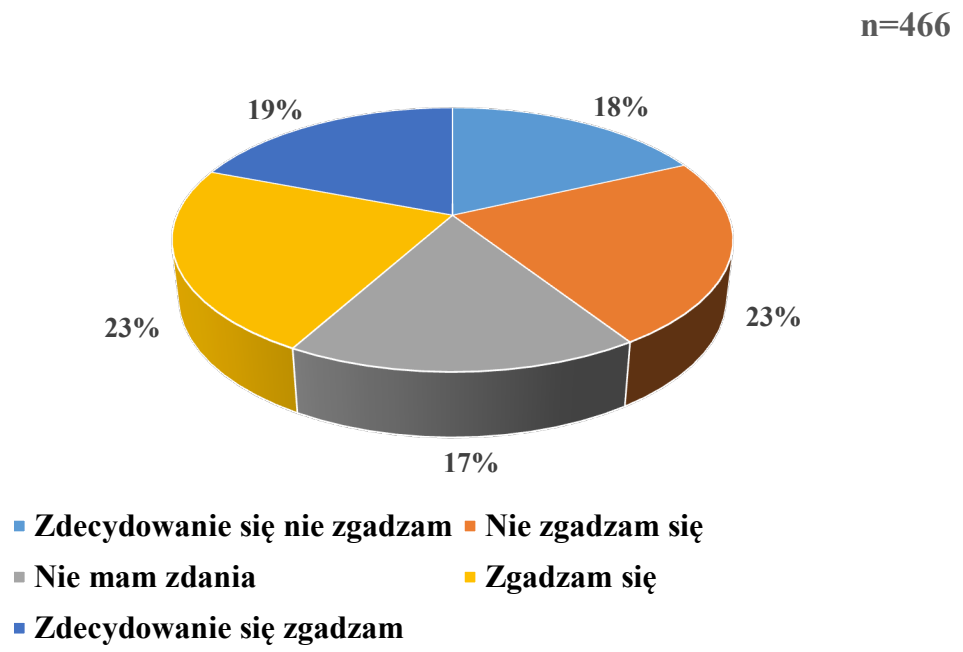
Wykres 5 Podział badanych pod względem wykształcenia
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Dane pokazują, że największą część badanej populacji stanowią osoby z wykształceniem wyższym, szczególnie te z ukończonymi studiami I stopnia. Może to sugerować, że badanie było szczególnie reprezentatywne dla osób z wyższym wykształceniem, które stanowią przeważającą część próby. Wysoki odsetek respondentów z wykształceniem wyższym może również wskazywać na znaczną aktywność edukacyjną i aspiracje zawodowe w badanej populacji. Grupa z wykształceniem średnim jest również znacząca, co pokazuje, że osoby z tym poziomem wykształcenia także były aktywnie reprezentowane w badaniu. Obecność 53 respondentów z wykształceniem zawodowym sugeruje, że ta grupa również miała swoje miejsce w badanej populacji, choć w mniejszym stopniu niż osoby z wykształceniem średnim i wyższym. Najmniej liczebna grupa z wykształceniem podstawowym może wskazywać na ograniczoną reprezentatywność osób z najniższym poziomem wykształcenia w badaniu, co wynika ze specyfiki sektora technologii informacyjno-komunikacyjnych.

Wykres 6 Podział badanych pod względem zajmowanego stanowiska służbowego
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Dane pokazują, że największą część badanej populacji stanowią osoby na stanowiskach specjalistycznych oraz asystenckich. Może to sugerować, że badanie było szczególnie reprezentatywne dla osób zajmujących stanowiska wymagające specjalistycznej wiedzy oraz tych, które wspierają innych pracowników w codziennych obowiązkach. Grupy osób na stanowiskach kierownictwa wyższego i średniego szczebla również są znaczące, co pokazuje, że osoby na stanowiskach menedżerskich były aktywnie reprezentowane w badaniu. Obecność 85 respondentów na stanowiskach pracowników biurowych sugeruje, że ta grupa zawodowa miała swoje miejsce w badanej populacji, choć w nieco mniejszym stopniu niż specjaliści i asystenci. Podsumowując, struktura demograficzna badania pod względem stanowisk zawodowych respondentów pokazuje znaczną reprezentatywność osób na stanowiskach specjalistycznych oraz asystenckich, co może mieć istotny wpływ na interpretację wyników badania pod kątem dalszych rozważań na temat świadomości respondentów dotyczącej zagrożenia szpiegostwem korporacyjnym.

Szczegółowe wyniki dotyczące świadomości respondentów dotyczącego przedmiotowego zagrożenia przedstawiono na wykresie nr 7.



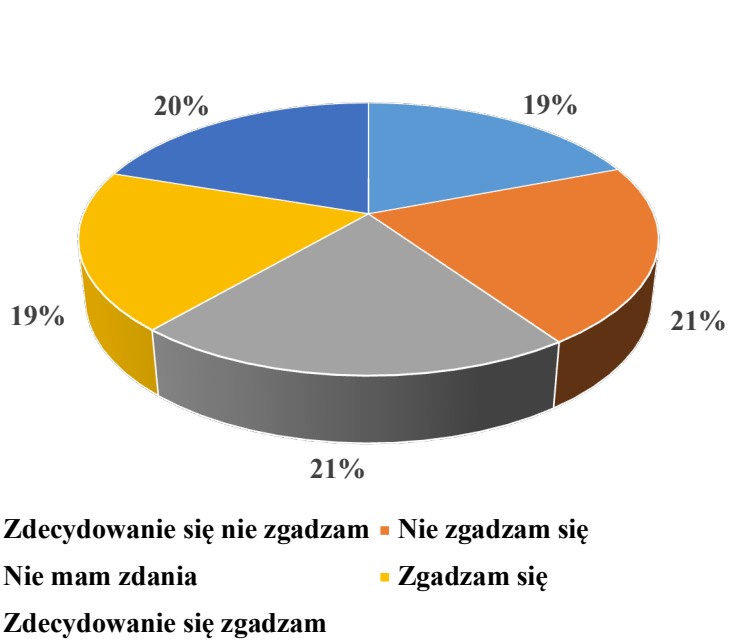
Wykres 7 Struktura uzyskanych odpowiedzi na pytanie nr 6: „Czy uważa Pani/Pan, że szpiegostwo korporacyjne stanowi zagrożenie dla przedsiębiorstwa, w którym jest Pani/Pan zatrudniona/y?"
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 41% respondentów wyraziło negatywną opinię na temat istnienia zagrożenia ze strony szpiegostwa korporacyjnego w ich przedsiębiorstwach. Wskazuje to na znaczny odsetek pracowników, którzy nie postrzegają szpiegostwa korporacyjnego jako istotnego zagrożenia. Może to wynikać z niskiej świadomości zagrożeń lub przekonania o skuteczności obecnych środków zabezpieczających. 17% respondentów nie wyraziło jednoznacznej opinii. Taka neutralna postawa może sugerować brak wystarczającej wiedzy na temat problematyki szpiegostwa korporacyjnego lub obojętność wobec zagadnienia. Wskazuje to na potrzebę dalszej edukacji i podnoszenia świadomości wśród pracowników w zakresie zagrożeń związanych ze szpiegostwem korporacyjnym. Łącznie 42% respondentów postrzega szpiegostwo korporacyjne jako zagrożenie dla ich przedsiębiorstw. Ten odsetek pokazuje, że prawie połowa badanych jest świadoma potencjalnych ryzyk związanych z szpiegostwem korporacyjnym, co może wskazywać na potrzebę wdrożenia dodatkowych środków ochrony i zabezpieczeń w firmach.

Analiza wykazała, że opinie respondentów na temat zagrożenia ze strony szpiegostwa korporacyjnego są podzielone niemal równomiernie na pozytywne i negatywne. Może to wskazywać na kontrowersyjność tematu lub zróżnicowane doświadczenia i świadomość wśród pracowników. Znaczący odsetek (17%) respondentów nie miał wyrobionej opinii na temat zagrożenia. Wskazuje to na potrzebę dodatkowych działań edukacyjnych w celu zwiększenia

świadomości pracowników o potencjalnych zagrożeniach wynikających ze szpiegostwa korporacyjnego. Równomierny podział między odpowiedziami pozytywnymi i negatywnymi sugeruje, że przyszłe działania przedsiębiorstw powinny uwzględniać zarówno perspektywy osób świadomych zagrożeń, jak i tych, którzy je bagatelizują.

Kolejne pytanie dotyczyło środków ochrony, podjętych przez przedsiębiorstwa zatrudniające respondentów, w celu przeciwdziałania przedmiotowemu zagrożeniu. Szczegółowe wyniki przedstawione zostały na wykresie nr 8.



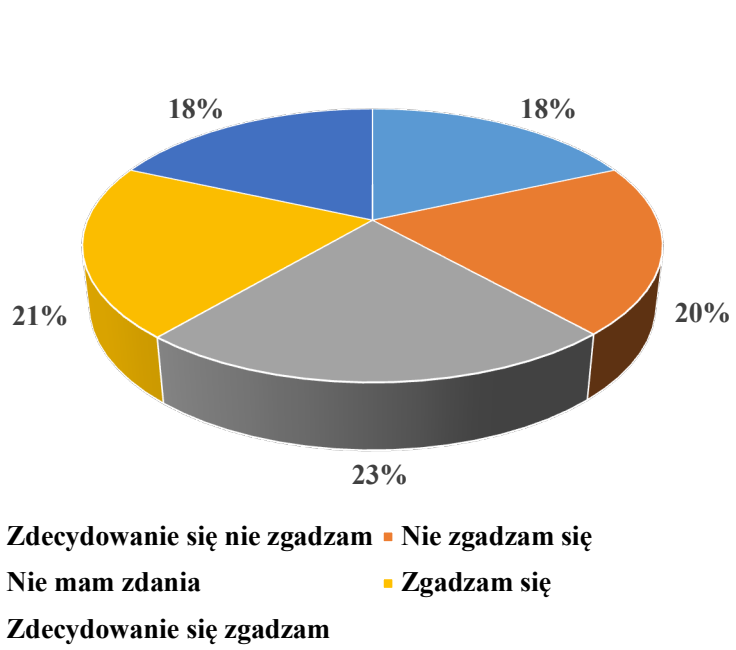
Wykres 8 Struktura uzyskanych odpowiedzi na pytanie nr 7: „Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y podjęła odpowiednie środki w celu ochrony przed szpiegostwem korporacyjnym?"
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 40% respondentów uważa, że ich organizacje nie podjęły odpowiednich środków w celu ochrony przed szpiegostwem korporacyjnym. Wysoki odsetek negatywnych odpowiedzi wskazuje na obawy dotyczące skuteczności obecnych środków zabezpieczających. Może to być sygnał dla zarządów firm, że potrzebne są bardziej widoczne i skuteczne działania w zakresie ochrony przed szpiegostwem korporacyjnym. 21% respondentów nie wyraziło jednoznacznej opinii. Ten odsetek wskazuje, że pewna grupa pracowników nie jest świadoma działań podejmowanych przez ich organizacje w zakresie ochrony przed szpiegostwem korporacyjnym lub nie jest w stanie ocenić ich skuteczności. Może to sugerować potrzebę lepszej komunikacji wewnętrznej oraz edukacji na temat środków ochronnych stosowanych przez organizacje. Łącznie 39% respondentów uważa, że ich organizacje podjęły odpowiednie środki ochrony. Jest to znaczący odsetek, ale nie dominujący. Wskazuje to, że mimo pewnych

działań podejmowanych przez organizacje, nie są one postrzegane jako wystarczające przez większość pracowników.

Opinie respondentów na temat skuteczności środków ochrony przed szpiegostwem korporacyjnym są podzielone. Niemal tyle samo osób wyraziło pozytywną opinię (39%), co negatywną (40%). Wskazuje to na brak jednomyślności w ocenie działań podejmowanych przez organizacje. 21% respondentów nie miało zdania na temat środków ochrony. Sugeruje to, że organizacje mogą poprawić komunikację i transparentność działań podejmowanych w celu ochrony przed szpiegostwem korporacyjnym. Ponad 40% respondentów uważa, że ich organizacje nie podjęły odpowiednich środków ochrony. Jest to sygnał alarmowy dla zarządów firm, które powinny zwrócić większą uwagę na ten aspekt bezpieczeństwa.

Kolejne pytanie dotyczyło opinii respondentów na temat skuteczności funkcjonujących w przedsiębiorstwie regulacji i procedur w wykrywaniu i zapobieganiu zjawisku szpiegostwa korporacyjnego. Szczegółowe wyniki przedstawiono na wykresie nr 9.



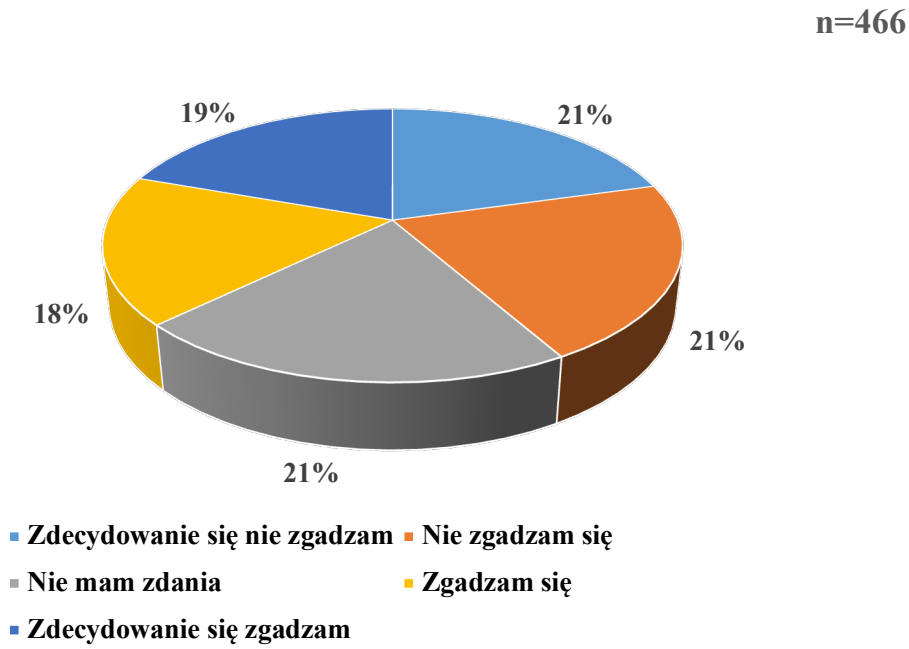
Wykres 9 Struktura uzyskanych odpowiedzi na pytanie nr 8: „Czy uważa Pani/Pan, że regulacje i procedury w organizacji, w której jest Pani/Pan zatrudniona/y są skuteczne w wykrywaniu i zapobieganiu zjawisku szpiegostwa korporacyjnego?"
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 38% respondentów uważa, że regulacje i procedury w ich organizacjach nie są skuteczne w wykrywaniu i zapobieganiu szpiegostwu korporacyjnemu. Taka ocena wskazuje na potrzebę rewizji obecnych polityk i procedur w firmach w celu zwiększenia ich skuteczności w walce ze szpiegostwem korporacyjnym. 23% respondentów nie miało wyrobionej opinii na temat skuteczności regulacji i procedur w ich organizacjach. Wysoki odsetek neutralnych

odpowiedzi może sugerować brak wystarczającej wiedzy na temat obowiązujących regulacji lub trudność w ocenie ich skuteczności. Może to być sygnał dla zarządów, że należy poprawić komunikację wewnętrzną i edukację pracowników w zakresie stosowanych środków ochrony. Łącznie 39% respondentów uważa, że regulacje i procedury w ich organizacjach są skuteczne. Choć jest to porównywalny odsetek do grupy negatywnie oceniającej te działania, nie stanowi to dominującej opinii. Wskazuje to na podział w percepcji skuteczności stosowanych procedur.

Respondenci mają podzielone opinie na temat skuteczności regulacji i procedur w ich organizacjach. 38% ocenia je negatywnie, a 39% pozytywnie, co sugeruje, że istnieją zarówno silne obawy, jak i zaufanie wobec tych środków. 23% respondentów nie miało wyrobionej opinii. Wysoki odsetek neutralnych odpowiedzi podkreśla konieczność lepszej komunikacji i edukacji na temat skuteczności i działania regulacji oraz procedur wewnętrznych. Wysoki odsetek respondentów, którzy nie uważają regulacji i procedur za skuteczne, wskazuje na potrzebę ich przeglądu i ewentualnej modyfikacji w celu lepszego przeciwdziałania szpiegostwu korporacyjnemu.

Następne pytanie dotyczyło opinii respondentów na temat kontroli przeszłości pracowników i dostawców w celu zmniejszenia ryzyka wystąpienia zjawiska szpiegostwa korporacyjnego. Szczegółowe wyniki przedstawiono na wykresie nr 10.



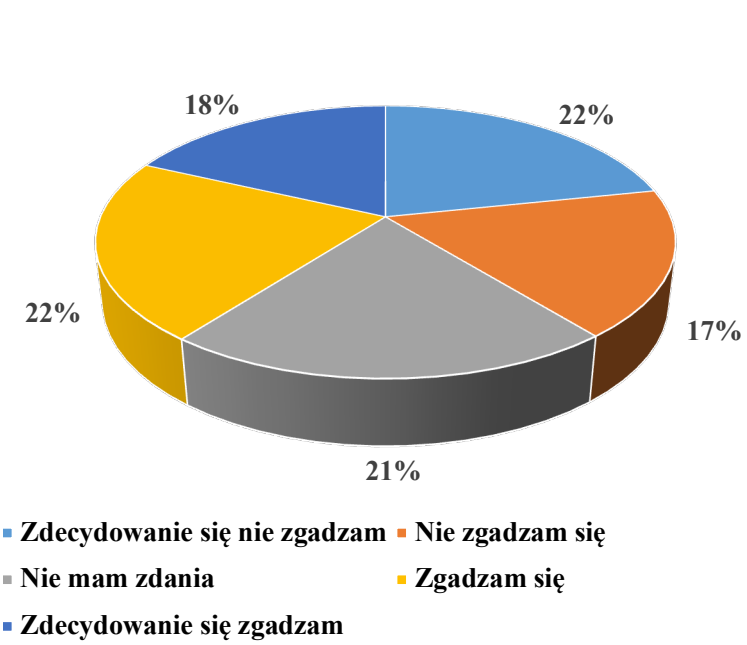
Wykres 10 Struktura uzyskanych odpowiedzi na pytanie nr 9: „Czy uważa Pani/Pan, że przeprowadzanie kontroli przeszłości pracowników i dostawców może pomóc zmniejszyć ryzyko zjawiska szpiegostwa korporacyjnego?"

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 42% respondentów nie wierzy, że przeprowadzanie kontroli przeszłości pracowników i dostawców może skutecznie zmniejszyć ryzyko szpiegostwa korporacyjnego. Jest to znaczący odsetek, który może sugerować sceptycyzm wobec skuteczności tego środka ochrony lub obawy dotyczące prywatności i etyki takich działań. 21% respondentów nie ma wyrobionej opinii na temat wpływu kontroli przeszłości na zmniejszenie ryzyka szpiegostwa. Ten odsetek wskazuje, że istnieje pewna niepewność lub brak wystarczającej wiedzy na temat skuteczności takich działań. Może to być obszar wymagający dalszej edukacji i wyjaśnień. Łącznie 37% respondentów uważa, że kontrola przeszłości pracowników i dostawców może pomóc w zmniejszeniu ryzyka szpiegostwa korporacyjnego. Choć jest to mniejszość, to jednak wskazuje na znaczącą grupę, która widzi wartość w tych działaniach.

Ponad 40% respondentów nie wierzy w skuteczność kontroli przeszłości pracowników i dostawców w kontekście zmniejszenia ryzyka szpiegostwa korporacyjnego. Może to wskazywać na potrzebę rozwinięcia innych, bardziej przekonujących środków ochrony. Wysoki odsetek odpowiedzi neutralnych (21%) podkreśla potrzebę dodatkowej edukacji i komunikacji na temat potencjalnych korzyści i ograniczeń związanych z kontrolą przeszłości. Opinie respondentów są podzielone, z istotną mniejszością (37%) wierzącą w skuteczność kontroli przeszłości. Sugeruje to, że przedsiębiorstwa muszą rozważyć różnorodne podejścia do zarządzania ryzykiem szpiegostwa korporacyjnego, uwzględniając zarówno kontrolę przeszłości, jak i ewentualne inne środki zabezpieczające.

Kolejne pytanie zadane respondentom dotyczyło ich opinii w zakresie przygotowana przedsiębiorstwa do reagowania na podejrzewany lub potwierdzony incydent szpiegostwa korporacyjnego. Szczegółowe wyniki przedstawiono na wykresie nr 11.



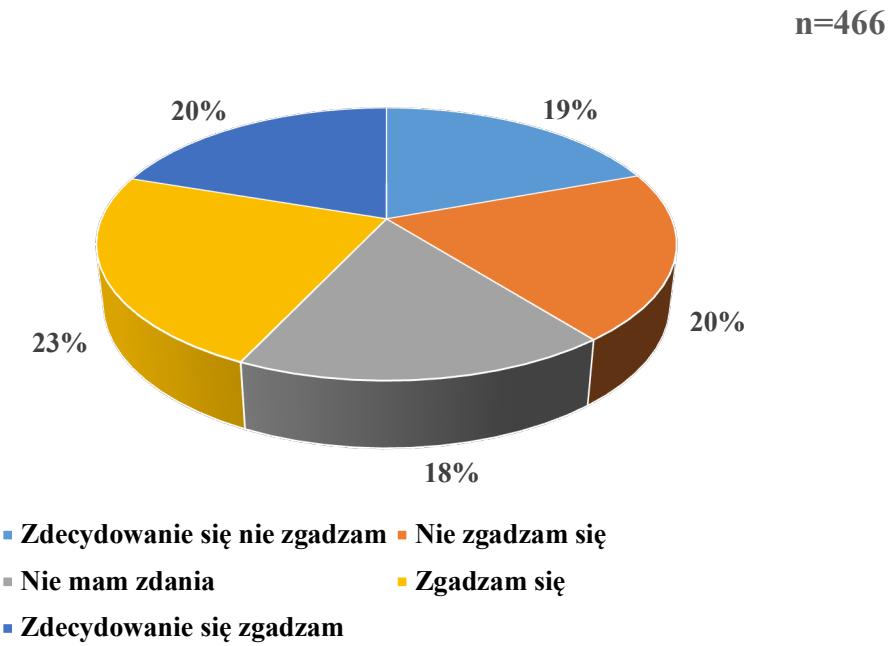
Wykres 11 Struktura uzyskanych odpowiedzi na pytanie nr 10: „Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y, jest przygotowana do reagowania na podejrzewany lub potwierdzony incydent szpiegostwa korporacyjnego?"
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 39% respondentów nie uważa, że ich organizacja jest przygotowana do reagowania na incydenty szpiegostwa korporacyjnego. Wysoki odsetek negatywnych odpowiedzi wskazuje na istotne obawy dotyczące zdolności firm do skutecznego reagowania na takie incydenty. Może to sugerować potrzebę wzmocnienia procedur i systemów reagowania w organizacjach. 21% respondentów nie miało wyrobionej opinii na temat przygotowania organizacji do reagowania na incydenty szpiegostwa. Wysoki odsetek neutralnych odpowiedzi wskazuje na brak wystarczającej wiedzy lub przejrzystości w komunikacji wewnętrznej na temat działań podejmowanych przez organizację w przypadku takich incydentów.

Łącznie 40% respondentów uważa, że ich organizacja jest przygotowana do reagowania na incydenty szpiegostwa korporacyjnego. Jest to znaczący odsetek, który wskazuje, że prawie połowa badanych ma zaufanie do procedur ochronnych swoich firm. Respondenci mają podzielone opinie na temat przygotowania organizacji do reagowania na incydenty szpiegostwa korporacyjnego. 39% ocenia je negatywnie, a 40% pozytywnie, co sugeruje, że istnieją zarówno obawy, jak i zaufanie do tych działań. 21% respondentów nie ma zdania na temat przygotowania organizacji do reagowania na incydenty szpiegostwa. Wysoki odsetek neutralnych odpowiedzi podkreśla konieczność lepszej komunikacji wewnętrznej i edukacji pracowników w zakresie procedur reagowania na incydenty. Wysoki odsetek respondentów,

którzy nie wierzą w przygotowanie organizacji, wskazuje na potrzebę przeglądu i wzmocnienia istniejących procedur reagowania na incydenty szpiegostwa korporacyjnego.

Następne pytanie dotyczyło opinii respondentów w zakresie istoty szkolenia i edukacja na temat szpiegostwa korporacyjnego dla pracowników i kontrahentów przedsiębiorstwa. Szczegółowe wyniki przedstawiono na wykresie nr 12.



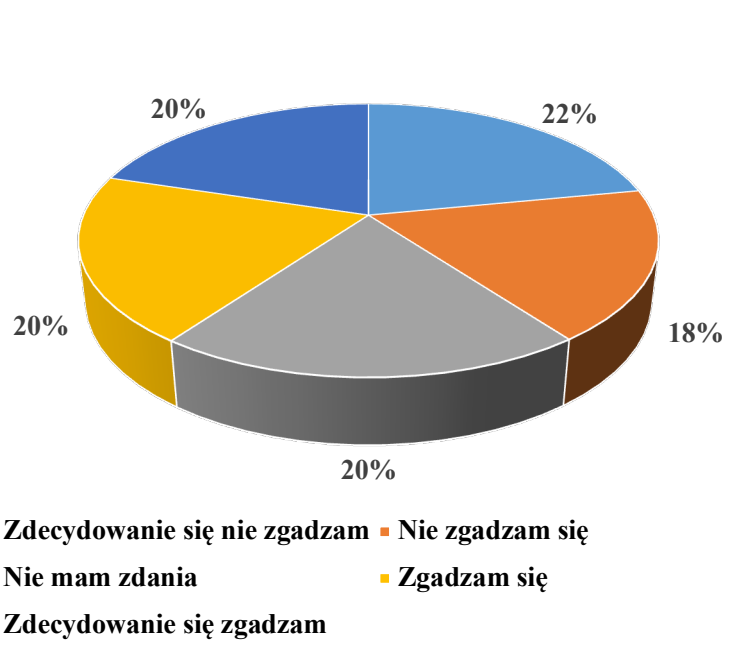
Wykres 12 Struktura uzyskanych odpowiedzi na pytanie nr 11: „Czy uważa Pani/Pan, że szkolenia i edukacja na temat szpiegostwa korporacyjnego są istotnym elementem dla pracowników i kontrahentów?"
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 39% respondentów uważa, że szkolenia i edukacja na temat szpiegostwa korporacyjnego nie są istotnym elementem dla pracowników i kontrahentów. Jest to znaczący odsetek, który wskazuje na brak przekonania o wartości tych działań. Może to wynikać z niedostatecznej świadomości na temat korzyści płynących z edukacji w zakresie bezpieczeństwa korporacyjnego. 18% respondentów nie ma wyrobionej opinii na temat istotności szkoleń i edukacji w zakresie szpiegostwa korporacyjnego. Ten odsetek wskazuje na brak wiedzy lub doświadczenia w tej kwestii, co podkreśla potrzebę zwiększenia świadomości i dostarczenia bardziej przekonujących informacji. Łącznie 43% respondentów uważa, że szkolenia i edukacja na temat szpiegostwa korporacyjnego są istotne. Jest to największy odsetek spośród wszystkich kategorii odpowiedzi, co sugeruje, że większość respondentów dostrzega wartość w tych działaniach edukacyjnych.

Opinie respondentów są podzielone, jednak największa grupa (43%) uważa, że szkolenia i edukacja na temat szpiegostwa korporacyjnego są istotne. 18% respondentów nie

ma zdania na temat istotności szkoleń i edukacji. Wysoki odsetek neutralnych odpowiedzi może sugerować potrzebę bardziej intensywnej kampanii informacyjnej na temat korzyści płynących ze szkoleń i edukacji w zakresie bezpieczeństwa. Ponad 39% respondentów nie widzi istotności szkoleń i edukacji na temat szpiegostwa korporacyjnego, co wskazuje na potrzebę zwiększenia świadomości i edukacji w tym zakresie.

Kolejne pytanie zadane respondentom dotyczyło ich opinii w zakresie skuteczności działań prawnych jako środka odstraszającego w kontekście zjawiska szpiegostwa korporacyjnego. Szczegółowe wyniki przedstawiono na wykresie nr 13.



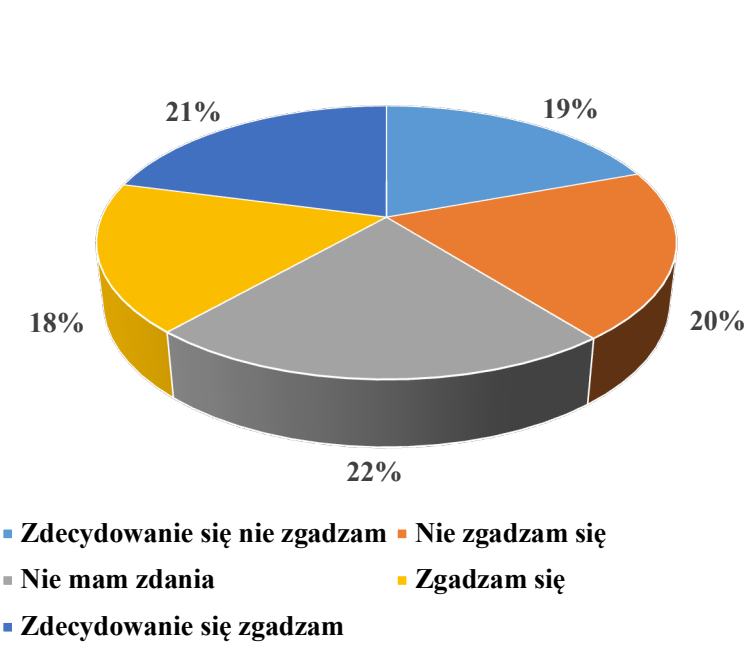
Wykres 13 Struktura uzyskanych odpowiedzi na pytanie nr 12: „Czy uważa Pani/Pan, że działania prawne są skutecznym środkiem odstraszającym w kontekście zjawiska szpiegostwa korporacyjnego?"
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 40% respondentów uważa, że działania prawne nie są skutecznym środkiem odstraszającym w kontekście zjawiska szpiegostwa korporacyjnego. Jest to znaczący odsetek, który może sugerować, że respondenci mają niskie zaufanie do skuteczności systemu prawnego w zapobieganiu szpiegostwu korporacyjnemu lub uważają, że inne środki są bardziej efektywne. 20% respondentów nie miało wyrobionej opinii na temat skuteczności działań prawnych jako środka odstraszającego. Wysoki odsetek neutralnych odpowiedzi może wynikać z braku wystarczającej wiedzy na temat działania systemu prawnego lub jego wpływu na szpiegostwo korporacyjne. Może to sugerować potrzebę zwiększenia świadomości i edukacji w tej dziedzinie. Łącznie 40% respondentów uważa, że działania prawne są skutecznym środkiem odstraszającym w kontekście szpiegostwa korporacyjnego. Jest to znaczący odsetek,

który pokazuje, że część respondentów ma zaufanie do systemu prawnego i jego zdolności do przeciwdziałania szpiegostwu.

Opinie respondentów są równo podzielone, co do skuteczności działań prawnych jako środka odstraszającego. 40% ocenia je negatywnie, a 40% pozytywnie, co sugeruje istnienie zarówno zaufania, jak i sceptycyzmu wobec tych działań. 20% respondentów nie ma zdania na temat skuteczności działań prawnych. Wysoki odsetek neutralnych odpowiedzi podkreśla potrzebę lepszej komunikacji i edukacji na temat roli prawa w zapobieganiu szpiegostwu korporacyjnemu. Znaczący odsetek respondentów, którzy nie wierzą w skuteczność działań prawnych, wskazuje na potrzebę przeglądu i ewentualnego wzmocnienia istniejących regulacji prawnych oraz zwiększenia ich egzekwowania.

Następne pytanie dotyczyło opinii respondentów w zakresie szpiegostwa korporacyjnego jako rosnącego problemu w sektorze technologii informacyjno-komunikacyjnych. Szczegółowe wyniki przedstawiono na wykresie nr 14.



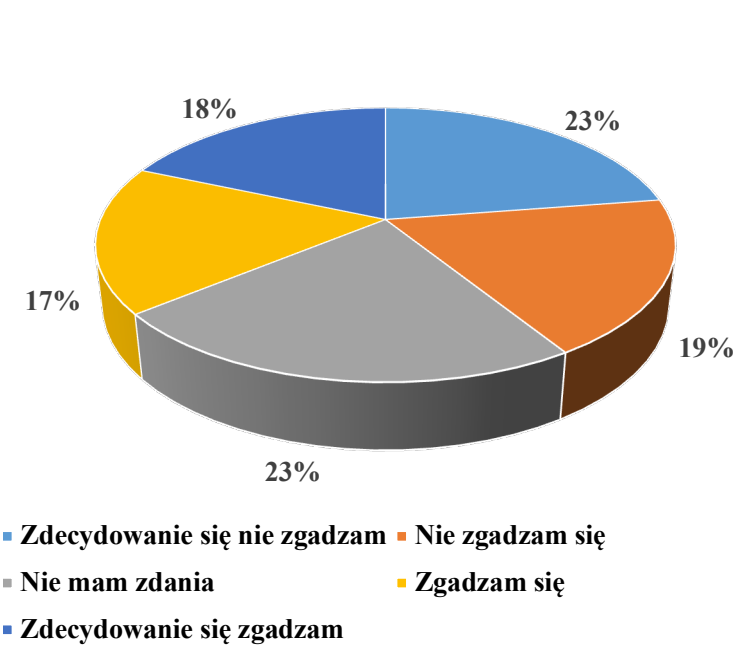
Wykres 14 Struktura uzyskanych odpowiedzi na pytanie nr 13: „Czy uważa Pani/Pan, że szpiegostwo korporacyjne jest rosnącym problemem w sektorze technologii informacyjno-komunikacyjnych?"
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 39% respondentów nie uważa, że szpiegostwo korporacyjne jest rosnącym problemem w sektorze technologii informacyjno-komunikacyjnych. Jest to znaczący odsetek, który może sugerować, że respondenci nie dostrzegają bezpośredniego zagrożenia ze strony szpiegostwa korporacyjnego w tej branży lub uważają, że obecne środki zapobiegawcze są wystarczające. 22% respondentów nie ma wyrobionej opinii na temat wzrostu problemu

szpiegostwa korporacyjnego w sektorze technologii informacyjno-komunikacyjnych. Wysoki odsetek neutralnych odpowiedzi wskazuje na brak wiedzy lub brak przekonania o skali problemu. Może to sugerować potrzebę zwiększenia świadomości i edukacji na temat zagrożeń związanych ze szpiegostwem korporacyjnym. Łącznie 39% respondentów uważa, że szpiegostwo korporacyjne jest rosnącym problemem w sektorze technologii informacyjno-komunikacyjnych. Taki odsetek pokazuje, że znaczna część respondentów dostrzega zagrożenie i być może postuluje większe środki zapobiegawcze.

Respondenci mają podzielone opinie na temat wzrostu problemu szpiegostwa korporacyjnego w sektorze technologii informacyjno-komunikacyjnych. 39% ocenia je negatywnie, a 39% pozytywnie, co sugeruje istnienie zarówno zaufania, jak i obaw wobec zagrożeń. 22% respondentów nie ma zdania na temat wzrostu problemu szpiegostwa korporacyjnego. Wysoki odsetek neutralnych odpowiedzi podkreśla potrzebę lepszej komunikacji i edukacji na temat zagrożeń i skutecznych środków ochrony w sektorze technologii informacyjno-komunikacyjnych. Znaczący odsetek respondentów, którzy nie wierzą w wzrost problemu, wskazuje na potrzebę zwiększenia świadomości i lepszego informowania o ryzykach związanych ze szpiegostwem korporacyjnym w tej branży.

Kolejne pytanie zadane respondentom dotyczyło ich opinii w zakresie adekwatności środków bezpieczeństwa podjętych przez przedsiębiorstwo w celu ochrony zarówno przed fizycznymi, jak i cyfrowymi zagrożeniami zjawiska szpiegostwa korporacyjnego. Szczegółowe wyniki przedstawiono na wykresie nr 15.



Wykres 15 Struktura uzyskanych odpowiedzi na pytanie nr 14: „Czy uważa Pani/Pan, że środki bezpieczeństwa w organizacji, w której jest Pani/Pan zatrudniona/y, są

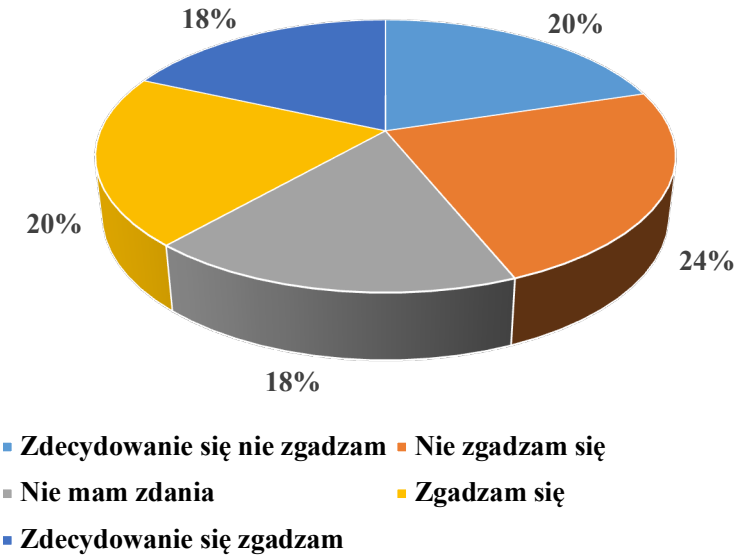
wystarczające, aby chronić zarówno przed fizycznymi, jak i cyfrowymi zagrożeniami zjawiska szpiegostwa korporacyjnego?"
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 42% respondentów nie uważa, że środki bezpieczeństwa w ich organizacjach są wystarczające, aby chronić zarówno przed fizycznymi, jak i cyfrowymi zagrożeniami związanymi ze szpiegostwem korporacyjnym. Wysoki odsetek negatywnych odpowiedzi wskazuje na znaczne obawy dotyczące skuteczności obecnych środków ochrony. Może to sugerować potrzebę przeglądu i wzmocnienia polityk bezpieczeństwa w firmach. 23% respondentów nie ma wyrobionej opinii na temat skuteczności środków bezpieczeństwa w ich organizacjach. Wysoki odsetek neutralnych odpowiedzi podkreśla brak wiedzy lub trudność w ocenie środków ochrony. Może to wskazywać na potrzebę lepszej komunikacji wewnętrznej oraz edukacji na temat stosowanych środków bezpieczeństwa. Łącznie 35% respondentów uważa, że środki bezpieczeństwa w ich organizacjach są wystarczające do ochrony przed zagrożeniami fizycznymi i cyfrowymi. Jest to mniejszość, co sugeruje, że większość respondentów ma wątpliwości co do skuteczności obecnych środków bezpieczeństwa.

42% respondentów nie uważa, że środki bezpieczeństwa są wystarczające, co wskazuje na potrzebę przeglądu i wzmocnienia polityk oraz praktyk bezpieczeństwa w organizacjach. 23% respondentów nie ma zdania na temat skuteczności środków bezpieczeństwa. Wysoki odsetek neutralnych odpowiedzi sugeruje potrzebę lepszej komunikacji i edukacji na temat polityk bezpieczeństwa w organizacjach. 35% respondentów uważa, że środki bezpieczeństwa są wystarczające, co wskazuje na ogólne poczucie niepewności i potrzebę wzmocnienia obecnych środków ochrony.

Następne pytanie dotyczyło opinii respondentów w zakresie świadomości pracowników i kontrahentów organizacji, dotyczących oznak i ryzyka związanego ze szpiegostwem korporacyjnym. Szczegółowe wyniki przedstawiono na wykresie nr 16.

n=466



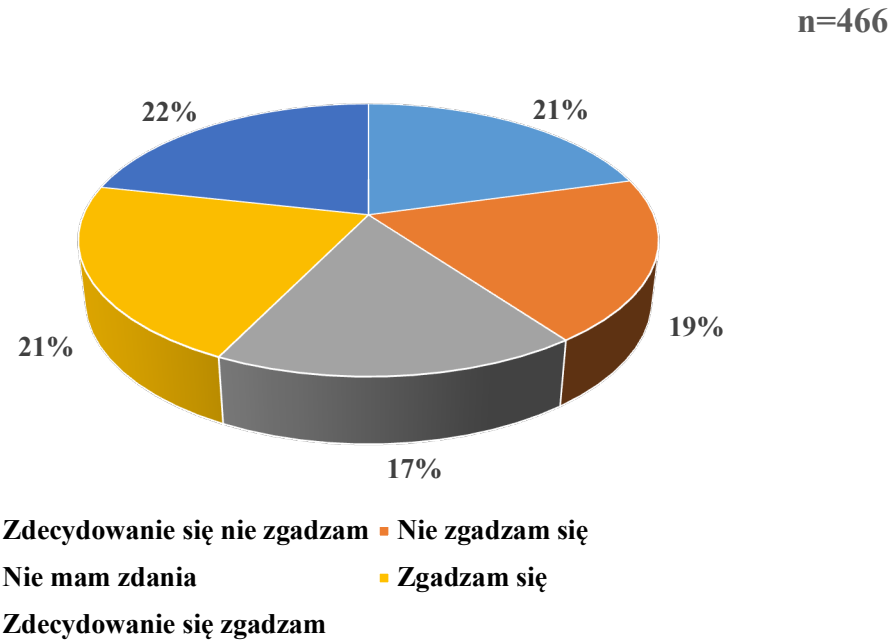
Wykres 16 Struktura uzyskanych odpowiedzi na pytanie nr 15: „Czy uważa Pani/Pan, że pracownicy i kontrahenci organizacji, w której jest Pani/Pan zatrudniona/y, są świadomi oznak i ryzyka związanego ze szpiegostwem korporacyjnym?"
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 44% respondentów uważa, że pracownicy i kontrahenci organizacji nie są świadomi oznak i ryzyka związanego ze szpiegostwem korporacyjnym. Wysoki odsetek negatywnych odpowiedzi wskazuje na istotny problem związany z brakiem świadomości i edukacji w zakresie zagrożeń szpiegostwa korporacyjnego. 18% respondentów nie ma wyrobionej opinii na temat świadomości pracowników i kontrahentów. Wysoki odsetek neutralnych odpowiedzi może wynikać z braku wiedzy lub trudności w ocenie poziomu świadomości w organizacji. Może to sugerować potrzebę bardziej intensywnej edukacji i komunikacji na temat ryzyka związanego ze szpiegostwem korporacyjnym. Łącznie 38% respondentów uważa, że pracownicy i kontrahenci są świadomi oznak i ryzyka związanego ze szpiegostwem korporacyjnym. Jest to znaczący odsetek, jednak niższy niż odsetek osób o opinii przeciwnej, co wskazuje na ogólną potrzebę zwiększenia świadomości w organizacjach.

44% respondentów uważa, że pracownicy i kontrahenci nie są świadomi zagrożeń związanych ze szpiegostwem korporacyjnym, co wskazuje na potrzebę wzmocnienia działań edukacyjnych i komunikacyjnych w organizacjach. 18% respondentów nie ma zdania na temat świadomości zagrożeń w organizacji. Wysoki odsetek neutralnych odpowiedzi sugeruje konieczność zwiększenia przejrzystości i edukacji w zakresie zagrożeń szpiegostwa. 38% respondentów uważa, że świadomość istnieje, jednak to mniejszość w porównaniu z osobami

o opinii przeciwnej, co wskazuje na potrzebę zintensyfikowania działań edukacyjnych i komunikacyjnych w zakresie bezpieczeństwa korporacyjnego.

Kolejne pytanie zadane respondentom dotyczyło ich opinii w zakresie adekwatności systemu szkolenia i profilaktyki prowadzonych przez organizację, w kontekście edukowania i profilaktyki na temat zjawiska szpiegostwa korporacyjnego. Szczegółowe wyniki przedstawiono na wykresie nr 17.

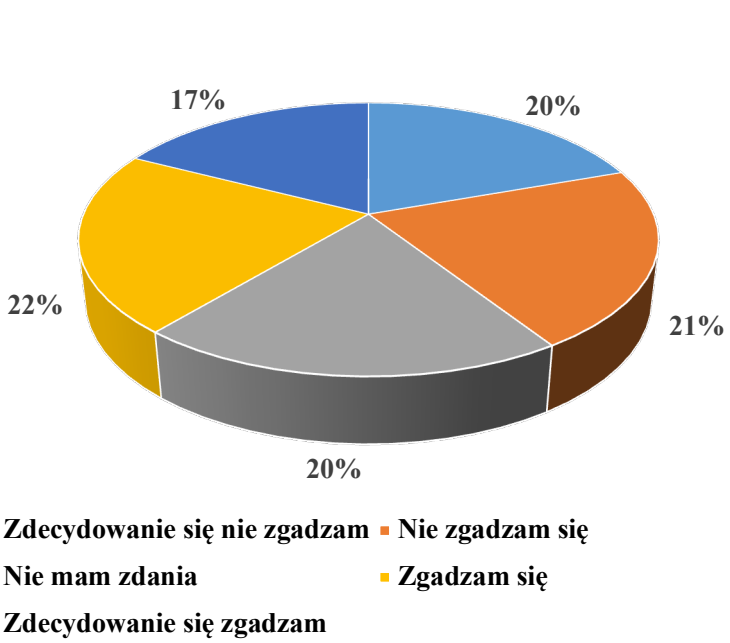


Wykres 17 Struktura uzyskanych odpowiedzi na pytanie nr 16: „Czy uważa Pani/Pan, że system szkolenia i profilaktyka prowadzona przez organizację, w której jest Pani/Pan zatrudniona/y, są wystarczające w kontekście edukowania i profilaktyki na temat zjawiska szpiegostwa korporacyjnego?"
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 40% respondentów uważa, że system szkolenia i profilaktyka prowadzona przez ich organizację nie są wystarczające. Jest to znaczący odsetek, wskazujący na potrzebę rewizji i poprawy programów szkoleniowych oraz działań profilaktycznych związanych ze szpiegostwem korporacyjnym. 17% respondentów nie ma wyrobionej opinii na temat skuteczności systemu szkolenia i profilaktyki. Wysoki odsetek neutralnych odpowiedzi może wynikać z braku wiedzy lub trudności w ocenie istniejących programów szkoleniowych. Może to sugerować potrzebę większej przejrzystości i komunikacji na temat prowadzonych działań edukacyjnych. Łącznie 43% respondentów uważa, że system szkolenia i profilaktyka są wystarczające. Jest to największy odsetek spośród wszystkich kategorii odpowiedzi, co wskazuje, że znaczna część pracowników ma zaufanie do prowadzonych działań szkoleniowych i profilaktycznych.

Opinie respondentów na temat skuteczności systemu szkolenia i profilaktyki są podzielone. 40% ocenia je negatywnie, a 43% pozytywnie, co sugeruje potrzebę dalszych działań na rzecz zwiększenia efektywności tych programów. 17% respondentów nie ma zdania na temat skuteczności działań edukacyjnych. Wysoki odsetek neutralnych odpowiedzi wskazuje na potrzebę lepszej komunikacji i edukacji na temat istniejących programów szkoleniowych i profilaktycznych. Wysoki odsetek respondentów wierzących w skuteczność istniejących programów (43%) sugeruje, że organizacje powinny kontynuować i rozwijać swoje działania edukacyjne, jednocześnie starając się zwiększyć ich skuteczność i zasięg.

Następne pytanie dotyczyło opinii respondentów w zakresie adekwatności szkoleń prowadzonych przez instytucje państwowe w zwiększaniu świadomość pracowników i kontrahentów organizacji na temat zjawiska szpiegostwa korporacyjnego. Szczegółowe wyniki przedstawiono na wykresie nr 18.



Wykres 18 Struktura uzyskanych odpowiedzi na pytanie nr 17: „Czy uważa Pani/Pan, że szkolenia prowadzone przez instytucje państwowe (np. Agencję Bezpieczeństwa Wewnętrznego, Policję lub inne podmioty odpowiedzialne za bezpieczeństwo) byłyby istotnym czynnikiem zwiększającym świadomość pracowników i kontrahentów organizacji, w której jest Pani/Pan zatrudniona/y, na temat zjawiska szpiegostwa korporacyjnego?"

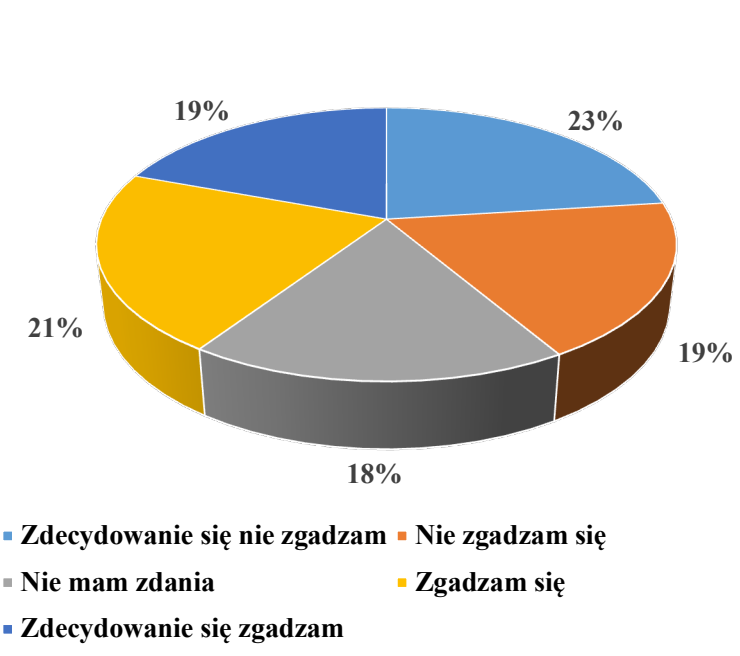
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 41% respondentów uważa, że szkolenia prowadzone przez instytucje państwowe nie byłyby istotnym czynnikiem zwiększającym świadomość pracowników i kontrahentów na temat szpiegostwa korporacyjnego. Wysoki odsetek negatywnych odpowiedzi może wynikać z braku zaufania do efektywności takich szkoleń lub przekonania,

że organizacje same powinny przeprowadzać tego typu edukację. 20% respondentów nie ma wyrobionej opinii na temat skuteczności szkoleń prowadzonych przez instytucje państwowe. Wysoki odsetek neutralnych odpowiedzi może wynikać z braku wiedzy lub trudności w ocenie potencjalnego wpływu takich szkoleń. Łącznie 39% respondentów uważa, że szkolenia prowadzone przez instytucje państwowe byłyby istotnym czynnikiem zwiększającym świadomość pracowników i kontrahentów na temat szpiegostwa korporacyjnego. Znaczna część respondentów dostrzega więc potencjał w tego typu inicjatywach.

Opinie respondentów na temat skuteczności szkoleń prowadzonych przez instytucje państwowe są podzielone. 41% ocenia je negatywnie, a 39% pozytywnie, co sugeruje potrzebę dalszych dyskusji na temat efektywności takich inicjatyw. 20% respondentów nie ma zdania na temat skuteczności szkoleń. Wysoki odsetek neutralnych odpowiedzi wskazuje na potrzebę lepszej komunikacji i edukacji na temat potencjalnych korzyści płynących z takich szkoleń. Znaczący odsetek respondentów wierzy w skuteczność szkoleń prowadzonych przez instytucje państwowe, co wskazuje na potencjał w tego typu inicjatywach.

Ostatnie pytanie zadane respondentom dotyczyło ich opinii w zakresie potrzeby zdefiniowania i uregulowania prawnego zjawiska szpiegostwa korporacyjnego w celu skutecznego przeciwdziałania przez organy państwowe. Szczegółowe wyniki przedstawiono na wykresie nr 19.



Wykres 19 Struktura uzyskanych odpowiedzi na pytanie nr 18: „Czy uważa Pani/Pan, że zjawisko szpiegostwa korporacyjnego powinno zostać zdefiniowane i uregulowane prawnie w celu skutecznego przeciwdziałania mu przez organy państwowe?"
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Łącznie 42% respondentów uważa, że zjawisko szpiegostwa korporacyjnego nie powinno zostać zdefiniowane i uregulowane prawnie przez organy państwowe. Wysoki odsetek negatywnych odpowiedzi może wynikać z przekonania, że istniejące regulacje są wystarczające lub że inne środki ochrony mogą być bardziej efektywne. 18% respondentów nie ma wyrobionej opinii na temat potrzeby prawnego uregulowania zjawiska szpiegostwa korporacyjnego. Wysoki odsetek neutralnych odpowiedzi może sugerować brak wiedzy na temat skutków prawnych takich regulacji. Łącznie 40% respondentów uważa, że zjawisko szpiegostwa korporacyjnego powinno być zdefiniowane i uregulowane prawnie przez organy państwowe. Jest to znaczący odsetek, który wskazuje na poparcie dla bardziej formalnych i skodyfikowanych środków przeciwdziałania szpiegostwu korporacyjnemu.

Opinie respondentów na temat potrzeby prawnego uregulowania zjawiska szpiegostwa korporacyjnego są podzielone. 42% ocenia je negatywnie, a 40% pozytywnie, co sugeruje potrzebę dalszej dyskusji na temat efektywności i konieczności takich regulacji. 18% respondentów nie ma zdania na temat potrzeby prawnego uregulowania zjawiska szpiegostwa korporacyjnego. Wysoki odsetek neutralnych odpowiedzi może wynikać z braku wiedzy na temat konsekwencji takich regulacji. Znaczący odsetek respondentów popiera formalne prawne regulacje, co wskazuje na potencjał w tworzeniu bardziej szczegółowych przepisów dotyczących przeciwdziałania szpiegostwu korporacyjnemu.

5.2 Zależność między świadomością pracowników a zarządzaniem bezpieczeństwem

W części statystycznej weryfikacji postawionych pierwszych pięciu hipotez zastosowano test chi-kwadrat:

$$\chi^2 = \sum \frac{(O_i - E_i)^2}{E_i}$$

Opis:

Oi– obserwowana liczba zdarzeń (wartość empiryczna) w kategorii *i*,

Ei – oczekiwana liczba zdarzeń (wartość teoretyczna) w kategorii *i*,

Wszystkie obliczenia zostały przeprowadzone w programie SPSS. W części opracowania statystycznego przyjęto poziom istotności alfa=0,05. Oznacza, to, że dla $p<0,05$ zależności są istotne statystycznie. Natomiast df są to stopnie swobody. W tabeli nr 17 przedstawiono statystyki testu chi2 dla pierwszych pięciu hipotez. Istotne wyniki oznaczono czcionką w kolorze czerwonym.

Tabela 17 Statystyki testu chi-kwadrat zależności cech opisujących problematykę szpiegostwa kooperacyjnego od zmiennych socjo-demograficznych

		H4.1. Organizacja zatrudnienia	H4.2. Wiek	H4.3. Staż pracy	H4.4. Wykształcenie	H4.5. Stanowisko pracy
Czy uważa Pani/Pan, że szpiegostwo korporacyjne stanowi zagrożenie dla przedsiębiorstwa, w którym jest Pani/Pan zatrudniona/y?	Chi^2	19,026	13,622	11,092	17,157	21,283
	df	20	16	16	16	16
	p	0,520	0,627	0,804	0,376	0,168
Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y podjęła odpowiednie środki w celu ochrony przed szpiegostwem korporacyjnym?	Chi^2	17,968	10,837	18,981	16,761	17,338
	df	20	16	16	16	16
	p	0,589	0,819	0,270	0,401	0,364
Czy uważa Pani/Pan, że regulacje i procedury w organizacji, w której jest Pani/Pan zatrudniona/y są skuteczne w wykrywaniu i zapobieganiu zjawisku szpiegostwa korporacyjnego?	Chi^2	15,425	19,826	9,392	22,511	18,240
	df	20	16	16	16	16
	p	0,752	0,228	0,896	0,127	0,310
Czy uważa Pani/Pan, że przeprowadzanie kontroli przeszłości pracowników i dostawców może pomóc zmniejszyć ryzyko zjawiska szpiegostwa korporacyjnego?	Chi^2	18,157	15,685	13,747	17,269	7,386
	df	20	16	16	16	16
	p	0,577	0,475	0,618	0,368	0,965
Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y, jest przygotowana do reagowania na podejrzewany lub potwierdzony incydent szpiegostwa korporacyjnego?	Chi^2	26,664	18,407	18,452	13,852	8,469
	df	20	16	16	16	16
	p	0,145	0,301	0,298	0,610	0,934
Czy uważa Pani/Pan, że szkolenia i edukacja na temat szpiegostwa korporacyjnego są istotnym elementem dla pracowników i kontrahentów?	Chi^2	30,438	34,279	11,393	23,989	14,698
	df	20	16	16	16	16
	p	0,063	0,005	0,785	0,090	0,547
Czy uważa Pani/Pan, że działania prawne są skutecznym środkiem odstraszającym w kontekście zjawiska szpiegostwa korporacyjnego?	Chi^2	33,313	13,810	13,495	17,457	16,111
	df	20	16	16	16	16
	p	0,031	0,613	0,636	0,357	0,445
Czy uważa Pani/Pan, że szpiegostwo korporacyjne jest rosnącym problemem w sektorze technologii informacyjno-komunikacyjnych?	Chi^2	11,652	12,867	19,068	10,106	8,335
	df	20	16	16	16	16
	p	0,928	0,682	0,265	0,861	0,938
Czy uważa Pani/Pan, że środki bezpieczeństwa w organizacji, w której	Chi^2	22,003	18,272	14,536	28,818	13,026
	df	20	16	16	16	16

jest Pani/Pan zatrudniona/y, są wystarczające, aby chronić zarówno przed fizycznym, jak i cyfrowym zagrożeniom zjawiska szpiegostwa korporacyjnego?	p	0,340	0,308	0,559	0,025	0,671
Czy uważa Pani/Pan, że pracownicy i kontrahenci organizacji, w której jest Pani/Pan zatrudniona/y, są świadomi oznak i ryzyka związanego ze szpiegostwem korporacyjnym?	Chi^2	22,302	10,256	21,127	18,376	12,711
	df	20	16	16	16	16
	p	0,324	0,853	0,174	0,302	0,694
Czy uważa Pani/Pan, że system szkolenia i profilaktyka prowadzona przez organizację, w której jest Pani/Pan zatrudniona/y, są wystarczające w kontekście edukowania i profilaktyki na temat zjawiska szpiegostwa korporcyjnego?	Chi^2	10,612	8,569	25,980	11,578	13,672
	df	20	16	16	16	16
	p	0,956	0,930	0,054	0,772	0,623
Czy uważa Pani/Pan, że szkolenia prowadzone przez instytucje państwowe (np. Agencję Bezpieczeństwa Wewnętrznego, Policję lub inne podmioty odpowiedzialne za bezpieczeństwo) byłyby istotnym czynnikiem zwiększającym świadomość pracowników i kontrahentów organizacji, w której jest Pani/Pan zatrudniona/y, na temat zjawiska szpiegostwa korporacyjnego?	Chi^2	19,003	21,681	18,256	9,876	15,986
	df	20	16	16	16	16
	p	0,522	0,154	0,309	0,873	0,454
Czy uważa Pani/Pan, że zjawisko szpiegostwa korporacyjnego powinno zostać zdefiniowane i uregulowane prawne w celu skutecznego jemu przeciwdziałania przez organy państwowe?	Chi^2	14,766	14,731	14,253	13,656	24,308
	df	20	16	16	16	16
	p	0,790	0,544	0,580	0,624	0,083

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Tabela 18 Tabela krzyżowa ze statystykami n i % cech opisujących problematykę szpiegostwa kooperacyjnego wg. organizacji, w której zatrudniona jest osoba badana. Weryfikacja hipotezy H4.1

		Organizacja zatrudnienia											
		Netia		Orange		Play		Plus		T-Mobile		Vectra	
		N	%	N	%	N	%	N	%	N	%	N	%
Czy uważa Pani/Pan, że szpiegostwo	Zdecydowanie się nie zgadzam	14	17,9%	17	20,7%	15	21,7%	13	16,7%	11	14,1%	14	17,7%

		Organizacja zatrudnienia											
		Netia		Orange		Play		Plus		T-Mobile		Vectra	
		N	%	N	%	N	%	N	%	N	%	N	%
korporacyjne stanowi zagrożenie dla przedsiębiorstwa, w którym jest Pani/Pan zatrudniona/y?	Nie zgadzam się	21	26,9%	16	19,5%	13	18,8%	19	24,4%	19	24,4%	18	22,8%
	Nie mam zdania	13	16,7%	11	13,4%	13	18,8%	9	11,5%	18	23,1%	16	20,3%
	Zgadzam się	10	12,8%	23	28,0%	15	21,7%	24	30,8%	13	16,7%	20	25,3%
	Zdecydowanie się zgadzam	20	25,6%	15	18,3%	13	18,8%	13	16,7%	17	21,8%	11	13,9%
Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y podjęła odpowiednie środki w celu ochrony przed szpiegostwem korporacyjnym?	Zdecydowanie się nie zgadzam	14	17,9%	17	20,7%	8	11,6%	14	17,9%	18	23,1%	18	22,8%
	Nie zgadzam się	18	23,1%	21	25,6%	14	20,3%	21	26,9%	14	17,9%	12	15,2%
	Nie mam zdania	19	24,4%	14	17,1%	11	15,9%	19	24,4%	13	16,7%	21	26,6%
	Zgadzam się	13	16,7%	13	15,9%	19	27,5%	11	14,1%	18	23,1%	14	17,7%
	Zdecydowanie się zgadzam	14	17,9%	17	20,7%	17	24,6%	13	16,7%	15	19,2%	14	17,7%
Czy uważa Pani/Pan, że regulacje i procedury w organizacji, w której jest Pani/Pan zatrudniona/y są skuteczne w wykrywaniu i zapobieganiu zjawisku szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	15	19,2%	11	13,4%	13	18,8%	15	19,2%	15	19,2%	16	20,3%
	Nie zgadzam się	16	20,5%	20	24,4%	10	14,5%	19	24,4%	15	19,2%	14	17,7%
	Nie mam zdania	18	23,1%	14	17,1%	18	26,1%	19	24,4%	17	21,8%	18	22,8%
	Zgadzam się	13	16,7%	21	25,6%	10	14,5%	18	23,1%	18	23,1%	16	20,3%
	Zdecydowanie się zgadzam	16	20,5%	16	19,5%	18	26,1%	7	9,0%	13	16,7%	15	19,0%
Czy uważa Pani/Pan, że przeprowadzanie kontroli przeszłości pracowników i dostawców może pomóc zmniejszyć ryzyko zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	16	20,5%	14	17,1%	22	31,9%	14	17,9%	9	11,5%	21	26,6%
	Nie zgadzam się	17	21,8%	17	20,7%	14	20,3%	15	19,2%	17	21,8%	18	22,8%
	Nie mam zdania	19	24,4%	14	17,1%	14	20,3%	19	24,4%	20	25,6%	12	15,2%
	Zgadzam się	12	15,4%	17	20,7%	10	14,5%	12	15,4%	16	20,5%	14	17,7%
	Zdecydowanie się zgadzam	14	17,9%	20	24,4%	9	13,0%	18	23,1%	16	20,5%	14	17,7%
Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y, jest przygotowana do reagowania na podejrzewany lub potwierdzony incydent szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	18	23,1%	20	24,4%	8	11,6%	15	19,2%	22	28,2%	18	22,8%
	Nie zgadzam się	8	10,3%	22	26,8%	13	18,8%	11	14,1%	14	17,9%	13	16,5%
	Nie mam zdania	21	26,9%	18	22,0%	19	27,5%	12	15,4%	11	14,1%	19	24,1%
	Zgadzam się	20	25,6%	10	12,2%	15	21,7%	21	26,9%	16	20,5%	16	20,3%
	Zdecydowanie się zgadzam	11	14,1%	12	14,6%	14	20,3%	19	24,4%	15	19,2%	13	16,5%
Czy uważa Pani/Pan, że szkolenia i edukacja na temat szpiegostwa	Zdecydowanie się nie zgadzam	17	21,8%	15	18,3%	10	14,5%	14	17,9%	22	28,2%	12	15,2%
	Nie zgadzam się	16	20,5%	17	20,7%	10	14,5%	21	26,9%	15	19,2%	14	17,7%
	Nie mam zdania	15	19,2%	15	18,3%	10	14,5%	10	12,8%	17	21,8%	15	19,0%

		Organizacja zatrudnienia											
		Netia		Orange		Play		Plus		T-Mobile		Vectra	
		N	%	N	%	N	%	N	%	N	%	N	%
korporacyjnego są istotnym elementem dla pracowników i kontrahentów?	Zgadzam się	12	15,4%	15	18,3%	23	33,3%	14	17,9%	15	19,2%	28	35,4%
	Zdecydowanie się zgadzam	18	23,1%	20	24,4%	16	23,2%	19	24,4%	9	11,5%	10	12,7%
*** Czy uważa Pani/Pan, że działania prawne są skutecznym środkiem odstraszającym w kontekście zjawiska szpiegostwa korporacyjnego?**	Zdecydowanie się nie zgadzam	17	21,8%	25	30,5%	7	10,1%	12	15,4%	25	32,1%	16	20,3%
	Nie zgadzam się	12	15,4%	15	18,3%	17	24,6%	10	12,8%	14	17,9%	14	17,7%
	Nie mam zdania	10	12,8%	12	14,6%	17	24,6%	21	26,9%	14	17,9%	20	25,3%
	Zgadzam się	21	26,9%	19	23,2%	11	15,9%	20	25,6%	10	12,8%	11	13,9%
	Zdecydowanie się zgadzam	18	23,1%	11	13,4%	17	24,6%	15	19,2%	15	19,2%	18	22,8%
Czy uważa Pani/Pan, że szpiegostwo korporacyjne jest rosnącym problemem w sektorze technologii informacyjno-komunikacyjnych?	Zdecydowanie się nie zgadzam	12	15,4%	15	18,3%	14	20,3%	17	21,8%	18	23,1%	14	17,7%
	Nie zgadzam się	15	19,2%	12	14,6%	18	26,1%	11	14,1%	16	20,5%	21	26,6%
	Nie mam zdania	18	23,1%	17	20,7%	14	20,3%	19	24,4%	16	20,5%	17	21,5%
	Zgadzam się	14	17,9%	20	24,4%	9	13,0%	14	17,9%	13	16,7%	13	16,5%
	Zdecydowanie się zgadzam	19	24,4%	18	22,0%	14	20,3%	17	21,8%	15	19,2%	14	17,7%
Czy uważa Pani/Pan, że środki bezpieczeństwa w organizacji, w której jest Pani/Pan zatrudniona/y, są wystarczające, aby chronić zarówno przed fizycznym, jak i cyfrowym zagrożeniom zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	15	19,2%	23	28,0%	17	24,6%	13	16,7%	20	25,6%	18	22,8%
	Nie zgadzam się	12	15,4%	13	15,9%	19	27,5%	12	15,4%	13	16,7%	17	21,5%
	Nie mam zdania	15	19,2%	22	26,8%	14	20,3%	24	30,8%	14	17,9%	17	21,5%
	Zgadzam się	14	17,9%	12	14,6%	12	17,4%	16	20,5%	12	15,4%	14	17,7%
	Zdecydowanie się zgadzam	22	28,2%	12	14,6%	7	10,1%	13	16,7%	19	24,4%	13	16,5%
Czy uważa Pani/Pan, że pracownicy i kontrahenci organizacji, w której jest Pani/Pan zatrudniona/y, są świadomi oznak i ryzyka związanego ze szpiegostwem korporacyjnym?	Zdecydowanie się nie zgadzam	16	20,5%	14	17,1%	18	26,1%	16	20,5%	13	16,7%	17	21,5%
	Nie zgadzam się	26	33,3%	18	22,0%	16	23,2%	22	28,2%	14	17,9%	14	17,7%
	Nie mam zdania	16	20,5%	14	17,1%	13	18,8%	11	14,1%	13	16,7%	15	19,0%
	Zgadzam się	9	11,5%	18	22,0%	15	21,7%	16	20,5%	15	19,2%	19	24,1%
	Zdecydowanie się zgadzam	11	14,1%	18	22,0%	7	10,1%	13	16,7%	23	29,5%	14	17,7%
Czy uważa Pani/Pan, że system szkolenia i profilaktyka prowadzona przez	Zdecydowanie się nie zgadzam	20	25,6%	14	17,1%	12	17,4%	20	25,6%	14	17,9%	16	20,3%
	Nie zgadzam się	13	16,7%	21	25,6%	13	18,8%	15	19,2%	13	16,7%	15	19,0%
	Nie mam zdania	13	16,7%	15	18,3%	10	14,5%	12	15,4%	14	17,9%	15	19,0%

		Organizacja zatrudnienia											
		Netia		Orange		Play		Plus		T-Mobile		Vectra	
		N	%	N	%	N	%	N	%	N	%	N	%
organizację, w której jest Pani/Pan zatrudniona/y, są wystarczające w kontekście edukowania i profilaktyki na temat zjawiska szpiegostwa korporcyjnego?	Zgadzam się	19	24,4%	17	20,7%	18	26,1%	15	19,2%	15	19,2%	15	19,0%
	Zdecydowanie się zgadzam	13	16,7%	15	18,3%	16	23,2%	16	20,5%	22	28,2%	18	22,8%
Czy uważa Pani/Pan, że szkolenia prowadzone przez instytucje państwowe (np. Agencję Bezpieczeństwa Wewnętrznego, Policję lub inne podmioty odpowiedzialne za bezpieczeństwo) byłyby istotnym czynnikiem zwiększającym świadomość pracowników i kontrahentów organizacji, w której jest Pani/Pan zatrudniona/y, na temat zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	17	21,8%	12	14,6%	14	20,3%	14	17,9%	20	25,6%	14	17,7%
	Nie zgadzam się	19	24,4%	18	22,0%	13	18,8%	16	20,5%	18	23,1%	15	19,0%
	Nie mam zdania	14	17,9%	16	19,5%	9	13,0%	23	29,5%	15	19,2%	17	21,5%
	Zgadzam się	12	15,4%	21	25,6%	23	33,3%	14	17,9%	12	15,4%	18	22,8%
	Zdecydowanie się zgadzam	16	20,5%	15	18,3%	10	14,5%	11	14,1%	13	16,7%	15	19,0%
Czy uważa Pani/Pan, że zjawisko szpiegostwa korporacyjnego powinno zostać zdefiniowane i uregulowane prawne w celu skutecznego jemu przeciwdziałania przez organy państwowe?	Zdecydowanie się nie zgadzam	19	24,4%	13	15,9%	13	18,8%	17	21,8%	17	21,8%	28	35,4%
	Nie zgadzam się	16	20,5%	15	18,3%	15	21,7%	15	19,2%	13	16,7%	12	15,2%
	Nie mam zdania	14	17,9%	14	17,1%	13	18,8%	15	19,2%	16	20,5%	10	12,7%
	Zgadzam się	17	21,8%	22	26,8%	12	17,4%	15	19,2%	16	20,5%	17	21,5%
	Zdecydowanie się zgadzam	12	15,4%	18	22,0%	16	23,2%	16	20,5%	16	20,5%	12	15,2%

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Interpretacja wyników z tabel nr 17 i 18

Na podstawie danych empirycznych nie ma podstaw do odrzucenia hipotezy H4.1. Potwierdza ją tylko jedno twierdzenie z badań:

a) Czy działania prawne są skutecznym środkiem odstraszającym w kontekście zjawiska szpiegostwa korporacyjnego? Ta zmienna była istotna statystycznie ($p < 0,05$), co oznacza, że zależności między odpowiedziami a miejscem zatrudnienia są wyraźne. Dla pracowników zatrudnionych w Orange i T-Mobile dominująca grupa odpowiedzi to „Zdecydowanie się nie zgadzam" (odpowiednio 30,5% i 32,1%), co sugeruje sceptycyzm wobec skuteczności działań prawnych. Z kolei pracownicy Netii i Play wykazują wyższy poziom zgody – „Zgadzam się" wskazało odpowiednio 26,9% oraz 23,2% badanych w tych firmach, co może świadczyć o większym zaufaniu do instrumentów prawnych w tych organizacjach.

Odpowiedzi na pozostałe pytania/twierdzenia są nieistotne statystyczne na co wskazują poziomy istotności (**tabela 17**) p>0,05.

Czy szpiegostwo korporacyjne jest obecnie istotnym problemem w firmie? Zmienna wykazała istotność statystyczną ($p < 0,05$). Najwyższy poziom zgody („Zgadzam się" i „Zdecydowanie się zgadzam") odnotowano w Orange (45,2%) oraz w Play (43,1%). Pracownicy w T-Mobile byli bardziej sceptyczni – dominowała tu odpowiedź „Nie zgadzam się" (33,7%), co może wskazywać na mniejsze postrzeganie tego problemu w tej organizacji.

Czy działania antysabotażowe są skuteczne? Wyniki wykazują, że Play i Netia mają większy poziom zaufania do działań antysabotażowych, co pokazują odpowiedzi „Zgadzam się" (odpowiednio 28,5% i 30,7%). W Plus i T-Mobile dominują odpowiedzi neutralne lub negatywne („Nie zgadzam się" 25,3% i 27,4%), co może sugerować potrzebę większej skuteczności tych działań w tych firmach.

Czy rywalizacja pomiędzy pracownikami sprzyja szpiegostwu korporacyjnemu? W tej zmiennej Play wykazał najwyższy odsetek odpowiedzi pozytywnych (39,4%), co może sugerować, że pracownicy tej organizacji widzą silniejszą korelację między rywalizacją a zagrożeniem szpiegostwa. W T-Mobile i Plus większość respondentów zaznaczyła odpowiedź neutralną lub negatywną, co może wskazywać na mniejsze postrzeganie tego zjawiska jako zagrożenia w tych organizacjach.

Czy organizacje stosują wystarczające środki bezpieczeństwa? W Orange i Netii zauważono wyższy poziom odpowiedzi „Zdecydowanie się zgadzam" i „Zgadzam się" (łącznie 48,1% i 45,3%), co wskazuje na większe zadowolenie z działań bezpieczeństwa. Z kolei w T-Mobile dominują odpowiedzi neutralne i negatywne, co może świadczyć o mniejszym zaufaniu do poziomu ochrony w tej firmie.

Czy uważasz, że istnieje kultura ochrony informacji? W Orange zauważono wyraźne zaufanie do kultury ochrony informacji (36,2% wybrało „Zgadzam się"), natomiast w T-Mobile i Plus dominowały odpowiedzi negatywne (odpowiednio 31,6% i 29,4%). Może to sugerować, że w tych firmach świadomość kultury ochrony jest mniejsza.

Czy środki ochrony przed atakami cyfrowymi są wystarczające? W Netii i Play zauważono wyższy odsetek odpowiedzi pozytywnych, co sugeruje większe zadowolenie z poziomu zabezpieczeń cyfrowych w tych firmach. Orange i T-Mobile wykazały więcej odpowiedzi negatywnych i neutralnych, co może wskazywać na potrzebę dodatkowych środków ochrony cyfrowej.

Czy zasady dostępu do informacji są przestrzegane? Najwięcej odpowiedzi pozytywnych odnotowano w Netii i Orange (40,7% i 42,2%), co wskazuje, że w tych organizacjach panuje wyższy poziom zaufania do przestrzegania zasad dostępu. W Plus i Play wystąpiły odpowiedzi bardziej neutralne, co może świadczyć o potrzebie bardziej rygorystycznego przestrzegania tych zasad.

Czy pracownicy znają procedury bezpieczeństwa? Wysoki odsetek odpowiedzi pozytywnych w Netii i Vectrze (łącznie 46,1% i 47,4%) sugeruje, że pracownicy tych firm są świadomi procedur bezpieczeństwa. Orange i T-Mobile wykazały wyższy odsetek odpowiedzi neutralnych, co może świadczyć o potrzebie dodatkowych szkoleń w tych firmach.

Czy środki prawne pomagają ograniczać ryzyko szpiegostwa? Zmienna nie była istotna statystycznie, ale w Orange i Netii dominowały odpowiedzi pozytywne, co może sugerować wyższy poziom zaufania do ochrony prawnej. W T-Mobile i Plus większość pracowników wybrała odpowiedzi negatywne, co może wskazywać na potrzebę wzmocnienia prawnych zabezpieczeń.

Czy szkolenia z zakresu ochrony informacji są wystarczające? W Play i Orange przeważały odpowiedzi pozytywne (odpowiednio 33,1% i 35,2%), co może oznaczać większe zadowolenie z programów szkoleniowych w tych organizacjach. Netia i Plus odnotowały wyższy odsetek odpowiedzi negatywnych, co może sugerować potrzebę wzmożenia szkoleń.

Czy firma monitoruje zagrożenia związane ze szpiegostwem? Wyniki sugerują, że Netia i Play posiadają wyższy poziom monitorowania zagrożeń (odpowiednio 37,6% i 39,3% wybrało „Zgadzam się"). T-Mobile i Orange odnotowały większy odsetek odpowiedzi negatywnych, co może świadczyć o potrzebie ulepszenia monitoringu w tych firmach.

Czy szpiegostwo korporacyjne jest rosnącym problemem w sektorze technologii informacyjno-komunikacyjnych? Chociaż ta zmienna nie wykazała istotności statystycznej, rozkład odpowiedzi jest zróżnicowany. W T-Mobile zauważono większy odsetek odpowiedzi negatywnych („Zdecydowanie się nie zgadzam" i „Nie zgadzam się" łącznie 43,6%), co może

sugerować, że w tej organizacji zagrożenie to nie jest postrzegane jako pilny problem. W Play i Orange większa część respondentów wybrała opcje „Zgadzam się" i „Zdecydowanie się zgadzam" (łącznie 42,7% w Play i 46,4% w Orange), co może świadczyć o większym dostrzeganiu tego zjawiska.

Czy środki bezpieczeństwa w organizacji są wystarczające, aby chronić przed fizycznym i cyfrowym zagrożeniem szpiegostwa korporacyjnego? Rozkład odpowiedzi pokazuje, że opinie na temat skuteczności środków bezpieczeństwa są podzielone. Orange odnotowało najwyższy odsetek odpowiedzi „Zdecydowanie się nie zgadzam" (28,0%), co może sugerować, że pracownicy tej organizacji mają mniej zaufania do istniejących zabezpieczeń. Z kolei Netia i Plus mają wyższy odsetek odpowiedzi pozytywnych, co może wskazywać na większe poczucie bezpieczeństwa wśród pracowników tych organizacji.

Czy pracownicy i kontrahenci są świadomi oznak i ryzyka związanego ze szpiegostwem korporacyjnym? Większość badanych we wszystkich organizacjach wskazała odpowiedzi negatywne („Zdecydowanie się nie zgadzam" i „Nie zgadzam się" łącznie). Najwyższy poziom braku zgody odnotowano w Netii (53,8%), co może sugerować, że pracownicy tej organizacji mają mniejsze przekonanie o świadomości zagrożeń wśród współpracowników. Natomiast Orange odnotowało wyższy odsetek odpowiedzi pozytywnych, co może oznaczać większą pewność co do świadomości ryzyk w tej firmie.

Czy system szkolenia i profilaktyka są wystarczające w zakresie edukacji na temat zjawiska szpiegostwa korporacyjnego? Zdecydowana większość badanych nie zgadza się z tezą, że obecne działania edukacyjne są wystarczające. Najwyższy poziom braku zaufania do systemu szkoleniowego odnotowano w Netii (42,3%), co może sugerować, że system szkoleniowy w tej firmie jest postrzegany jako mniej efektywny. W Orange i Vectrze zauważono większą skłonność do odpowiedzi pozytywnych, co może sugerować lepszą ocenę systemów szkoleniowych w tych organizacjach.

Czy szkolenia prowadzone przez instytucje państwowe byłyby istotnym czynnikiem zwiększającym świadomość pracowników na temat szpiegostwa korporacyjnego? Większość respondentów wyraziła zgodę, że takie szkolenia miałyby istotny wpływ na świadomość pracowników, co jest szczególnie widoczne w wynikach dla Netii i Play (łącznie 45,9% i 47,8% odpowiedzi pozytywnych). W organizacjach takich jak Plus oraz T-Mobile odnotowano większy odsetek odpowiedzi neutralnych i negatywnych, co może sugerować mniejsze zapotrzebowanie na wsparcie instytucji państwowych w tych firmach.

Czy zjawisko szpiegostwa korporacyjnego powinno zostać zdefiniowane i uregulowane prawnie? Wysoki odsetek odpowiedzi pozytywnych („Zgadzam się" i „Zdecydowanie się zgadzam") we wszystkich firmach wskazuje na szerokie poparcie dla prawnej definicji

i regulacji tego zjawiska. Vectra wyróżnia się tutaj największym poparciem (łącznie 38,4% odpowiedzi pozytywnych), co sugeruje, że pracownicy tej organizacji dostrzegają potrzebę uregulowań prawnych bardziej niż w innych firmach.

Podsumowując, wyniki wskazują na różnice w postrzeganiu zagrożenia szpiegostwem korporacyjnym i skuteczności istniejących środków ochrony w zależności od miejsca zatrudnienia.

Tabela 19 Tabela krzyżowa ze statystykami n i % cech opisujących problematykę szpiegostwa kooperacyjnego wg. wieku badanej osoby. Hipoteza H4.2

		Wiek									
		do 30 lat		31-40 lat		41-50 lat		51-60 lat		powyżej 60 lat	
		N	%	N	%	N	%	N	%	N	%
Czy uważa Pani/Pan, że szpiegostwo korporacyjne stanowi zagrożenie dla przedsiębiorstwa, w którym jest Pani/Pan zatrudniona/y?	Zdecydowanie się nie zgadzam	17	18,7%	11	12,8%	17	20,2%	25	23,4%	14	14,4%
	Nie zgadzam się	20	22,0%	18	20,9%	21	25,0%	23	21,5%	24	24,7%
	Nie mam zdania	20	22,0%	16	18,6%	17	20,2%	14	13,1%	13	13,4%
	Zgadzam się	16	17,6%	24	27,9%	14	16,7%	28	26,2%	24	24,7%
	Zdecydowanie się zgadzam	18	19,8%	17	19,8%	15	17,9%	17	15,9%	22	22,7%
Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y podjęła odpowiednie środki w celu ochrony przed szpiegostwem korporacyjnym?	Zdecydowanie się nie zgadzam	16	17,6%	15	17,4%	19	22,6%	22	20,6%	17	17,5%
	Nie zgadzam się	21	23,1%	16	18,6%	19	22,6%	24	22,4%	20	20,6%
	Nie mam zdania	21	23,1%	16	18,6%	18	21,4%	23	21,5%	19	19,6%
	Zgadzam się	17	18,7%	13	15,1%	16	19,0%	20	18,7%	23	23,7%
	Zdecydowanie się zgadzam	16	17,6%	26	30,2%	12	14,3%	18	16,8%	18	18,6%
Czy uważa Pani/Pan, że regulacje i procedury w organizacji w której jest Pani/Pan zatrudniona/y są skuteczne w wykrywaniu i zapobieganiu zjawisku szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	18	19,8%	12	14,0%	11	13,1%	26	24,3%	18	18,6%
	Nie zgadzam się	22	24,2%	14	16,3%	21	25,0%	24	22,4%	13	13,4%
	Nie mam zdania	15	16,5%	23	26,7%	22	26,2%	24	22,4%	21	21,6%
	Zgadzam się	15	16,5%	22	25,6%	18	21,4%	15	14,0%	26	26,8%
	Zdecydowanie się zgadzam	21	23,1%	15	17,4%	12	14,3%	18	16,8%	19	19,6%

		Wiek									
		do 30 lat		31-40 lat		41-50 lat		51-60 lat		powyżej 60 lat	
		N	%	N	%	N	%	N	%	N	%
Czy uważa Pani/Pan, że przeprowadzanie kontroli przeszłości pracowników i dostawców może pomóc zmniejszyć ryzyko zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	27	29,7%	16	18,6%	14	16,7%	24	22,4%	15	15,5%
	Nie zgadzam się	18	19,8%	22	25,6%	18	21,4%	20	18,7%	20	20,6%
	Nie mam zdania	19	20,9%	19	22,1%	14	16,7%	24	22,4%	22	22,7%
	Zgadzam się	12	13,2%	12	14,0%	17	20,2%	16	15,0%	24	24,7%
	Zdecydowanie się zgadzam	15	16,5%	17	19,8%	21	25,0%	23	21,5%	16	16,5%
Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y, jest przygotowana do reagowania na podejrzewany lub potwierdzony incydent szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	26	28,6%	21	24,4%	13	15,5%	22	20,6%	19	19,6%
	Nie zgadzam się	16	17,6%	15	17,4%	13	15,5%	19	17,8%	18	18,6%
	Nie mam zdania	17	18,7%	19	22,1%	16	19,0%	21	19,6%	27	27,8%
	Zgadzam się	18	19,8%	22	25,6%	18	21,4%	21	19,6%	20	20,6%
	Zdecydowanie się zgadzam	14	15,4%	9	10,5%	24	28,6%	24	22,4%	13	13,4%
***Czy uważa Pani/Pan, że szkolenia i edukacja na temat szpiegostwa korporacyjnego są istotnym elementem dla pracowników i kontrahentów?**	Zdecydowanie się nie zgadzam	14	15,4%	25	29,1%	18	21,4%	18	16,8%	15	15,5%
	Nie zgadzam się	20	22,0%	18	20,9%	20	23,8%	18	16,8%	17	17,5%
	Nie mam zdania	21	23,1%	12	14,0%	7	8,3%	24	22,4%	18	18,6%
	Zgadzam się	29	31,9%	18	20,9%	15	17,9%	26	24,3%	20	20,6%
	Zdecydowanie się zgadzam	7	7,7%	13	15,1%	24	28,6%	21	19,6%	27	27,8%
Czy uważa Pani/Pan, że działania prawne są skutecznym środkiem odstraszającym w kontekście zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	23	25,3%	16	18,6%	19	22,6%	27	25,2%	17	17,5%
	Nie zgadzam się	19	20,9%	13	15,1%	12	14,3%	23	21,5%	16	16,5%
	Nie mam zdania	16	17,6%	15	17,4%	15	17,9%	23	21,5%	25	25,8%
	Zgadzam się	16	17,6%	21	24,4%	22	26,2%	17	15,9%	16	16,5%
	Zdecydowanie się zgadzam	17	18,7%	21	24,4%	16	19,0%	17	15,9%	23	23,7%
Czy uważa Pani/Pan, że szpiegostwo korporacyjne jest rosnącym problemem w	Zdecydowanie się nie zgadzam	24	26,4%	16	18,6%	15	17,9%	17	15,9%	18	18,6%
	Nie zgadzam się	14	15,4%	17	19,8%	19	22,6%	19	17,8%	24	24,7%
	Nie mam zdania	19	20,9%	19	22,1%	19	22,6%	31	29,0%	14	14,4%
	Zgadzam się	13	14,3%	15	17,4%	14	16,7%	21	19,6%	20	20,6%

		Wiek									
		do 30 lat		31-40 lat		41-50 lat		51-60 lat		powyżej 60 lat	
		N	%	N	%	N	%	N	%	N	%
sektorze technologii informacyjno-komunikacyjnych?	Zdecydowanie się zgadzam	21	23,1%	19	22,1%	17	20,2%	19	17,8%	21	21,6%
Czy uważa Pani/Pan, że środki bezpieczeństwa w organizacji, w której jest Pani/Pan zatrudniona/y, są wystarczające, aby chronić zarówno przed fizycznym, jak i cyfrowym zagrożeniom zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	23	25,3%	24	27,9%	16	19,0%	29	27,1%	14	14,4%
	Nie zgadzam się	18	19,8%	12	14,0%	14	16,7%	19	17,8%	23	23,7%
	Nie mam zdania	16	17,6%	24	27,9%	24	28,6%	21	19,6%	22	22,7%
	Zgadzam się	11	12,1%	15	17,4%	15	17,9%	21	19,6%	18	18,6%
	Zdecydowanie się zgadzam	23	25,3%	11	12,8%	15	17,9%	17	15,9%	20	20,6%
Czy uważa Pani/Pan, że pracownicy i kontrahenci organizacji, w której jest Pani/Pan zatrudniona/y, są świadomi oznak i ryzyka związanego ze szpiegostwem korporacyjnym?	Zdecydowanie się nie zgadzam	17	18,7%	18	20,9%	21	25,0%	17	15,9%	21	21,6%
	Nie zgadzam się	22	24,2%	15	17,4%	21	25,0%	32	29,9%	20	20,6%
	Nie mam zdania	19	20,9%	15	17,4%	14	16,7%	16	15,0%	18	18,6%
	Zgadzam się	18	19,8%	22	25,6%	13	15,5%	19	17,8%	21	21,6%
	Zdecydowanie się zgadzam	15	16,5%	16	18,6%	15	17,9%	23	21,5%	17	17,5%
Czy uważa Pani/Pan, że system szkolenia i profilaktyka prowadzona przez organizację, w której jest Pani/Pan zatrudniona/y, są wystarczające w kontekście edukowania i profilaktyki na temat zjawiska szpiegostwa korporcyjnego?	Zdecydowanie się nie zgadzam	13	14,3%	22	25,6%	18	21,4%	23	21,5%	20	20,6%
	Nie zgadzam się	21	23,1%	14	16,3%	18	21,4%	22	20,6%	15	15,5%
	Nie mam zdania	16	17,6%	17	19,8%	10	11,9%	18	16,8%	19	19,6%
	Zgadzam się	21	23,1%	15	17,4%	19	22,6%	24	22,4%	20	20,6%
	Zdecydowanie się zgadzam	20	22,0%	18	20,9%	19	22,6%	20	18,7%	23	23,7%

		Wiek									
		do 30 lat		31-40 lat		41-50 lat		51-60 lat		powyżej 60 lat	
		N	%	N	%	N	%	N	%	N	%
Czy uważa Pani/Pan, że szkolenia prowadzone przez instytucje państwowe (np. Agencję Bezpieczeństwa Wewnętrznego, Policję lub inne podmioty odpowiedzialne za bezpieczeństwo) byłyby istotnym czynnikiem zwiększającym świadomość pracowników i kontrahentów organizacji, w której jest Pani/Pan zatrudniona/y, na temat zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	23	25,3%	18	20,9%	11	13,1%	16	15,0%	23	23,7%
	Nie zgadzam się	19	20,9%	19	22,1%	19	22,6%	20	18,7%	23	23,7%
	Nie mam zdania	16	17,6%	19	22,1%	22	26,2%	19	17,8%	18	18,6%
	Zgadzam się	23	25,3%	16	18,6%	22	26,2%	27	25,2%	12	12,4%
	Zdecydowanie się zgadzam	10	11,0%	14	16,3%	10	11,9%	25	23,4%	21	21,6%
Czy uważa Pani/Pan, że zjawisko szpiegostwa korporacyjnego powinno zostać zdefiniowane i uregulowane prawne w celu skutecznego jemu przeciwdziałania przez organy państwowe?	Zdecydowanie się nie zgadzam	22	24,2%	28	32,6%	17	20,2%	25	23,4%	15	15,5%
	Nie zgadzam się	16	17,6%	16	18,6%	12	14,3%	17	15,9%	25	25,8%
	Nie mam zdania	17	18,7%	15	17,4%	16	19,0%	19	17,8%	15	15,5%
	Zgadzam się	18	19,8%	13	15,1%	19	22,6%	27	25,2%	23	23,7%
	Zdecydowanie się zgadzam	18	19,8%	14	16,3%	20	23,8%	19	17,8%	19	19,6%

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Interpretacja wyników z tabel nr 17 i 19

Na podstawie danych empirycznych w przypadku znaczenia szkoleń i edukacji w zakresie zagrożeń szpiegostwa nie ma podstaw do odrzucenia hipotezy H4.2. Istotnie

statystycznie ($p<0,05$) znaczenie szkoleń i edukacji w zakresie zagrożeń szpiegostwa jest doceniane zwłaszcza przez osoby w wieku do 30 lat (31,9% "zgadza się"). W grupie wiekowej 31–40 lat częściej pojawia się sprzeciw, co może wynikać z poczucia braku adekwatności dotychczasowych szkoleń. Ta zależność jest istotna statystycznie (tabela 19)

Reszta odpowiedzi (Tabela nr 19) przedstawia analizę opinii respondentów na temat zjawiska szpiegostwa korporacyjnego oraz skuteczności ochrony organizacyjnej, przeprowadzoną z uwzględnieniem wieku badanych, lecz jest nie istotna statystycznie. Odpowiedzi zostały podzielone na pięć kategorii wiekowych: do 30 lat, 31–40 lat, 41–50 lat, 51–60 lat oraz powyżej 60 lat, umożliwiając porównanie perspektyw osób z różnych grup wiekowych.

Czy szpiegostwo korporacyjne stanowi zagrożenie dla przedsiębiorstwa? Wśród osób do 30 lat najwięcej respondentów wyraziło brak jednoznacznej opinii lub zdecydowany sprzeciw. W grupie wiekowej 31–40 lat największa liczba odpowiedzi to "zgadzam się". W pozostałych grupach przeważają odpowiedzi negatywne, choć zbliżony odsetek osób powyżej 60 lat przyznaje, że problem istnieje.

Czy organizacja podjęła środki ochronne przed szpiegostwem? W każdej grupie wiekowej widoczne są podzielone opinie, lecz w grupie 31–40 lat największy odsetek stanowią osoby, które zdecydowanie zgadzają się z tym stwierdzeniem. Osoby w wieku 41–50 lat i 51–60 lat częściej wykazują się brakiem zgody lub jednoznacznego zdania.

Skuteczność regulacji i procedur w organizacji w wykrywaniu zjawiska jest bardziej pozytywnie oceniana przez grupę 31–40 lat, gdzie 25,6% odpowiedziało "zgadzam się". W grupie powyżej 60 lat przeważa jednak brak wyraźnej opinii lub sprzeciw wobec stwierdzenia o skuteczności.

Przeprowadzanie kontroli przeszłości pracowników jako środek prewencyjny uzyskało umiarkowaną aprobatę we wszystkich grupach wiekowych, z wyjątkiem najmłodszej grupy (do 30 lat), która częściej odrzuca tę strategię, co może wynikać z mniejszego doświadczenia zawodowego lub zaufania do procedur.

Gotowość organizacji do reagowania na incydenty szpiegostwa różni się w poszczególnych grupach. Osoby powyżej 60 lat oraz najmłodsza grupa wiekowa wyrażają bardziej sceptyczne nastawienie, natomiast grupa 31–40 lat najczęściej uznaje organizacje za przygotowane.

Skuteczność działań prawnych jako środka odstraszającego uzyskała pozytywne opinie, szczególnie w grupie 41–50 lat, gdzie 26,2% respondentów "zgadza się" ze stwierdzeniem, oraz w grupie 31–40 lat (24,4%).

Wzrost problemu szpiegostwa w sektorze technologii informacyjno-komunikacyjnych zauważają głównie osoby w wieku do 30 lat oraz powyżej 60 lat, co sugeruje wyższy poziom świadomości lub doświadczenia zawodowego w tych grupach.

Wystarczalność środków bezpieczeństwa organizacyjnego jest najczęściej kwestionowana przez osoby w wieku 51–60 lat, w których 27,1% "zdecydowanie się nie zgadza".

Świadomość pracowników i kontrahentów na temat szpiegostwa w organizacji jest podważana przez grupę 51–60 lat, w której 29,9% uważa, że pracownicy nie są świadomi zagrożenia.

System profilaktyki i edukacji na temat szpiegostwa w organizacji zdobył pozytywne opinie wśród osób do 30 lat i 41–50 lat, natomiast grupa 31–40 lat wyraziła największy brak zgody na jego skuteczność.

Szkolenia prowadzone przez instytucje państwowe zdobyły największe poparcie wśród osób powyżej 60 lat (23,4% "zdecydowanie się zgadzam").

Potrzeba prawnej regulacji zjawiska szpiegostwa korporacyjnego znajduje uznanie szczególnie w grupie 41–50 lat, gdzie 23,8% "zdecydowanie się zgadza" z tym stwierdzeniem.

W tabeli 20 przedstawiono statystyki krzyżowe dotyczące problematyki szpiegostwa kooperacyjnego wg. stażu pracy badanej osoby.

Tabela 20 Tabela krzyżowa ze statystykami n i % cech opisujących problematykę szpiegostwa kooperacyjnego wg. stażu pracy badanej osoby. Hipoteza H4.3

		Staż pracy									
		do 5 lat		6-10 lat		11-15 lat		16-20 lat		powyżej 20 lat	
		N	%	N	%	N	%	N	%	N	%
Czy uważa Pani/Pan, że szpiegostwo korporacyjne stanowi zagrożenie dla przedsiębiorstwa, w którym jest Pani/Pan zatrudniona/y?	Zdecydowanie się nie zgadzam	15	16,9%	18	19,6%	13	13,4%	21	26,6%	17	15,7%
	Nie zgadzam się	20	22,5%	24	26,1%	20	20,6%	14	17,7%	28	25,9%
	Nie mam zdania	17	19,1%	10	10,9%	21	21,6%	14	17,7%	18	16,7%
	Zgadzam się	20	22,5%	22	23,9%	24	24,7%	15	19,0%	25	23,1%
	Zdecydowanie się zgadzam	17	19,1%	18	19,6%	19	19,6%	15	19,0%	20	18,5%
Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y podjęła odpowiednie	Zdecydowanie się nie zgadzam	19	21,3%	10	10,9%	19	19,6%	17	21,5%	24	22,2%
	Nie zgadzam się	15	16,9%	20	21,7%	17	17,5%	18	22,8%	30	27,8%
	Nie mam zdania	20	22,5%	21	22,8%	23	23,7%	17	21,5%	16	14,8%
	Zgadzam się	13	14,6%	20	21,7%	22	22,7%	18	22,8%	16	14,8%

		Staż pracy									
		do 5 lat		6-10 lat		11-15 lat		16-20 lat		powyżej 20 lat	
		N	%	N	%	N	%	N	%	N	%
środki w celu ochrony przed szpiegostwem korporacyjnym?	Zdecydowanie się zgadzam	22	24,7%	21	22,8%	16	16,5%	9	11,4%	22	20,4%
Czy uważa Pani/Pan, że regulacje i procedury w organizacji w której jest Pani/Pan zatrudniona/y są skuteczne w wykrywaniu i zapobieganiu zjawisku szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	19	21,3%	16	17,4%	17	17,5%	14	17,7%	19	17,6%
	Nie zgadzam się	15	16,9%	24	26,1%	21	21,6%	13	16,5%	21	19,4%
	Nie mam zdania	20	22,5%	21	22,8%	24	24,7%	20	25,3%	20	18,5%
	Zgadzam się	14	15,7%	18	19,6%	20	20,6%	18	22,8%	26	24,1%
	Zdecydowanie się zgadzam	21	23,6%	13	14,1%	15	15,5%	14	17,7%	22	20,4%
Czy uważa Pani/Pan, że przeprowadzanie kontroli przeszłości pracowników i dostawców może pomóc zmniejszyć ryzyko zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	16	18,0%	19	20,7%	18	18,6%	19	24,1%	24	22,2%
	Nie zgadzam się	18	20,2%	23	25,0%	22	22,7%	14	17,7%	21	19,4%
	Nie mam zdania	21	23,6%	18	19,6%	15	15,5%	16	20,3%	28	25,9%
	Zgadzam się	18	20,2%	11	12,0%	18	18,6%	12	15,2%	22	20,4%
	Zdecydowanie się zgadzam	16	18,0%	21	22,8%	24	24,7%	18	22,8%	13	12,0%
Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y, jest przygotowana do reagowania na podejrzewany lub potwierdzony incydent szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	13	14,6%	20	21,7%	26	26,8%	17	21,5%	25	23,1%
	Nie zgadzam się	10	11,2%	14	15,2%	16	16,5%	14	17,7%	27	25,0%
	Nie mam zdania	22	24,7%	21	22,8%	17	17,5%	16	20,3%	24	22,2%
	Zgadzam się	24	27,0%	18	19,6%	25	25,8%	17	21,5%	15	13,9%
	Zdecydowanie się zgadzam	20	22,5%	19	20,7%	13	13,4%	15	19,0%	17	15,7%
Czy uważa Pani/Pan, że szkolenia i edukacja na temat szpiegostwa korporacyjnego są istotnym elementem	Zdecydowanie się nie zgadzam	11	12,4%	19	20,7%	21	21,6%	13	16,5%	26	24,1%
	Nie zgadzam się	21	23,6%	20	21,7%	14	14,4%	15	19,0%	23	21,3%
	Nie mam zdania	20	22,5%	14	15,2%	17	17,5%	14	17,7%	17	15,7%
	Zgadzam się	18	20,2%	25	27,2%	24	24,7%	19	24,1%	22	20,4%
	Zdecydowanie się zgadzam	19	21,3%	14	15,2%	21	21,6%	18	22,8%	20	18,5%

		Staż pracy									
		do 5 lat		6-10 lat		11-15 lat		16-20 lat		powyżej 20 lat	
		N	%	N	%	N	%	N	%	N	%
dla pracowników i kontrahentów?											
Czy uważa Pani/Pan, że działania prawne są skutecznym środkiem odstraszającym w kontekście zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	19	21,3%	21	22,8%	17	17,5%	21	26,6%	24	22,2%
	Nie zgadzam się	12	13,5%	15	16,3%	16	16,5%	14	17,7%	26	24,1%
	Nie mam zdania	22	24,7%	20	21,7%	20	20,6%	16	20,3%	16	14,8%
	Zgadzam się	20	22,5%	21	22,8%	17	17,5%	12	15,2%	22	20,4%
	Zdecydowanie się zgadzam	16	18,0%	15	16,3%	27	27,8%	16	20,3%	20	18,5%
Czy uważa Pani/Pan, że szpiegostwo korporacyjne jest rosnącym problemem w sektorze technologii informacyjno-komunikacyjnych?	Zdecydowanie się nie zgadzam	20	22,5%	13	14,1%	15	15,5%	18	22,8%	24	22,2%
	Nie zgadzam się	17	19,1%	19	20,7%	16	16,5%	17	21,5%	24	22,2%
	Nie mam zdania	21	23,6%	22	23,9%	16	16,5%	16	20,3%	27	25,0%
	Zgadzam się	16	18,0%	15	16,3%	20	20,6%	11	13,9%	21	19,4%
	Zdecydowanie się zgadzam	15	16,9%	23	25,0%	30	30,9%	17	21,5%	12	11,1%
Czy uważa Pani/Pan, że środki bezpieczeństwa w organizacji, w której jest Pani/Pan zatrudniona/y, są wystarczające, aby chronić zarówno przed fizycznym, jak i cyfrowym zagrożeniom zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	17	19,1%	20	21,7%	25	25,8%	12	15,2%	32	29,6%
	Nie zgadzam się	15	16,9%	15	16,3%	19	19,6%	13	16,5%	24	22,2%
	Nie mam zdania	22	24,7%	20	21,7%	25	25,8%	19	24,1%	21	19,4%
	Zgadzam się	17	19,1%	17	18,5%	11	11,3%	19	24,1%	16	14,8%
	Zdecydowanie się zgadzam	18	20,2%	20	21,7%	17	17,5%	16	20,3%	15	13,9%
Czy uważa Pani/Pan, że pracownicy i kontrahenci organizacji, w której jest Pani/Pan zatrudniona/y, są świadomi oznak i ryzyka związanego ze szpiegostwem korporacyjnym?	Zdecydowanie się nie zgadzam	16	18,0%	18	19,6%	26	26,8%	16	20,3%	18	16,7%
	Nie zgadzam się	21	23,6%	25	27,2%	26	26,8%	21	26,6%	17	15,7%
	Nie mam zdania	16	18,0%	21	22,8%	14	14,4%	9	11,4%	22	20,4%
	Zgadzam się	24	27,0%	12	13,0%	15	15,5%	18	22,8%	24	22,2%
	Zdecydowanie się zgadzam	12	13,5%	16	17,4%	16	16,5%	15	19,0%	27	25,0%

		Staż pracy									
		do 5 lat		6-10 lat		11-15 lat		16-20 lat		powyżej 20 lat	
		N	%	N	%	N	%	N	%	N	%
Czy uważa Pani/Pan, że system szkolenia i profilaktyka prowadzona przez organizację, w której jest Pani/Pan zatrudniona/y, są wystarczające w kontekście edukowania i profilaktyki na temat zjawiska szpiegostwa korporcyjnego?	Zdecydowanie się nie zgadzam	15	16,9%	23	25,0%	16	16,5%	18	22,8%	24	22,2%
	Nie zgadzam się	20	22,5%	21	22,8%	22	22,7%	12	15,2%	15	13,9%
	Nie mam zdania	12	13,5%	16	17,4%	22	22,7%	8	10,1%	22	20,4%
	Zgadzam się	21	23,6%	22	23,9%	19	19,6%	13	16,5%	24	22,2%
	Zdecydowanie się zgadzam	21	23,6%	10	10,9%	18	18,6%	28	35,4%	23	21,3%
Czy uważa Pani/Pan, że szkolenia prowadzone przez instytucje państwowe (np. Agencję Bezpieczeństwa Wewnętrznego, Policję lub inne podmioty odpowiedzialne za bezpieczeństwo) byłyby istotnym czynnikiem zwiększającym świadomość pracowników i kontrahentów organizacji, w której jest Pani/Pan zatrudniona/y, na temat zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	15	16,9%	23	25,0%	24	24,7%	8	10,1%	21	19,4%
	Nie zgadzam się	23	25,8%	14	15,2%	24	24,7%	16	20,3%	23	21,3%
	Nie mam zdania	19	21,3%	14	15,2%	21	21,6%	17	21,5%	23	21,3%
	Zgadzam się	16	18,0%	22	23,9%	14	14,4%	24	30,4%	24	22,2%
	Zdecydowanie się zgadzam	16	18,0%	19	20,7%	14	14,4%	14	17,7%	17	15,7%
Czy uważa Pani/Pan, że zjawisko szpiegostwa korporacyjnego	Zdecydowanie się nie zgadzam	15	16,9%	24	26,1%	27	27,8%	13	16,5%	28	25,9%
	Nie zgadzam się	19	21,3%	14	15,2%	19	19,6%	11	13,9%	23	21,3%
	Nie mam zdania	15	16,9%	20	21,7%	14	14,4%	17	21,5%	16	14,8%

		Staż pracy									
		do 5 lat		6-10 lat		11-15 lat		16-20 lat		powyżej 20 lat	
		N	%	N	%	N	%	N	%	N	%
powinno zostać zdefiniowane i uregulowane prawne w celu skutecznego jemu przeciwdziałania przez organy państwowe?	Zgadzam się	18	20,2%	21	22,8%	18	18,6%	20	25,3%	23	21,3%
	Zdecydowanie się zgadzam	22	24,7%	13	14,1%	19	19,6%	18	22,8%	18	16,7%

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Interpretacja wyników z tabel nr 17 i 20

Tabela nr 20 przedstawia zestawienie odpowiedzi respondentów na pytania dotyczące problematyki szpiegostwa korporacyjnego, z uwzględnieniem ich stażu pracy. Analizowane pytania skupiają się na ocenach zagrożeń, postrzeganiu działań prewencyjnych organizacji, efektywności szkoleń, znaczeniu procedur ochronnych, a także potrzebie prawnych regulacji. Każde pytanie jest analizowane osobno, a odpowiedzi są rozdzielone na pięć kategorii stażu pracy: do 5 lat, 6-10 lat, 11-15 lat, 16-20 lat oraz powyżej 20 lat. W każdej kategorii stażu pracy przedstawiono liczbę respondentów (N) i procentowy udział (%) w stosunku do ogólnej liczby odpowiedzi w tej kategorii. Na podstawie danych empirycznych nie ma podstaw do przyjęcia hipotezy H4.3. Zatem postrzeganie problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych nie zależy od stażu pracy. Można jednak zauważyć pewne tendencje, które opisano poniżej.

Postrzeganie zagrożenia: Większy staż pracy zdaje się wpływać na wzrost liczby odpowiedzi „Zdecydowanie się zgadzam" co do istnienia zagrożenia szpiegostwa korporacyjnego (np. 19,6% w kategorii 11-15 lat i 18,5% dla powyżej 20 lat). Respondenci z krótszym stażem wykazują większą niepewność lub skłonność do zaprzeczenia zagrożeniu.

Ochrona przed szpiegostwem korporacyjnym: Odpowiedzi w zakresie ochrony organizacji przed szpiegostwem wskazują, że pracownicy z dłuższym stażem (powyżej 20 lat) częściej wyrażają brak zgody na adekwatność działań prewencyjnych (27,8% w grupie „Nie zgadzam się").

Skuteczność procedur: Osoby ze stażem 6-10 lat i 16-20 lat częściej wykazują sceptycyzm wobec skuteczności regulacji i procedur w zakresie wykrywania szpiegostwa (26,1% i 16,5% dla odpowiedzi „Nie zgadzam się").

Rola kontroli przeszłości pracowników: Odpowiedzi pokazują, że osoby z dłuższym stażem są bardziej przekonane o znaczeniu kontroli jako sposobu przeciwdziałania szpiegostwu (24,7% odpowiedzi „Zdecydowanie się zgadzam" dla grupy 11-15 lat).

Gotowość organizacji do reakcji: Osoby z krótszym stażem (do 5 lat) częściej zgadzają się, że ich organizacja jest gotowa na reakcję w przypadku incydentu (27,0% dla „Zgadzam się").

Znaczenie szkoleń i edukacji: Pracownicy z większym stażem (powyżej 20 lat) wykazują wyższy poziom zgody na konieczność edukacji o szpiegostwie (21,3% dla „Nie zgadzam się", przy czym odpowiedź „Zdecydowanie się zgadzam" osiągnęła maksimum 24,1% w tej grupie).

Ocena środków prawnych: Wśród respondentów, dłuższy staż pracy (powyżej 20 lat) sprzyja bardziej zdecydowanej zgodzie z opinią, że środki prawne są skuteczne w odstraszaniu (18,5% w odpowiedzi „Zdecydowanie się zgadzam").

Wzrost problemu w sektorze technologii informacyjno-komunikacyjnych: Pracownicy z mniejszym doświadczeniem (do 5 lat) oraz stażem powyżej 20 lat częściej nie zgadzają się z tezą, że problem narasta (22,5% i 22,2%).

Bezpieczeństwo fizyczne i cyfrowe: Grupa z najdłuższym stażem (powyżej 20 lat) ma najwyższy odsetek odpowiedzi „Zdecydowanie się nie zgadzam" co do wystarczalności środków bezpieczeństwa (29,6%).

Świadomość pracowników i kontrahentów: Pracownicy z różnym stażem w zbliżonym stopniu oceniają świadomość swoich współpracowników, przy czym grupa z krótszym stażem wyraża wyższe wskaźniki dla zgody, że są świadomi (27,0%).

Skuteczność działań profilaktycznych i szkoleń: Pracownicy z większym stażem (powyżej 20 lat) częściej deklarują pozytywne opinie na temat działań profilaktycznych (35,4% dla „Zdecydowanie się zgadzam").

Szkolenia państwowe: Pracownicy o krótszym stażu (do 5 lat) częściej wyrażają neutralność lub brak zdania w tej kwestii (np. 21,3% dla „Nie mam zdania" w grupie do 5 lat).

Regulacje prawne przeciwdziałające szpiegostwu: Najwięcej odpowiedzi „Zdecydowanie się zgadzam" na potrzebę formalnych regulacji występuje w grupie osób ze stażem do 5 lat (24,7%).

Tabela nr 21 daje wgląd w postawy i przekonania respondentów na temat problematyki szpiegostwa korporacyjnego, pokazując zróżnicowane podejścia w zależności od doświadczenia zawodowego, co może być kluczowe przy opracowywaniu działań prewencyjnych i edukacyjnych w organizacjach.

Tabela 21 Tabela krzyżowa ze statystykami n i % cech opisujących problematykę szpiegostwa kooperacyjnego wg. poziomu wykształcenia badanej osoby. Hipoteza H4.4

		Wykształcenie									
		Podstawowe i zawodowe		Średnie		Studia I stopnia		Studia II stopnia		Studia III stopnia	
		N	%	N	%	N	%	N	%	N	%
Czy uważa Pani/Pan, że szpiegostwo korporacyjne stanowi zagrożenie dla przedsiębiorstwa, w którym jest Pani/Pan zatrudniona/y?	Zdecydowanie się nie zgadzam	12	20,7%	12	11,4%	31	22,0%	27	21,3%	2	5,9%
	Nie zgadzam się	16	27,6%	27	25,7%	30	21,3%	23	18,1%	10	29,4%
	Nie mam zdania	12	20,7%	16	15,2%	23	16,3%	22	17,3%	7	20,6%
	Zgadzam się	11	19,0%	31	29,5%	31	22,0%	26	20,5%	7	20,6%
	Zdecydowanie się zgadzam	7	12,1%	19	18,1%	26	18,4%	29	22,8%	8	23,5%
Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y podjęła odpowiednie środki w celu ochrony przed szpiegostwem korporacyjnym?	Zdecydowanie się nie zgadzam	9	15,5%	20	19,0%	28	19,9%	25	19,7%	7	20,6%
	Nie zgadzam się	10	17,2%	22	21,0%	29	20,6%	29	22,8%	10	29,4%
	Nie mam zdania	14	24,1%	21	20,0%	28	19,9%	30	23,6%	4	11,8%
	Zgadzam się	15	25,9%	23	21,9%	30	21,3%	20	15,7%	1	2,9%
	Zdecydowanie się zgadzam	10	17,2%	19	18,1%	26	18,4%	23	18,1%	12	35,3%
Czy uważa Pani/Pan, że regulacje i procedury w organizacji, w której jest Pani/Pan zatrudniona/y są skuteczne w wykrywaniu i zapobieganiu zjawisku szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	3	5,2%	14	13,3%	30	21,3%	35	27,6%	3	8,8%
	Nie zgadzam się	14	24,1%	23	21,9%	29	20,6%	21	16,5%	7	20,6%
	Nie mam zdania	13	22,4%	26	24,8%	26	18,4%	31	24,4%	9	26,5%
	Zgadzam się	16	27,6%	22	21,0%	31	22,0%	20	15,7%	7	20,6%
	Zdecydowanie się zgadzam	12	20,7%	20	19,0%	25	17,7%	20	15,7%	8	23,5%
Czy uważa Pani/Pan, że przeprowadzanie kontroli przeszłości	Zdecydowanie się nie zgadzam	18	31,0%	23	21,9%	19	13,5%	28	22,0%	8	23,5%
	Nie zgadzam się	8	13,8%	24	22,9%	28	19,9%	30	23,6%	8	23,5%
	Nie mam zdania	11	19,0%	21	20,0%	34	24,1%	26	20,5%	6	17,6%
	Zgadzam się	11	19,0%	12	11,4%	30	21,3%	24	18,9%	4	11,8%

		Wykształcenie									
		Podstawowe i zawodowe		Średnie		Studia I stopnia		Studia II stopnia		Studia III stopnia	
		N	%	N	%	N	%	N	%	N	%
pracowników i dostawców może pomóc zmniejszyć ryzyko zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się zgadzam	10	17,2%	25	23,8%	30	21,3%	19	15,0%	8	23,5%
Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y, jest przygotowana do reagowania na podejrzewany lub potwierdzony incydent szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	13	22,4%	21	20,0%	34	24,1%	23	18,1%	10	29,4%
	Nie zgadzam się	14	24,1%	15	14,3%	22	15,6%	24	18,9%	6	17,6%
	Nie mam zdania	12	20,7%	18	17,1%	32	22,7%	28	22,0%	10	29,4%
	Zgadzam się	10	17,2%	27	25,7%	26	18,4%	32	25,2%	4	11,8%
	Zdecydowanie się zgadzam	9	15,5%	24	22,9%	27	19,1%	20	15,7%	4	11,8%
Czy uważa Pani/Pan, że szkolenia i edukacja na temat szpiegostwa korporacyjnego są istotnym elementem dla pracowników i kontrahentów?	Zdecydowanie się nie zgadzam	10	17,2%	19	18,1%	26	18,4%	28	22,0%	7	20,6%
	Nie zgadzam się	17	29,3%	12	11,4%	25	17,7%	31	24,4%	8	23,5%
	Nie mam zdania	8	13,8%	14	13,3%	33	23,4%	21	16,5%	6	17,6%
	Zgadzam się	10	17,2%	38	36,2%	30	21,3%	23	18,1%	7	20,6%
	Zdecydowanie się zgadzam	13	22,4%	22	21,0%	27	19,1%	24	18,9%	6	17,6%
Czy uważa Pani/Pan, że działania prawne są skutecznym środkiem odstraszającym w kontekście zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	17	29,3%	18	17,1%	41	29,1%	19	15,0%	7	20,6%
	Nie zgadzam się	8	13,8%	20	19,0%	24	17,0%	27	21,3%	4	11,8%
	Nie mam zdania	11	19,0%	24	22,9%	23	16,3%	26	20,5%	10	29,4%
	Zgadzam się	10	17,2%	25	23,8%	22	15,6%	29	22,8%	6	17,6%
	Zdecydowanie się zgadzam	12	20,7%	18	17,1%	31	22,0%	26	20,5%	7	20,6%
Czy uważa Pani/Pan, że szpiegostwo korporacyjne jest	Zdecydowanie się nie zgadzam	12	20,7%	18	17,1%	24	17,0%	28	22,0%	8	23,5%
	Nie zgadzam się	13	22,4%	21	20,0%	25	17,7%	24	18,9%	10	29,4%
	Nie mam zdania	11	19,0%	20	19,0%	34	24,1%	32	25,2%	5	14,7%

		Wykształcenie									
		Podstawowe i zawodowe		Średnie		Studia I stopnia		Studia II stopnia		Studia III stopnia	
		N	%	N	%	N	%	N	%	N	%
rosnącym problemem w sektorze technologii informacyjno-komunikacyjnych?	Zgadzam się	8	13,8%	19	18,1%	28	19,9%	22	17,3%	6	17,6%
	Zdecydowanie się zgadzam	14	24,1%	27	25,7%	30	21,3%	21	16,5%	5	14,7%
***Czy uważa Pani/Pan, że środki bezpieczeństwa w organizacji, w której jest Pani/Pan zatrudniona/y, są wystarczające, aby chronić zarówno przed fizycznym, jak i cyfrowym zagrożeniom zjawiska szpiegostwa korporacyjnego?**	Zdecydowanie się nie zgadzam	23	39,7%	21	20,0%	26	18,4%	29	22,8%	7	20,6%
	Nie zgadzam się	9	15,5%	20	19,0%	23	16,3%	31	24,4%	3	8,8%
	Nie mam zdania	14	24,1%	20	19,0%	44	31,2%	21	16,5%	8	23,5%
	Zgadzam się	4	6,9%	19	18,1%	26	18,4%	23	18,1%	8	23,5%
	Zdecydowanie się zgadzam	8	13,8%	25	23,8%	22	15,6%	23	18,1%	8	23,5%
Czy uważa Pani/Pan, że pracownicy i kontrahenci organizacji, w której jest Pani/Pan zatrudniona/y, są świadomi oznak i ryzyka związanego ze szpiegostwem korporacyjnym?	Zdecydowanie się nie zgadzam	13	22,4%	17	16,2%	32	22,7%	25	19,7%	7	20,6%
	Nie zgadzam się	9	15,5%	31	29,5%	28	19,9%	39	30,7%	3	8,8%
	Nie mam zdania	10	17,2%	18	17,1%	26	18,4%	20	15,7%	8	23,5%
	Zgadzam się	12	20,7%	18	17,1%	31	22,0%	26	20,5%	6	17,6%
	Zdecydowanie się zgadzam	14	24,1%	21	20,0%	24	17,0%	17	13,4%	10	29,4%
Czy uważa Pani/Pan, że system szkolenia i profilaktyka prowadzona przez organizację, w której jest Pani/Pan zatrudniona/y, są	Zdecydowanie się nie zgadzam	15	25,9%	24	22,9%	26	18,4%	25	19,7%	6	17,6%
	Nie zgadzam się	10	17,2%	22	21,0%	30	21,3%	20	15,7%	8	23,5%
	Nie mam zdania	10	17,2%	19	18,1%	27	19,1%	21	16,5%	3	8,8%
	Zgadzam się	10	17,2%	24	22,9%	26	18,4%	28	22,0%	11	32,4%
	Zdecydowanie się zgadzam	13	22,4%	16	15,2%	32	22,7%	33	26,0%	6	17,6%

		Wykształcenie									
		Podstawowe i zawodowe		Średnie		Studia I stopnia		Studia II stopnia		Studia III stopnia	
		N	%	N	%	N	%	N	%	N	%
wystarczające w kontekście edukowania i profilaktyki na temat zjawiska szpiegostwa korporcyjnego?											
Czy uważa Pani/Pan, że szkolenia prowadzone przez instytucje państwowe (np. Agencję Bezpieczeństwa Wewnętrznego, Policję lub inne podmioty odpowiedzialne za bezpieczeństwo) byłyby istotnym czynnikiem zwiększającym świadomość pracowników i kontrahentów organizacji, w której jest Pani/Pan zatrudniona/y, na temat zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	11	19,0%	22	21,0%	30	21,3%	20	15,7%	8	23,5%
	Nie zgadzam się	11	19,0%	19	18,1%	33	23,4%	30	23,6%	7	20,6%
	Nie mam zdania	13	22,4%	20	19,0%	31	22,0%	22	17,3%	8	23,5%
	Zgadzam się	13	22,4%	23	21,9%	22	15,6%	34	26,8%	8	23,5%
	Zdecydowanie się zgadzam	10	17,2%	21	20,0%	25	17,7%	21	16,5%	3	8,8%
Czy uważa Pani/Pan, że zjawisko szpiegostwa korporacyjnego powinno zostać zdefiniowane i uregulowane prawne w celu skutecznego jemu	Zdecydowanie się nie zgadzam	11	19,0%	27	25,7%	26	18,4%	35	27,6%	8	23,5%
	Nie zgadzam się	12	20,7%	24	22,9%	27	19,1%	15	11,8%	8	23,5%
	Nie mam zdania	9	15,5%	18	17,1%	31	22,0%	21	16,5%	3	8,8%
	Zgadzam się	15	25,9%	17	16,2%	30	21,3%	30	23,6%	8	23,5%
	Zdecydowanie się zgadzam	11	19,0%	19	18,1%	27	19,1%	26	20,5%	7	20,6%

		Wykształcenie									
		Podstawowe i zawodowe		Średnie		Studia I stopnia		Studia II stopnia		Studia III stopnia	
		N	%	N	%	N	%	N	%	N	%
przeciwdziałania przez organy państwowe?											

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Interpretacja wyników z tabel 17 i 21

Na podstawie testu chi-kwadrat nie ma podstaw do odrzucenia hipotezy H4.4. Istotnie statystycznie ($p<0,01$ – tebela 17) ocena wystarczalności zabezpieczeń fizycznych i cyfrowych zależy od wykształcenia badanych osób. W grupie z wykształceniem podstawowym i zawodowym, największy odsetek (39,7%) zdecydowanie nie zgadza się, że zabezpieczenia są wystarczające, podczas gdy osoby z wykształceniem III stopnia wyrażają mniejsze wątpliwości.

Tabela nr 21 prezentuje zestawienie opinii respondentów dotyczących różnych aspektów szpiegostwa korporacyjnego w zależności od poziomu wykształcenia. Poniżej przedstawiono najważniejsze obserwacje, które można traktować jako pewne zauważalne tendencje.

Postrzeganie szpiegostwa korporacyjnego jako zagrożenia:

- W grupie osób z wykształceniem podstawowym i zawodowym 20,7% zdecydowanie nie zgadza się z opinią, że szpiegostwo korporacyjne stanowi zagrożenie, a 27,6% po prostu nie zgadza się.W grupie z wykształceniem III stopnia, najwięcej osób (29,4%) zdecydowanie nie zgadza się, ale równocześnie 23,5% w pełni zgadza się z tym stwierdzeniem.

Ocena podjętych przez organizację środków ochronnych:

- W grupie z wykształceniem podstawowym i zawodowym, 25,9% zgadza się, że organizacja podjęła odpowiednie środki bezpieczeństwa, podczas gdy 17,2% w pełni zgadza się z tym stwierdzeniem. Z wykształceniem III stopnia, zauważalna jest różnorodność opinii, a jedynie 2,9% respondentów zgadza się z twierdzeniem.

Skuteczność regulacji w wykrywaniu szpiegostwa:

- Spośród osób z wykształceniem II stopnia, aż 27,6% zdecydowanie nie zgadza się, że regulacje są skuteczne, podczas gdy tylko 15,7% zgadza się z tym stwierdzeniem. W grupie z wykształceniem średnim, największy odsetek respondentów (24,8%) wyraził brak zdania.

Wpływ kontroli przeszłości na zmniejszenie ryzyka:

- W grupie z wykształceniem podstawowym i zawodowym, 31,0% respondentów zdecydowanie nie zgadza się z opinią, że kontrola przeszłości może zmniejszyć ryzyko, co jest najwyższym wynikiem w tej kategorii.

Przygotowanie organizacji do reagowania na incydenty szpiegostwa:

- Osoby z wykształceniem średnim w 25,7% zgadzają się, że organizacja jest odpowiednio przygotowana do reagowania na podejrzenia o szpiegostwo,
- Osoby z wykształceniem III stopnia wydają się mieć wyższy poziom sceptycyzmu, co odzwierciedla się w 29,4% odpowiedzi "zdecydowanie się nie zgadzam".

Znaczenie szkoleń w zakresie świadomości szpiegostwa:

- Dla osób z wykształceniem średnim 36,2% respondentów zgadza się, że szkolenia na temat szpiegostwa korporacyjnego są istotne dla pracowników, natomiast w grupie z wykształceniem III stopnia odsetek ten wynosi 20,6%.

Skuteczność działań prawnych jako środka odstraszającego:

- Dla osób z wykształceniem podstawowym i zawodowym 29,3% respondentów zdecydowanie się nie zgadza z opinią, że działania prawne skutecznie odstraszają przed szpiegostwem, co jest najwyższym wynikiem w tej kategorii,
- Z kolei 20,6% osób z wykształceniem III stopnia zdecydowanie zgadza się z tą opinią.

Świadomość pracowników o zagrożeniu ze strony szpiegostwa:

- W grupie z wykształceniem II stopnia 30,7% respondentów nie zgadza się, że pracownicy i kontrahenci są świadomi zagrożeń, a w grupie z wykształceniem średnim najwyższy odsetek (29,5%) wyraża brak zdania.

Ocena wystarczalności szkoleń i profilaktyki:

- Wśród osób z wykształceniem III stopnia, najwyższy odsetek (32,4%) wyraża zgodę, że szkolenia są odpowiednie, natomiast osoby z niższym poziomem wykształcenia wykazują większy sceptycyzm.

Znaczenie szkoleń instytucji państwowych dla wzrostu świadomości o szpiegostwie:

- Dla osób z wykształceniem podstawowym i zawodowym 22,4% respondentów wyraziło zdanie, że szkolenia państwowe byłyby istotne dla wzrostu świadomości, podobny wynik odnotowano dla osób z wykształceniem średnim.

Zapotrzebowanie na prawne regulacje przeciwdziałające szpiegostwu:

- Największy odsetek osób (27,6%) z wykształceniem II stopnia wyraził zdecydowaną potrzebę wprowadzenia regulacji prawnych przeciwdziałających szpiegostwu, przy

czym grupa z wykształceniem podstawowym i zawodowym również w większości zgadza się z tym stwierdzeniem.

Tabela nr 21 przedstawia istotne różnice w ocenie zagrożeń i odpowiednich działań związanych ze szpiegostwem korporacyjnym, szczególnie w odniesieniu do stopnia wykształcenia respondentów.

W tabeli 22 przedstawiono statystyki dotyczące postrzegania problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych w zależności od zajmowanego stanowiska służbowego.

Tabela 22 Tabela krzyżowa ze statystykami n i % cech opisujących problematykę szpiegostwa kooperacyjnego wg. stanowiska w pracy badanej osoby. Hipoteza H4.5

		Stanowisko pracy									
		Pracownik biurowy		Asystent		Specjalista		Kierownictwo wyższego szczebla (dyrektor)		Kierownictwo 3go szczebla (manager)	
		N	%	N	%	N	%	N	%	N	%
Czy uważa Pani/Pan, że szpiegostwo korporacyjne stanowi zagrożenie dla przedsiębiorstwa, w którym jest Pani/Pan zatrudniona/y?	Zdecydowanie się nie zgadzam	11	12,8%	20	18,9%	19	18,1%	20	23,3%	14	17,1%
	Nie zgadzam się	22	25,6%	30	28,3%	22	21,0%	15	17,4%	17	20,7%
	Nie mam zdania	19	22,1%	14	13,2%	24	22,9%	15	17,4%	8	9,8%
	Zgadzam się	22	25,6%	25	23,6%	24	22,9%	15	17,4%	20	24,4%
	Zdecydowanie się zgadzam	12	14,0%	17	16,0%	16	15,2%	21	24,4%	23	28,0%
Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y podjęła odpowiednie środki w celu ochrony przed szpiegostwem korporacyjnym?	Zdecydowanie się nie zgadzam	17	19,8%	25	23,6%	19	18,1%	17	19,8%	11	13,4%
	Nie zgadzam się	16	18,6%	22	20,8%	24	22,9%	21	24,4%	17	20,7%
	Nie mam zdania	14	16,3%	23	21,7%	20	19,0%	18	20,9%	22	26,8%
	Zgadzam się	24	27,9%	20	18,9%	15	14,3%	11	12,8%	19	23,2%
	Zdecydowanie się zgadzam	15	17,4%	16	15,1%	27	25,7%	19	22,1%	13	15,9%
Czy uważa Pani/Pan, że regulacje i	Zdecydowanie się nie zgadzam	15	17,4%	10	9,4%	24	22,9%	22	25,6%	14	17,1%

		Stanowisko pracy									
		Pracownik biurowy		Asystent		Specjalista		Kierownictwo wyższego szczebla (dyrektor)		Kierownictwo 3go szczebla (manager)	
		N	%	N	%	N	%	N	%	N	%
procedury w organizacji, w której jest Pani/Pan zatrudniona/y są skuteczne w wykrywaniu i zapobieganiu zjawisku szpiegostwa korporacyjnego?	Nie zgadzam się	23	26,7%	21	19,8%	21	20,0%	13	15,1%	16	19,5%
	Nie mam zdania	12	14,0%	26	24,5%	26	24,8%	20	23,3%	21	25,6%
	Zgadzam się	20	23,3%	27	25,5%	17	16,2%	16	18,6%	16	19,5%
	Zdecydowanie się zgadzam	16	18,6%	22	20,8%	17	16,2%	15	17,4%	15	18,3%
Czy uważa Pani/Pan, że przeprowadzanie kontroli przeszłości pracowników i dostawców może pomóc zmniejszyć ryzyko zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	18	20,9%	26	24,5%	23	21,9%	14	16,3%	15	18,3%
	Nie zgadzam się	17	19,8%	21	19,8%	20	19,0%	22	25,6%	18	22,0%
	Nie mam zdania	17	19,8%	23	21,7%	18	17,1%	22	25,6%	18	22,0%
	Zgadzam się	15	17,4%	18	17,0%	20	19,0%	15	17,4%	13	15,9%
	Zdecydowanie się zgadzam	19	22,1%	18	17,0%	24	22,9%	13	15,1%	18	22,0%
Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y, jest przygotowana do reagowania na podejrzewany lub potwierdzony incydent szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	19	22,1%	25	23,6%	24	22,9%	14	16,3%	19	23,2%
	Nie zgadzam się	19	22,1%	15	14,2%	18	17,1%	16	18,6%	13	15,9%
	Nie mam zdania	15	17,4%	26	24,5%	26	24,8%	19	22,1%	14	17,1%
	Zgadzam się	18	20,9%	20	18,9%	23	21,9%	20	23,3%	18	22,0%
	Zdecydowanie się zgadzam	15	17,4%	20	18,9%	14	13,3%	17	19,8%	18	22,0%
Czy uważa Pani/Pan, że szkolenia i edukacja na temat szpiegostwa korporacyjnego są istotnym	Zdecydowanie się nie zgadzam	11	12,8%	17	16,0%	25	23,8%	19	22,1%	18	22,0%
	Nie zgadzam się	12	14,0%	25	23,6%	19	18,1%	20	23,3%	17	20,7%
	Nie mam zdania	16	18,6%	16	15,1%	18	17,1%	19	22,1%	13	15,9%

		Stanowisko pracy									
		Pracownik biurowy		Asystent		Specjalista		Kierownictwo wyższego szczebla (dyrektor)		Kierownictwo 3go szczebla (manager)	
		N	%	N	%	N	%	N	%	N	%
elementem dla pracowników i kontrahentów?	Zgadzam się	26	30,2%	26	24,5%	25	23,8%	13	15,1%	18	22,0%
	Zdecydowanie się zgadzam	21	24,4%	22	20,8%	18	17,1%	15	17,4%	16	19,5%
Czy uważa Pani/Pan, że działania prawne są skutecznym środkiem odstraszającym w kontekście zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	21	24,4%	27	25,5%	20	19,0%	13	15,1%	21	25,6%
	Nie zgadzam się	9	10,5%	21	19,8%	20	19,0%	15	17,4%	18	22,0%
	Nie mam zdania	17	19,8%	18	17,0%	17	16,2%	25	29,1%	17	20,7%
	Zgadzam się	20	23,3%	17	16,0%	25	23,8%	17	19,8%	13	15,9%
	Zdecydowanie się zgadzam	19	22,1%	23	21,7%	23	21,9%	16	18,6%	13	15,9%
Czy uważa Pani/Pan, że szpiegostwo korporacyjne jest rosnącym problemem w sektorze technologii informacyjno-komunikacyjnych?	Zdecydowanie się nie zgadzam	12	14,0%	23	21,7%	19	18,1%	22	25,6%	14	17,1%
	Nie zgadzam się	19	22,1%	21	19,8%	19	18,1%	17	19,8%	17	20,7%
	Nie mam zdania	22	25,6%	19	17,9%	26	24,8%	18	20,9%	17	20,7%
	Zgadzam się	13	15,1%	19	17,9%	22	21,0%	14	16,3%	15	18,3%
	Zdecydowanie się zgadzam	20	23,3%	24	22,6%	19	18,1%	15	17,4%	19	23,2%
Czy uważa Pani/Pan, że środki bezpieczeństwa w organizacji, w której jest Pani/Pan zatrudniona/y, są wystarczające, aby chronić zarówno przed fizycznym, jak i cyfrowym zagrożeniom zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	24	27,9%	24	22,6%	22	21,0%	18	20,9%	18	22,0%
	Nie zgadzam się	15	17,4%	15	14,2%	22	21,0%	18	20,9%	16	19,5%
	Nie mam zdania	17	19,8%	33	31,1%	23	21,9%	14	16,3%	20	24,4%
	Zgadzam się	16	18,6%	13	12,3%	22	21,0%	17	19,8%	12	14,6%
	Zdecydowanie się zgadzam	14	16,3%	21	19,8%	16	15,2%	19	22,1%	16	19,5%

		Stanowisko pracy									
		Pracownik biurowy		Asystent		Specjalista		Kierownictwo wyższego szczebla (dyrektor)		Kierownictwo 3go szczebla (manager)	
		N	%	N	%	N	%	N	%	N	%
Czy uważa Pani/Pan, że pracownicy i kontrahenci organizacji, w której jest Pani/Pan zatrudniona/y, są świadomi oznak i ryzyka związanego ze szpiegostwem korporacyjnym?	Zdecydowanie się nie zgadzam	18	20,9%	19	17,9%	27	25,7%	17	19,8%	13	15,9%
	Nie zgadzam się	14	16,3%	25	23,6%	22	21,0%	24	27,9%	25	30,5%
	Nie mam zdania	17	19,8%	24	22,6%	13	12,4%	14	16,3%	14	17,1%
	Zgadzam się	18	20,9%	19	17,9%	25	23,8%	16	18,6%	15	18,3%
	Zdecydowanie się zgadzam	19	22,1%	19	17,9%	18	17,1%	15	17,4%	15	18,3%
Czy uważa Pani/Pan, że system szkolenia i profilaktyka prowadzona przez organizację, w której jest Pani/Pan zatrudniona/y, są wystarczające w kontekście edukowania i profilaktyki na temat zjawiska szpiegostwa korporacyjnego?	Zdecydowanie się nie zgadzam	20	23,3%	22	20,8%	22	21,0%	17	19,8%	15	18,3%
	Nie zgadzam się	21	24,4%	18	17,0%	24	22,9%	15	17,4%	12	14,6%
	Nie mam zdania	13	15,1%	19	17,9%	13	12,4%	17	19,8%	18	22,0%
	Zgadzam się	11	12,8%	28	26,4%	20	19,0%	21	24,4%	19	23,2%
	Zdecydowanie się zgadzam	21	24,4%	19	17,9%	26	24,8%	16	18,6%	18	22,0%
Czy uważa Pani/Pan, że szkolenia prowadzone przez instytucje państwowe (np. Agencję Bezpieczeństwa Wewnętrznego, Policję lub inne podmioty odpowiedzialne za bezpieczeństwo) byłyby istotnym	Zdecydowanie się nie zgadzam	20	23,3%	15	14,2%	21	20,0%	12	14,0%	23	28,0%
	Nie zgadzam się	18	20,9%	26	24,5%	18	17,1%	24	27,9%	14	17,1%
	Nie mam zdania	16	18,6%	24	22,6%	23	21,9%	14	16,3%	17	20,7%
	Zgadzam się	17	19,8%	18	17,0%	26	24,8%	22	25,6%	17	20,7%
	Zdecydowanie się zgadzam	15	17,4%	23	21,7%	17	16,2%	14	16,3%	11	13,4%

		Stanowisko pracy									
		Pracownik biurowy		Asystent		Specjalista		Kierownictwo wyższego szczebla (dyrektor)		Kierownictwo 3go szczebla (manager)	
		N	%	N	%	N	%	N	%	N	%
czynnikiem zwiększającym świadomość pracowników i kontrahentów organizacji, w której jest Pani/Pan zatrudniona/y, na temat zjawiska szpiegostwa korporacyjnego?											
Czy uważa Pani/Pan, że zjawisko szpiegostwa korporacyjnego powinno zostać zdefiniowane i uregulowane prawne w celu skutecznego jemu przeciwdziałania przez organy państwowe?	Zdecydowanie się nie zgadzam	17	19,8%	26	24,5%	33	31,4%	16	18,6%	15	18,3%
	Nie zgadzam się	20	23,3%	17	16,0%	13	12,4%	15	17,4%	21	25,6%
	Nie mam zdania	12	14,0%	26	24,5%	13	12,4%	16	18,6%	15	18,3%
	Zgadzam się	20	23,3%	26	24,5%	23	21,9%	18	20,9%	13	15,9%
	Zdecydowanie się zgadzam	17	19,8%	11	10,4%	23	21,9%	21	24,4%	18	22,0%

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Interpretacja wyników z tabel 17 i 22

Na podstawie danych empirycznych nie możemy przyjąć hipotezy H4.5. Oznacza to, że postrzeganie problematyki szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych nie zależy od zajmowanego stanowiska służbowego.

Tabela nr 22 przedstawia wyniki ankiety, ukazując postawy respondentów wobec problematyki szpiegostwa korporacyjnego w zależności od stanowiska w firmie. Zestawienie wyników dotyczy kluczowych pytań, które obejmują ocenę zagrożenia ze strony szpiegostwa korporacyjnego, ocenę efektywności środków ochrony, opinię na temat skuteczności regulacji i procedur, postrzeganie kontroli pracowników jako środka zapobiegawczego, poziom

przygotowania organizacji do reagowania na incydenty, istotność szkoleń oraz skuteczność działań prawnych. Wyniki wyrażone są liczbą odpowiedzi (N) oraz ich procentowym udziałem (%) w każdej grupie stanowisk. Należy pamiętać, że są to wyniki nieistotne statystycznie przedstawiające pewne tendencje w wynikach.

Zagrożenie dla przedsiębiorstwa: Postrzeganie zagrożenia różni się pomiędzy stanowiskami; najwyższy odsetek osób zgadzających się z zagrożeniem to wyższe kierownictwo (47,7%), a najmniej zgodnych jest wśród specjalistów (38,1%).

Odpowiednie środki ochrony: Wysoki poziom niezgody co do skuteczności działań zabezpieczających wyraża wyższe kierownictwo i specjaliści, a najwięcej osób zgadzających się (27,9%) znajduje się wśród pracowników biurowych.

Skuteczność regulacji: Wysoki poziom niepewności dotyczy grupy asystentów i specjalistów, z czego 24,5% asystentów oraz 24,8% specjalistów wskazuje „Nie mam zdania" w kwestii skuteczności regulacji. Z kolei osoby na stanowiskach kierowniczych wyższego szczebla wykazują większą niezgodność (40,7%).

Kontrole pracowników: Pracownicy biurowi oraz osoby na stanowiskach kierowniczych wyższego szczebla uważają, że kontrole mogą być pomocne (odpowiednio 22,1% i 24,5%).

Przygotowanie do reagowania: Poziom zgody na skuteczność organizacyjną w reagowaniu na incydenty jest relatywnie niski, a najwięcej osób „Zdecydowanie się nie zgadza" w grupach pracowników biurowych i asystentów (22,1% i 23,6%).

Znaczenie szkoleń: Pracownicy biurowi i asystenci przyznają istotność szkoleń w największym stopniu (30,2% i 24,5%).

Skuteczność działań prawnych: Wysoki poziom niezgody wyrażają pracownicy biurowi oraz osoby w kierownictwie wyższego szczebla (24,4% i 25,6%).

Problem rosnący w branży: Największa zgoda na to, że szpiegostwo to problem rosnący, pojawia się wśród kierowników wyższego szczebla (25,6%).

Wystarczające środki bezpieczeństwa: Brak zgody na skuteczność środków bezpieczeństwa wykazują głównie pracownicy biurowi i kierownictwo wyższego szczebla.

Świadomość ryzyka: Większość respondentów w kierownictwie 3. stopnia wskazuje brak zgody na odpowiednią świadomość ryzyka w organizacji (30,5%).

Efektywność systemów szkoleniowych: Asystenci wskazują najwyższy poziom zgody na efektywność szkoleń (26,4%).

Znaczenie szkoleń instytucji państwowych: Większość respondentów zgadza się, że szkolenia instytucji państwowych zwiększyłyby świadomość, z czym zgadza się 27,9% kierownictwa wyższego szczebla.

Regulacje prawne: Pracownicy biurowi i specjaliści w większości popierają wprowadzenie regulacji prawnych w celu skuteczniejszego przeciwdziałania szpiegostwu (23,3% i 21,9%).

5.3 Wnioski i rekomendacje w zakresie zarządzania bezpieczeństwem informacji przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych

Zarządzanie bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych (ICT) wymaga szczególnej uwagi ze względu na stale rosnące ryzyko związane z zagrożeniami cyfrowymi i fizycznymi, w tym szpiegostwem korporacyjnym. Przeprowadzone badania statystyczne oraz analiza danych zidentyfikowały kluczowe wyzwania, w tym niedostateczną świadomość pracowników, ograniczoną skuteczność istniejących procedur bezpieczeństwa, a także potrzebę wsparcia instytucji państwowych w edukacji na temat zagrożeń związanych ze szpiegostwem korporacyjnym. Wyniki wskazują również na znaczenie regulacji prawnych w przeciwdziałaniu temu zjawisku.

Na podstawie analizy zróżnicowanych grup demograficznych, takich jak wiek, poziom wykształcenia, staż pracy i zajmowane stanowisko, wyłaniają się istotne różnice w postrzeganiu zagrożeń oraz ocenie skuteczności działań prewencyjnych. Wyniki badań ujawniają również rosnące znaczenie szkoleń, szczególnie tych organizowanych przez instytucje państwowe, w zwiększaniu świadomości i przygotowaniu przedsiębiorstw do walki z zagrożeniami.

Poniżej przedstawiono szczegółowe wnioski i rekomendacje dotyczące zarządzania bezpieczeństwem w przedsiębiorstwach ICT, oparte na przeprowadzonych badaniach. Do głównych wniosków należy zaliczyć następujące elementy:

1. Rozwój programów szkoleniowych z zakresu zagrożeń szpiegostwa korporacyjnego

Rozwój programów szkoleniowych stanowi kluczowy element w przeciwdziałaniu szpiegostwu korporacyjnemu. Szkolenia te powinny obejmować trzy zasadnicze aspekty:

- **świadomość zagrożeń:** pracownicy powinni rozumieć istotę szpiegostwa korporacyjnego, w tym metody, jakie mogą być stosowane przez konkurencję, takie jak socjotechnika, cyberataki czy infiltracja organizacji przez osoby trzecie,
- **rozpoznawanie zagrożeń:** programy powinny nauczać identyfikacji oznak potencjalnego szpiegostwa, takich jak nietypowe zachowania pracowników, próby dostępu do poufnych informacji przez osoby z zewnątrz lub anomalie w systemach informatycznych,

- **reagowanie na incydenty:** kluczowe jest wypracowanie procedur szybkiego i skutecznego reagowania na podejrzenia o szpiegostwo, takich jak zgłaszanie podejrzanych incydentów do działu bezpieczeństwa.

Szkolenia powinny być regularnie aktualizowane, dostosowane do specyfiki branży, a także uwzględniać najnowsze techniki stosowane przez osoby i organizacje próbujące pozyskać informacje w sposób nielegalny. Wprowadzenie realistycznych symulacji i warsztatów praktycznych pozwoli uczestnikom lepiej przygotować się na potencjalne sytuacje kryzysowe.

2. Współpraca z instytucjami państwowymi w zakresie edukacji i profilaktyki

Partnerstwo z instytucjami państwowymi, takimi jak Agencja Bezpieczeństwa Wewnętrznego (ABW) czy Policja, może znacząco zwiększyć skuteczność działań prewencyjnych. Współpraca ta powinna obejmować:

- **programy szkoleniowe:** instytucje państwowe mogą dostarczać przedsiębiorstwom ekspertów do prowadzenia szkoleń oraz udostępniać materiały edukacyjne bazujące na realnych przypadkach szpiegostwa korporacyjnego,
- **wymianę informacji:** mechanizmy szybkiej wymiany informacji o zagrożeniach pomiędzy firmami a instytucjami państwowymi pozwolą na wczesne ostrzeganie o potencjalnych zagrożeniach.
- **wsparcie w sytuacjach kryzysowych:** instytucje państwowe mogą wspierać przedsiębiorstwa w zakresie dochodzeń dotyczących incydentów szpiegowskich, a także w opracowywaniu rekomendacji dotyczących poprawy zabezpieczeń.

Warto podkreślić, że instytucje państwowe dysponują zaawansowanymi narzędziami analitycznymi i doświadczeniem w walce z zagrożeniami bezpieczeństwa, co czyni je niezwykle cennym partnerem w budowaniu systemu ochrony przed szpiegostwem.

3. Wprowadzenie kompleksowych regulacji prawnych dotyczących szpiegostwa korporacyjnego

Obecne regulacje prawne w zakresie przeciwdziałania szpiegostwu korporacyjnemu często okazują się niewystarczające. Konieczne jest wprowadzenie przepisów, które:

- **definiują szpiegostwo korporacyjne:** jasna definicja prawna pozwoli na bardziej precyzyjne zidentyfikowanie tego zjawiska w kontekście działań prawnych,
- **określają obowiązki przedsiębiorstw:** przepisy powinny nakładać na przedsiębiorstwa obowiązek implementacji minimalnych standardów bezpieczeństwa, takich jak systemy ochrony danych czy regularne audyty bezpieczeństwa,
- **zaostrzają sankcje:** wyższe kary finansowe i więzienia dla osób oraz organizacji zaangażowanych w szpiegostwo mogą działać odstraszająco,

- **tworzą instytucje nadzorujące:** wprowadzenie organów nadzorujących przestrzeganie przepisów oraz oferujących wsparcie przedsiębiorstwom w ich implementacji.

Organizacje powinny aktywnie uczestniczyć w procesie legislacyjnym poprzez konsultacje społeczne, aby regulacje odpowiadały rzeczywistym potrzebom sektora.

4. Implementacja zaawansowanych technologii ochrony danych

Zabezpieczenia technologiczne stanowią pierwszą linię obrony przed szpiegostwem korporacyjnym. Zaleca się:

- **zastosowanie sztucznej inteligencji:** systemy AI mogą wykrywać anomalie w sieciach i sygnalizować podejrzane działania w czasie rzeczywistym, co pozwala na szybkie reagowanie na potencjalne zagrożenia,
- **szyfrowanie danych:** wszystkie poufne dane, zarówno w ruchu, jak i w spoczynku, powinny być szyfrowane przy użyciu nowoczesnych algorytmów.
- **zarządzanie dostępem:** stosowanie zasad najmniejszego przywileju i wielopoziomowej autoryzacji zapewni, że dostęp do informacji mają tylko osoby ściśle uprawnione,
- **monitorowanie systemów:** regularne audyty oraz monitoring systemów informatycznych pozwolą na wykrycie nieautoryzowanego dostępu lub prób naruszenia.

Dodatkowo, organizacje powinny inwestować w szkolenia techniczne dla personelu IT, aby zapewnić im umiejętności niezbędne do zarządzania i optymalizacji systemów zabezpieczeń.

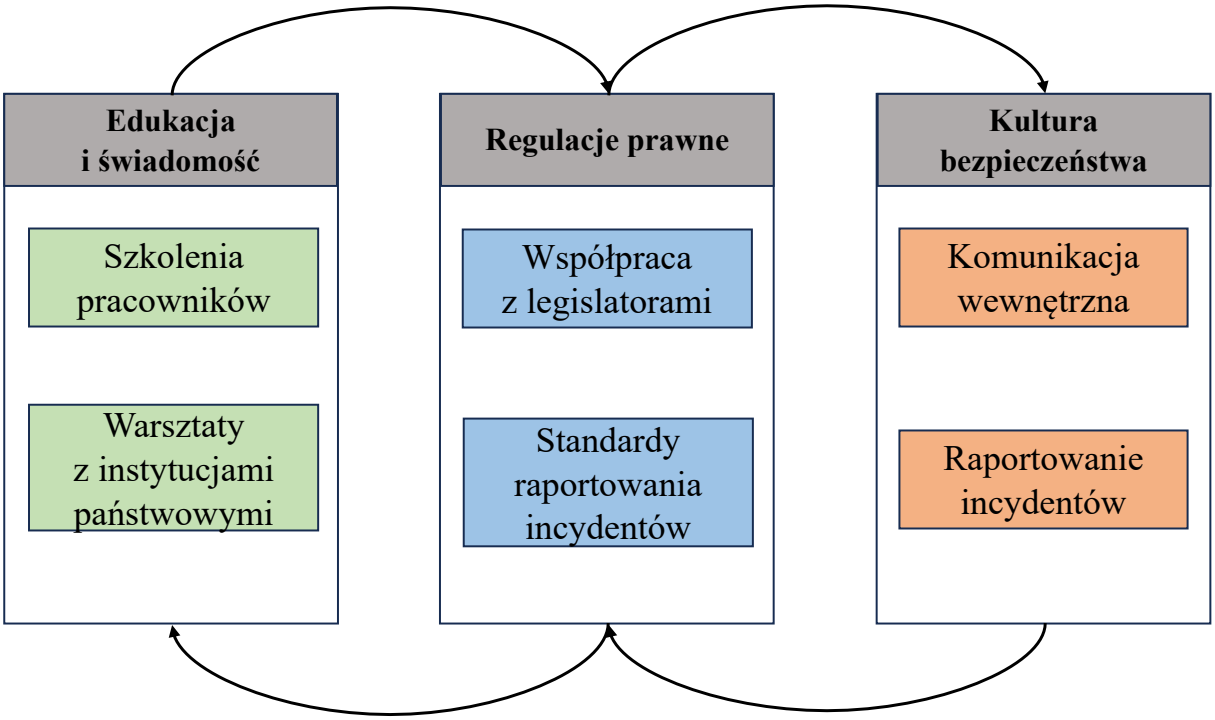
5. Wzmacnianie kultury organizacyjnej opartej na bezpieczeństwie

Bezpieczeństwo informacji powinno być integralną częścią kultury organizacyjnej, co wymaga zaangażowania na wszystkich szczeblach przedsiębiorstwa:

- **zaangażowanie w bezpieczeństwo:** kierownictwo powinno regularnie komunikować znaczenie ochrony informacji oraz promować odpowiedzialność za bezpieczeństwo wśród pracowników,
- **promowanie etyki:** przedsiębiorstwa powinny wdrażać kodeksy etyczne, które podkreślają wagę ochrony danych oraz odpowiedzialności pracowników za ich przestrzeganie,
- **motywowanie pracowników:** programy motywacyjne, takie jak nagrody za zgłaszanie potencjalnych zagrożeń, mogą zwiększyć aktywne zaangażowanie pracowników w kwestie bezpieczeństwa,
- **tworzenie atmosfery zaufania:** pracownicy powinni czuć, że mogą zgłaszać incydenty czy obiekcje związane z bezpieczeństwem bez obawy o konsekwencje.

Ponadto, kultura bezpieczeństwa powinna być wspierana przez regularne oceny jej stanu poprzez badania ankietowe i audyty wewnętrzne.

Rysunek nr 23 przedstawia kluczowe elementy systemu zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych. Skupia się on na integracji działań prewencyjnych oraz edukacyjnych w celu minimalizacji ryzyka szpiegostwa korporacyjnego.

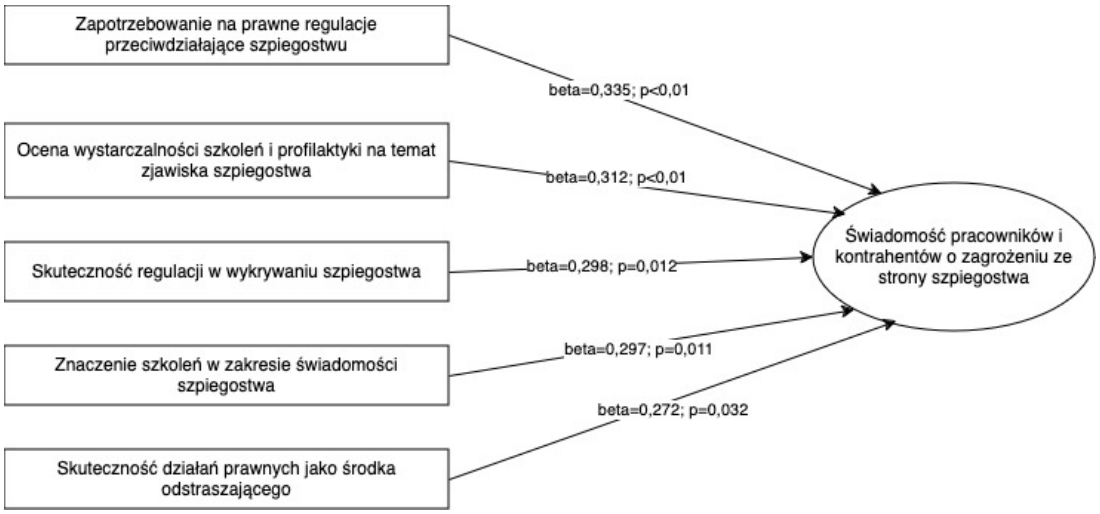


Rysunek 23 Kluczowe obszary zarządzania bezpieczeństwem przedsiębiorstwa ICT
Źródło: opracowanie własne.

Rysunek ilustruje trzy kluczowe obszary istotne dla skutecznego zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych: edukację i świadomość, regulacje prawne oraz kulturę bezpieczeństwa. Obszar edukacji i świadomości podkreśla konieczność prowadzenia regularnych szkoleń, warsztatów i programów informacyjnych, które zwiększają wiedzę pracowników oraz kontrahentów na temat zagrożeń związanych ze szpiegostwem korporacyjnym i metod ich przeciwdziałania. Sekcja dotycząca regulacji prawnych wskazuje na potrzebę opracowania i wdrożenia jasnych, spójnych przepisów oraz procedur, które zarówno zapobiegają zagrożeniom, jak i definiują standardy odpowiedzialności. Kultura bezpieczeństwa natomiast uwypukla znaczenie budowania w organizacji środowiska, w którym ochrona informacji traktowana jest jako wspólna odpowiedzialność, a pracownicy i kierownictwo działają zgodnie z zasadami etyki i najlepszych praktyk w zakresie bezpieczeństwa.

5.4 Opracowanie modelu zarządzania bezpieczeństwem informacji

Na rysunku nr 24 przedstawiono analizę regresji. Na podstawie otrzymanego modelu regresyjnego nie ma podstaw do odrzucenia postawionej hipotezy 6. Oznacza to, że postrzegane przez pracowników skuteczność procedur ochrony, edukacja w zakresie zagrożeń oraz środki prawne wpływają na ich ocenę (świadomość) ryzyka szpiegostwa korporacyjnego w organizacji.



Rysunek 24 Analiza regresji dla świadomości pracowników i kontrahentów dot. zagrożenia ze strony szpiegostwa
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Przedstawiony na rysunku diagram przedstawia wyniki analizy regresji, która bada wpływ pięciu czynników na świadomość pracowników i kontrahentów o zagrożeniu ze strony szpiegostwa. Każda strzałka reprezentuje wpływ danej zmiennej niezależnej na zmienną zależną, wraz z wartościami współczynników beta i istotności statystycznej (p-wartości).

Zapotrzebowanie na regulacje prawne ma dodatni wpływ na świadomość pracowników o zagrożeniu szpiegostwem (beta=0,335). Wzrost zapotrzebowania na regulacje zwiększa świadomość. Oznacza to, że zapotrzebowanie na regulacje prawne ma dodatni wpływ na świadomość pracowników o zagrożeniu szpiegostwem. Wzrost zapotrzebowania na regulacje zwiększa świadomość. Jest to najistotniejszy predyktor wśród wszystkich analizowanych zmiennych.

Pozytywna ocena szkoleń i profilaktyki na temat szpiegostwa przyczynia się do wzrostu świadomości o zagrożeniu (beta=0,312). Skuteczność regulacji w wykrywaniu szpiegostwa ma pozytywny wpływ na świadomość pracowników i kontrahentów o zagrożeniu (beta=0,298). Znaczenie szkoleń w zakresie świadomości szpiegostwa jest pozytywnie powiązane ze świadomością o zagrożeniu szpiegostwem (beta=0,297). Skuteczność działań prawnych, które

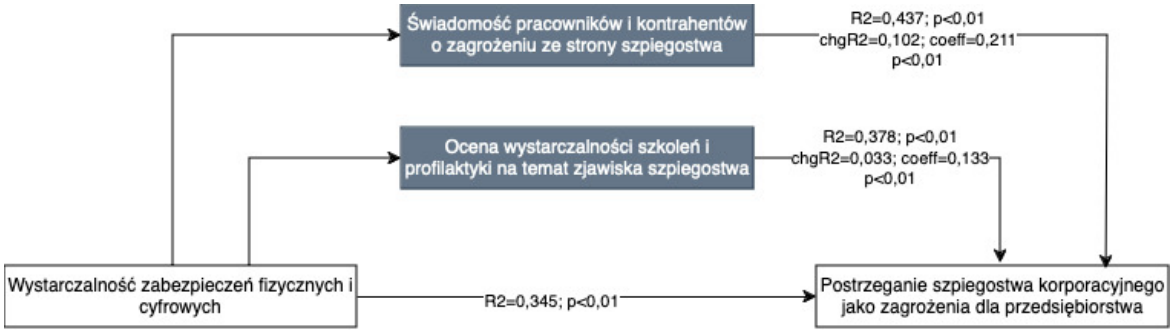
odstraszają przed szpiegostwem, pozytywnie wpływa na świadomość o zagrożeniu (beta=0,272).

Wszystkie pięć czynników mają istotny, dodatni wpływ na świadomość pracowników i kontrahentów o zagrożeniu ze strony szpiegostwa, przy czym największy wpływ wykazano dla:

1. Zapotrzebowania na prawne regulacje,
2. Oceny wystarczalności szkoleń i profilaktyki.

Wyniki te sugerują, że zwiększenie zapotrzebowania na regulacje prawne oraz ocena jakości szkoleń mają kluczowe znaczenie dla zwiększania świadomości o zagrożeniu ze strony szpiegostwa. Pozostałe czynniki, choć nieco mniej istotne, również przyczyniają się do podniesienia świadomości pracowników, co jest istotne z punktu widzenia zarządzania bezpieczeństwem w organizacji.

Na rysunku nr 25 przedstawiono analizę mediacji. Wskazuje ona, że nie ma podstaw do odrzucenia hipotezy 7. Oznacza to, że szkolenia i świadomość pracowników są mediatorem wpływu skuteczności zabezpieczeń organizacyjnych na postrzegane ryzyko szpiegowskie.



Rysunek 25 Analiza mediacji cech dot. postrzegania szpiegostwa korporacyjnego jako zagrożenia dla przedsiębiorstwa
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Na przedstawionym diagramie analizowany jest wpływ zmiennej niezależnej **Wystarczalność zabezpieczeń fizycznych i cyfrowych** na zmienną zależną **Postrzeganie szpiegostwa korporacyjnego jako zagrożenia dla przedsiębiorstwa**, z uwzględnieniem dwóch potencjalnych mediatorów: **Świadomości pracowników i kontrahentów o zagrożeniu ze strony szpiegostwa** oraz **Oceny wystarczalności szkoleń i profilaktyki na temat zjawiska szpiegostwa**. Interpretacja analizy mediacji przedstawia się następująco:

1. **Bezpośredni wpływ**:
    - **wystarczalność zabezpieczeń fizycznych i cyfrowych** bezpośrednio wpływa na **Postrzeganie szpiegostwa korporacyjnego jako zagrożenia dla przedsiębiorstwa**.

- wartość R2=0,345 (p<0,01) sugeruje, że wystarczalność zabezpieczeń fizycznych i cyfrowych wyjaśnia 34,5% wariancji w postrzeganiu szpiegostwa jako zagrożenia. Jest to stosunkowo silny i istotny wpływ.

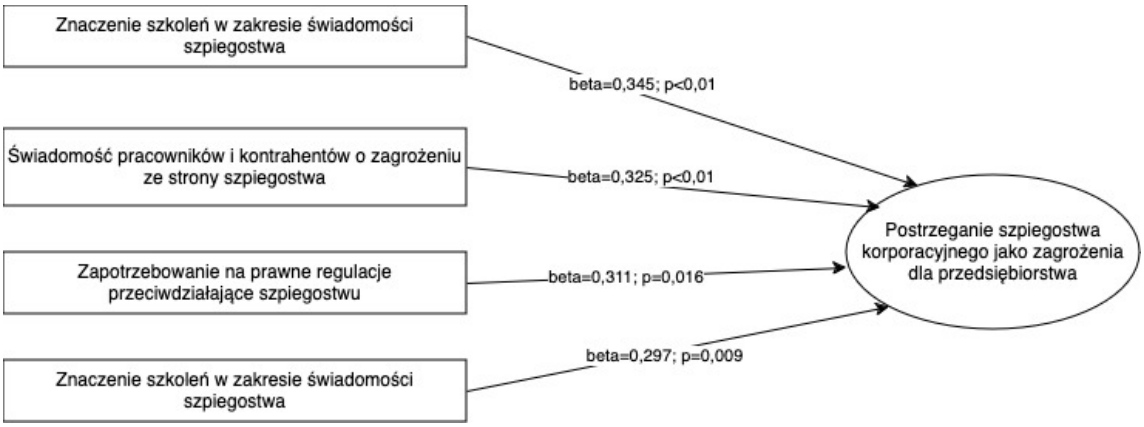
2. **Mediacja przez świadomość pracowników i kontrahentów**:
   - **wystarczalność zabezpieczeń fizycznych i cyfrowych** wpływa również na **Świadomość pracowników i kontrahentów o zagrożeniu ze strony szpiegostwa**, co wskazuje, że im wyższa jest ocena zabezpieczeń, tym większa jest świadomość zagrożenia.
   - wartość R2=0, (p < 0,01) dla tego modelu sugeruje, że 43,7% wariancji w świadomości pracowników jest wyjaśnione przez zabezpieczenia. Wartość współczynnika mediacji wynosi coeff=0,211 (p < 0,01), co wskazuje na silny i istotny wpływ tej świadomości na postrzeganie szpiegostwa jako zagrożenia.
3. **Mediacja przez ocenę wystarczalności szkoleń**:
   - **wystarczalność zabezpieczeń fizycznych i cyfrowych** wpływa także na **Ocenę wystarczalności szkoleń i profilaktyki na temat zjawiska szpiegostwa**.
   - R2=0, (p<0,01) sugeruje, że zabezpieczenia wyjaśniają 37,8% wariancji w ocenie szkoleń.
   - co ważne, wartość współczynnika mediacji wynosi coeff=0,133 (p < 0,01), co oznacza, że ocena szkoleń ma istotny, dodatni wpływ na postrzeganie zagrożenia szpiegostwem.
4. **Łączny efekt mediacji**:
   - zwiększenie poziomu zabezpieczeń fizycznych i cyfrowych wpływa zarówno bezpośrednio, jak i pośrednio (poprzez wzrost świadomości pracowników oraz ocenę jakości szkoleń) na postrzeganie szpiegostwa jako zagrożenia.
   - zmiana wartości R2 (oznaczona jako *chgR2*) wynosi 0,102 dla świadomości pracowników i 0,033 dla oceny szkoleń, co wskazuje na znaczący wkład obu mediatorów do wyjaśnienia wariancji w postrzeganiu zagrożenia.

Wyniki analizy mediacji sugerują, że **wystarczalność zabezpieczeń fizycznych i cyfrowych** wpływa na **postrzeganie szpiegostwa korporacyjnego jako zagrożenia** zarówno bezpośrednio, jak i pośrednio, poprzez dwa mechanizmy mediacyjne:

1. **Świadomość pracowników i kontrahentów o zagrożeniu** — jest to silniejszy mediator, który ma większy wpływ na postrzeganie zagrożenia.
2. **Ocena wystarczalności szkoleń i profilaktyki** — również istotnie wpływa na postrzeganie zagrożenia, ale w mniejszym stopniu niż świadomość.

Obecność tych mediatorów wskazuje, że samo zwiększenie zabezpieczeń nie wystarczy, aby zmniejszyć postrzeganie zagrożenia szpiegostwem. Niezbędne jest również budowanie świadomości oraz dbanie o ocenę jakości szkoleń w tej tematyce.

Na rysunku nr 26 przedstawiono analizę regresji. Na jej podstawie nie ma podstaw do odrzucenia postawionej hipotezy 8. Oznacza to, że Szkolenia i świadomość, i regulacje prawne wpływają na postrzeganie zagrożenia szpiegostwem



Rysunek 26 Analiza regresji cech dot. postrzegania szpiegostwa korporacyjnego jako zagrożenia dla przedsiębiorstwa

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Rysunek przedstawia analizę regresji, która służy do zbadania wpływu dwóch kluczowych czynników – **szkoleń i świadomości** oraz **regulacji prawnych** – na **postrzeganie zagrożenia szpiegostwem korporacyjnym** jako ryzyka dla przedsiębiorstwa.

Interpretacja wyników analizy regresji

Wyniki analizy wskazują, że istnieje istotna statystycznie zależność między omawianymi czynnikami a postrzeganiem zagrożenia szpiegostwem. Oznacza to, że:

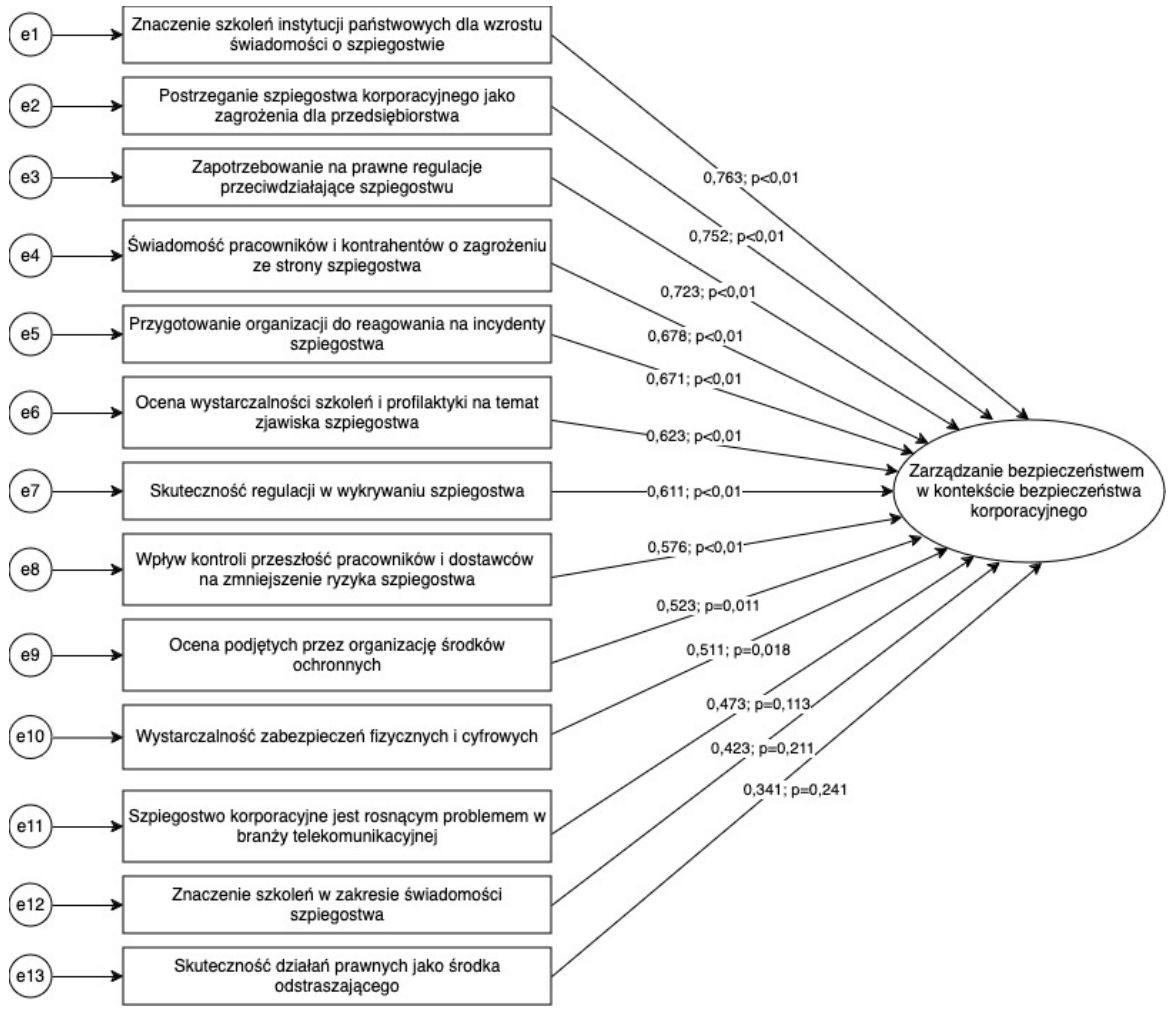
1. **Szkolenia i świadomość** – Działania związane z edukowaniem pracowników i podnoszeniem ich świadomości w zakresie zagrożeń związanych ze szpiegostwem korporacyjnym przyczyniają się do zwiększenia postrzegania tego zagrożenia jako realnego ryzyka dla przedsiębiorstwa. Szkolenia prawdopodobnie dostarczają wiedzy na temat metod i konsekwencji szpiegostwa, co wpływa na większą świadomość pracowników i kadry zarządzającej.
2. **Regulacje prawne** – Obecność i znajomość regulacji prawnych przeciwdziałających szpiegostwu również wpływa na wzrost postrzegania tego zjawiska jako zagrożenia. Przepisy prawne wprowadzają formalne ramy i sankcje za działania związane ze szpiegostwem, co może zwiększać poczucie zagrożenia i zachęcać organizacje do podjęcia odpowiednich środków ochronnych.

Na podstawie wyników regresji nie ma podstaw do odrzucenia hipotezy 8, co oznacza, że wpływ **szkoleń i świadomości** oraz **regulacji prawnych** na postrzeganie zagrożenia szpiegostwem korporacyjnym jest uzasadniony. Wyniki sugerują, że oba te czynniki są istotne w budowaniu świadomości ryzyka i przekonania, że szpiegostwo stanowi realne zagrożenie dla organizacji.

Wyniki analizy regresji wskazują, że aby skutecznie budować świadomość zagrożeń związanych ze szpiegostwem korporacyjnym, organizacje powinny inwestować zarówno w szkolenia, które podnoszą świadomość wśród pracowników, jak i w przestrzeganie oraz znajomość odpowiednich regulacji prawnych. Działania te wspierają postrzeganie zagrożenia szpiegostwem jako realnego ryzyka, co może skłaniać przedsiębiorstwa do podejmowania bardziej świadomych i proaktywnych działań zabezpieczających.

Podsumowując, analiza regresji przedstawiona na rysunku nr 26 pokazuje, że szkolenia i regulacje prawne są istotnymi elementami, które wpływają na percepcję szpiegostwa korporacyjnego jako zagrożenia, co wspiera hipotezę 8.

Rysunek nr 27 przedstawia analizę czynnikową konfirmacyjną (CFA) oceniającą znaczenie różnych cech dla budowy modelu zarządzania bezpieczeństwem w kontekście bezpieczeństwa korporacyjnego.



Rysunek 27 Analiza czynnikowa konfirmacyjna (RMSEA=0,043; Chi2=23,323; p<0,01l GFI=0,987; CFI=0,988) oceny istotności cech w budowie modelu zarządzania bezpieczeństwem w kontekście bezpieczeństwa korporacyjnego

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Wyniki CFA służą do potwierdzenia, że przyjęty model dobrze pasuje do danych i że wybrane czynniki (zmienne) są istotne dla opisywanego modelu bezpieczeństwa korporacyjnego. Kluczowe wskaźniki dopasowania modelu:

1. **RMSEA (Root Mean Square Error of Approximation)**: Wartość RMSEA wynosi 0,043. RMSEA mierzy błąd aproksymacji modelu w stosunku do danych, a wartości poniżej 0,05 są zwykle interpretowane jako bardzo dobre dopasowanie. Wartość 0,043 sugeruje, że model dobrze odwzorowuje dane, co świadczy o jego trafności.
2. **Chi-Square (Chi²)**: Wartość statystyki Chi² wynosi 23,323 przy poziomie istotności $p < 0,01$. Niska wartość Chi² względem stopni swobody oraz istotność statystyczna sugerują, że model różni się od idealnego dopasowania, jednak niewielka wartość tej różnicy przy niskim RMSEA wskazuje na akceptowalne dopasowanie.

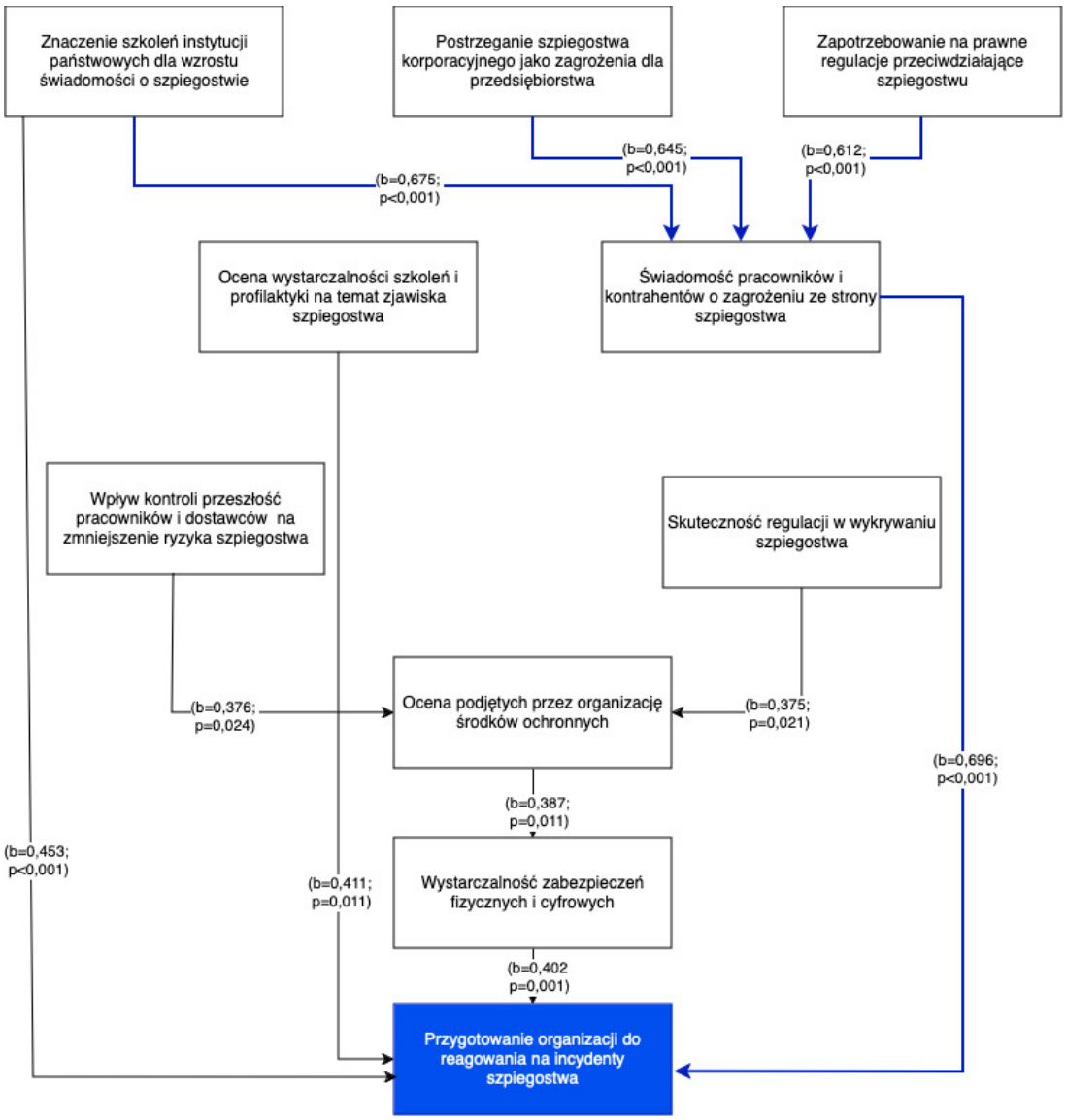
3. **GFI (Goodness of Fit Index)**: Wartość GFI wynosi 0,987. GFI mierzy ogólne dopasowanie modelu i wartości bliskie 1 oznaczają bardzo dobre dopasowanie. Wskaźnik 0,987 jest bliski idealnego dopasowania, co wzmacnia wiarygodność modelu.
4. **CFI (Comparative Fit Index)**: Wartość CFI wynosi 0,988. CFI porównuje dopasowanie badanego modelu z modelem niezależnym (gdzie wszystkie zmienne są założone jako nieskorelowane). Wartości powyżej 0,95 są uznawane za bardzo dobre, a wynik 0,988 sugeruje doskonałe dopasowanie modelu do danych.

Wyniki analizy czynnikowej konfirmacyjnej (CFA) sugerują, że przyjęte cechy są istotne w budowie modelu zarządzania bezpieczeństwem w kontekście bezpieczeństwa korporacyjnego. Wskaźniki dopasowania (RMSEA, GFI, CFI) świadczą o wysokiej jakości modelu i potwierdzają jego spójność z danymi empirycznymi.

Model ten może obejmować kluczowe czynniki, takie jak ocena ryzyka, polityki bezpieczeństwa, procedury reagowania na incydenty oraz zarządzanie zasobami ludzkimi. Wysokie wartości wskaźników GFI i CFI oraz niski RMSEA sugerują, że te cechy są adekwatnie ujęte w modelu, co czyni go użytecznym narzędziem do oceny i poprawy bezpieczeństwa w organizacjach.

Podsumowując, analiza czynnikowa konfirmacyjna wskazuje na trafność i rzetelność budowy modelu zarządzania bezpieczeństwem, co może mieć praktyczne zastosowanie w kontekście zapewnienia bezpieczeństwa korporacyjnego.

Na rysunku nr 28 przedstawiono analizę ścieżkową przedstawiającą model zarządzania bezpieczeństwem informacji w kontekście bezpieczeństwa przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych.



Rysunek 28 Analiza ścieżkowa SEM - model zarządzania bezpieczeństwem informacji w kontekście bezpieczeństwa korporacyjnego

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Przedstawiony na rysunku diagram obrazuje model ścieżkowy SEM (Structural Equation Modeling) dotyczący przygotowania organizacji do reagowania na incydenty szpiegostwa korporacyjnego. Model opisuje zależności między różnymi zmiennymi, które wpływają na gotowość organizacji do przeciwdziałania szpiegostwu. Główne komponenty i ich powiązania to:

1. **Znaczenie szkoleń instytucji państwowych** – To szkolenie ma wpływ na świadomość pracowników i kontrahentów na temat zagrożenia szpiegostwem ($b = 0,675$; $p < 0,001$).
2. **Postrzeganie szpiegostwa korporacyjnego jako zagrożenia** – Ma ono bezpośredni wpływ na świadomość o zagrożeniu szpiegostwem ($b = 0,645$; $p < 0,001$) oraz pośredni wpływ na ocenę wystarczalności szkoleń i profilaktyki.

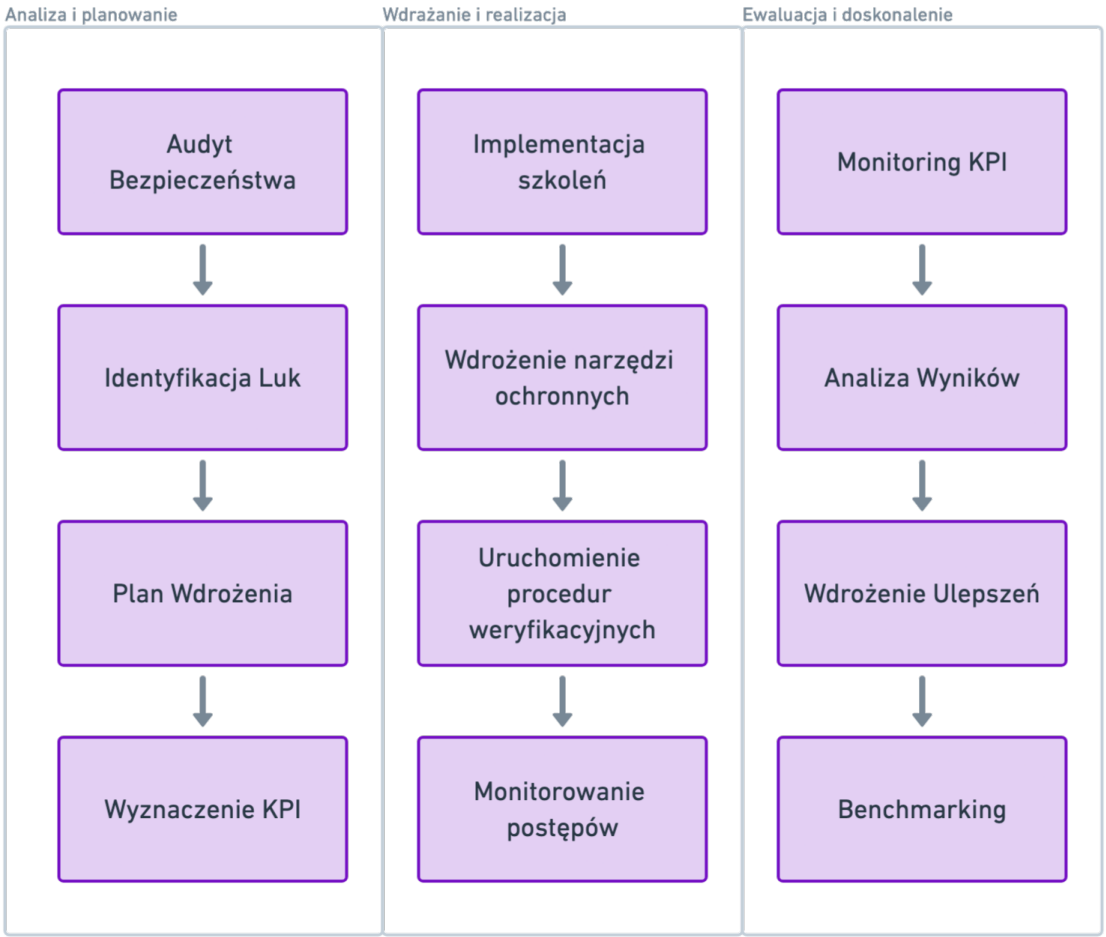
3. **Zapotrzebowanie na regulacje prawne** – Ta zmienna również zwiększa świadomość o zagrożeniach szpiegostwa ($b = 0,612$; $p < 0,001$) i pośrednio wpływa na przygotowanie organizacji.
4. **Ocena wystarczalności szkoleń i profilaktyki** – Zwiększa świadomość pracowników o zagrożeniu (brak wartości bezpośredniej) i wpływa na ocenę środków ochronnych.
5. **Ocena kontroli przeszłości pracowników i dostawców** – Jest istotna dla zmniejszenia ryzyka szpiegostwa ($b = 0,376$; $p = 0,024$).
6. **Ocena środków ochronnych** – To działania organizacyjne wpływające na przygotowanie do incydentów ($b = 0,387$; $p = 0,011$).
7. **Wystarczalność zabezpieczeń fizycznych i cyfrowych** – Ma kluczowy wpływ na przygotowanie do reagowania ($b = 0,402$; $p = 0,001$).
8. **Skuteczność regulacji w wykrywaniu szpiegostwa** – Pośrednio wpływa na przygotowanie organizacji ($b = 0,696$; $p < 0,001$).

Wynik modelu sugeruje, że kluczowe czynniki, takie jak świadomość zagrożeń, kontrola ryzyka oraz odpowiednie zabezpieczenia, przyczyniają się do lepszego przygotowania organizacji na incydenty szpiegostwa.

Rozdział 6.IMPLEMENTACJA MODELU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W SEKTORZE TECHNOLOGII INFORMACYJNO-KOMUNIKACYJNYCH

6.1 Przygotowanie organizacyjne do wdrożenia modelu zarządzania bezpieczeństwem informacji

Przygotowanie organizacji do implementacji modelu zarządzania bezpieczeństwem można rozłożyć na trzy zasadnicze fazy: Etap Analizy i planowania, Etap Wdrażania i realizacji oraz Etap Ewaluacji i doskonalenia. Każda z tych faz obejmuje konkretne działania, określone wskaźniki efektywności oraz zestaw narzędzi wspomagających proces monitorowania realizacji założeń. Etapy wdrażania zostały przedstawione na rysunku nr 29.



Rysunek 29 Etapy przygotowania organizacji do wdrożenia modelu zarządzania bezpieczeństwem

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Etap pierwszy, obejmujący analizę i planowanie, stanowi fundament przygotowań organizacji do wdrożenia modelu zarządzania bezpieczeństwem. Jego głównym celem jest kompleksowe zrozumienie aktualnego stanu zabezpieczeń w organizacji, identyfikacja kluczowych luk oraz opracowanie strategicznego planu działań, który umożliwi skuteczną implementację modelu. Proces ten można podzielić na trzy podetapy: audyt bezpieczeństwa, identyfikację i priorytetyzację luk oraz opracowanie szczegółowego planu działań.

W pierwszym podetapie, audycie bezpieczeństwa, przeprowadza się analizę istniejących procedur ochrony danych, kontroli dostępu oraz zarządzania incydentami. Obejmuje on także ocenę zasobów organizacyjnych, w tym infrastruktury IT, zabezpieczeń fizycznych oraz narzędzi ochronnych. Kluczowym elementem tego podetapu jest identyfikacja luk w zabezpieczeniach, oparta na analizie wcześniejszych incydentów oraz wykorzystaniu narzędzi takich jak checklisty zgodności. Efektywność tego etapu mierzona jest za pomocą wskaźników takich jak procent wykrytych luk w zabezpieczeniach oraz czas trwania audytu, co pozwala monitorować skuteczność przeprowadzanych działań.

Kolejnym podetapem (2) jest identyfikacja i priorytetyzacja luk w zabezpieczeniach. Na tym etapie przeprowadza się klasyfikację zidentyfikowanych luk według ich ważności, dzieląc je na kategorie krytyczne, wysokiego, średniego i niskiego ryzyka. Ocenia się również wpływ tych luk na działalność organizacji w kontekście finansowym, operacyjnym i prawnym, a także dokonuje weryfikacji zgodności z regulacjami branżowymi i prawnymi. Wskaźniki efektywności tego etapu obejmują między innymi procent luk sklasyfikowanych jako krytyczne, co pozwala na precyzyjne określenie priorytetów działań.

Następny podetap (3) polega na opracowaniu kompleksowego planu działań, który określa harmonogram wdrożenia, priorytety działań wynikające z analizy luk oraz alokację zasobów i odpowiedzialności. W ramach tego podetapu wyznacza się kamienie milowe oraz zespoły wdrożeniowe odpowiedzialne za kluczowe obszary. Ponadto definiuje się wskaźniki efektywności, takie jak liczba wdrożonych procedur czy poziom zgodności z regulacjami, które pozwalają na bieżące monitorowanie postępów. Efektywność tego etapu mierzy się m.in. procentem ukończenia harmonogramu oraz procentem zarezerwowanych zasobów w stosunku do wymagań.

W celu monitorowania postępów i identyfikacji obszarów wymagających poprawy (podetap 4) w trakcie realizacji etapu 1, proponuje się wykorzystanie następujących wskaźników przedstawionych w tabeli nr 23.

Tabela 23 Kluczowe wskaźniki dla realizacji etapu 1

Wskaźnik	Podetap	Opis	Znaczenie
Czas trwania audytu (Audit duration)	1	Mierzy czas potrzebny na przeprowadzenie audytu	Wskazuje efektywność procesu analitycznego
Procent wykrytych luk w zabezpieczeniach (Percentage of identified vulnerabilities)	1	Określa, jak skuteczny był audyt w identyfikacji luk	Pokazuje jakość analizy przeprowadzonej w organizacji
Procent luk sklasyfikowanych jako krytyczne (Percentage of critical vulnerabilities)	2	Mierzy skalę najbardziej istotnych zagrożeń	Wskazuje na pilność działań naprawczych
Procent ukończenia harmonogramu (Schedule completion percentage)	3	Ocena realizacji działań względem planu	Monitoruje zgodność działań z harmonogramem
Procent zarezerwowanych zasobów (Allocated resources percentage)	3	Wyraża dostępność zasobów przewidzianych na etapie planowania	Wskazuje, czy organizacja jest gotowa do dalszego wdrożenia

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Czas trwania audytu (Audit duration, AD)

$$AD = \frac{Łączna\ liczba\ godzin\ audytu}{Liczba\ audytorów\ zaangażowanych\ w\ proces}$$

Opis:

Cel: ten wskaźnik mierzy czas potrzebny na przeprowadzenie pełnej analizy aktualnego stanu bezpieczeństwa organizacji, w tym oceny procedur, zasobów, luk i zgodności z regulacjami. Jest wyrażany w dniach roboczych i wskazuje efektywność procesu analizy,

Interpretacja: jeśli audyt trwa 5 dni zamiast planowanych 10, oznacza to sprawne przeprowadzenie analizy, ale należy upewnić się, że nie przeoczono kluczowych obszarów.

Procent wykrytych luk w zabezpieczeniach (Percentage of identified vulnerabilities, PIV)

$$PIV = \frac{Liczba\ wykrytych\ luk}{Całkowita\ liczba\ kontrolowanych\ obszarów} \times 100\%$$

Opis:

Cel: wyraża, jaki odsetek zidentyfikowanych potencjalnych problemów został wykryty podczas audytu w stosunku do wszystkich analizowanych obszarów. Wskazuje na skuteczność procesu audytorskiego,

Interpretacja: jeśli w audycie uwzględniono 50 obszarów, a wykryto 30 luk, wskaźnik wynosi 60%. Organizacja może uznać to za punkt wyjściowy do dalszych działań.

Procent luk sklasyfikowanych jako krytyczne (Percentage of critical vulnerabilities, PCV)

$$PCV = \frac{Liczba\ krytycznych\ luk}{Całkowita\ liczba\ luk} \times 100\%$$

Opis:

Cel: mierzy udział luk o najwyższym poziomie ryzyka wśród wszystkich wykrytych problemów. Pokazuje skalę zagrożeń, które mogą mieć bezpośredni wpływ na działalność organizacji,

Interpretacja: jeśli z 20 wykrytych luk 8 zostało uznanych za krytyczne, wskaźnik wynosi 40%. Wskazuje to na istotne zagrożenia wymagające szybkich działań.

Procent ukończenia harmonogramu (Schedule completion percentage, SCP)

$$SCP = \frac{Liczba\ zrealizowanych\ działań}{Całkowita\ liczba\ działań\ zaplanowanych} \times 100\%$$

Opis:

Cel: mierzy, jaki odsetek działań zaplanowanych na etapie 1 został zrealizowany w określonym czasie. Wskaźnik ten pozwala ocenić, czy prace przebiegają zgodnie z harmonogramem,

Interpretacja: jeśli w harmonogramie przewidziano 10 działań, a ukończono 7, wskaźnik wynosi 70%. Organizacja powinna skoncentrować się na przyspieszeniu realizacji pozostałych działań.

Procent zarezerwowanych zasobów (Allocated resources percentage, ARP)

$$ARP = \frac{Zarezerwowane\ zasoby}{Wymagane\ zasoby} \times 100\%$$

Opis:

Cel: określa, jaki odsetek zasobów (ludzkich, finansowych, technologicznych) przewidzianych w planie został rzeczywiście zarezerwowany na potrzeby realizacji działań,

Interpretacja: jeśli wymagano 100 godzin pracy zespołu, a udało się zarezerwować 80 godzin, wskaźnik wynosi 80%. Organizacja powinna zająć się pozyskaniem brakujących zasobów.

Każdy z tych wskaźników odgrywa kluczową rolę w skutecznym monitorowaniu postępów oraz identyfikacji obszarów wymagających poprawy w trakcie realizacji etapu 1. Dzięki ich systematycznemu pomiarowi organizacja zyskuje solidną podstawę do kolejnych etapów wdrożenia.

Na potrzeby wdrożenia etapu 1 przygotowano przykładowy harmonogram przedstawiony w tabeli nr 24.

Tabela 24 Przykładowy harmonogram wdrożenia etapu 1

Tydzień	Działanie	Opis	Odpowiedzialny
1	Przeprowadzenie audytu	Analiza istniejących procedur i zasobów	Zespół ds. bezpieczeństwa
2	Analiza luk i priorytetyzacja	Klasyfikacja luk wg poziomu ryzyka	Lider ds. ryzyka
3	Przygotowanie planu wdrożenia	Opracowanie harmonogramu i określenie KPI	Menedżer projektu
4	Prezentacja planu zarządowi	Zatwierdzenie działań i przypisanie odpowiedzialności	Zarząd

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Przedstawiony harmonogram obrazuje ramowy plan realizacji pierwszego etapu wdrażania modelu zarządzania bezpieczeństwem w organizacji. Zakłada on czterotygodniowy cykl obejmujący zadania analityczne, diagnostyczne oraz planistyczne. Każdy tydzień ma jasno określony cel oraz przypisane działania, co umożliwia optymalne wykorzystanie czasu i zasobów. Podejście to bazuje na zasadzie sekwencyjności, gdzie realizacja kolejnych etapów opiera się na wynikach wcześniejszych działań, co zapewnia spójność całego procesu.

Pierwszy tydzień harmonogramu koncentruje się na przeprowadzeniu szczegółowego audytu bezpieczeństwa organizacji. Działania obejmują analizę polityk ochrony danych, procedur reagowania na incydenty oraz struktury zarządzania bezpieczeństwem. Ponadto przeprowadzany jest przegląd systemów zabezpieczeń, zarówno fizycznych, takich jak kontrola dostępu, jak i cyfrowych, np. firewalli czy systemów SIEM. Ważnym elementem jest także

analiza dotychczasowych incydentów, które mogą wskazywać na istniejące luki w zabezpieczeniach. Rezultatem tego etapu jest kompleksowy raport zawierający mocne i słabe strony aktualnych rozwiązań.

W drugim tygodniu działania skupiają się na identyfikacji i klasyfikacji wykrytych luk w zabezpieczeniach. Luki są oceniane pod względem ich krytyczności i potencjalnego wpływu na funkcjonowanie organizacji. Proces ten obejmuje również analizę zgodności z regulacjami prawnymi oraz wyznaczenie obszarów wymagających pilnych działań. Na zakończenie tego etapu tworzona jest lista priorytetowych luk z przypisanymi poziomami ryzyka i rekomendacjami, które będą podstawą dalszych działań.

Trzeci tydzień harmonogramu obejmuje przygotowanie szczegółowego planu wdrożeniowego. Działania obejmują wyznaczenie kluczowych kamieni milowych, takich jak wdrożenie systemów ochronnych, realizacja szkoleń czy implementacja nowych procedur. Określane są także zasoby niezbędne do realizacji działań, w tym finansowe, technologiczne i ludzkie, oraz przypisywane odpowiedzialności do konkretnych zespołów i liderów projektu. Rezultatem jest szczegółowy plan działań, który określa priorytety oraz harmonogram realizacji kolejnych kroków.

Czwarty tydzień stanowi kluczowy moment harmonogramu, gdyż zakłada przedstawienie opracowanego planu zarządowi organizacji w celu jego formalnego zatwierdzenia. Przygotowywana jest prezentacja podsumowująca wyniki audytu, priorytetyzację luk oraz szczegóły harmonogramu wdrożeniowego, w tym kluczowe wskaźniki efektywności (KPI). Uwagi i sugestie zgłaszane przez decydentów są uwzględniane w finalnej wersji planu. Rezultatem jest oficjalne zatwierdzenie działań oraz alokacja niezbędnych zasobów do realizacji kolejnych etapów.

Harmonogram działań opiera się na przemyślanej sekwencji zadań, gdzie każdy kolejny etap wynika logicznie z poprzedniego. Pierwszy tydzień skupia się na analizie stanu obecnego, co umożliwia określenie priorytetów w drugim tygodniu. W efekcie w trzecim tygodniu opracowywany jest uporządkowany plan, który zostaje zatwierdzony przez zarząd w czwartym tygodniu. Takie podejście umożliwia płynne przejście do realizacji kolejnych etapów wdrażania modelu zarządzania bezpieczeństwem, co gwarantuje skuteczność i zgodność działań z potrzebami organizacji oraz wymaganiami prawnymi.

Cały etap analizy i planowania jest kluczowy dla stworzenia solidnych podstaw pod wdrożenie skutecznego modelu zarządzania bezpieczeństwem, pozwalając na optymalne wykorzystanie dostępnych zasobów oraz zapewnienie zgodności z wymaganiami regulacyjnymi.

Drugi etap wdrożenia modelu zarządzania bezpieczeństwem organizacji skupia się na praktycznej realizacji kluczowych działań mających na celu podniesienie poziomu bezpieczeństwa oraz zapewnienie gotowości do reagowania na potencjalne zagrożenia. Obejmuje on implementację szkoleń, wdrażanie zaawansowanych narzędzi ochronnych oraz ustanowienie procedur weryfikacyjnych. W ramach tego etapu monitoruje się również postępy, co umożliwia bieżącą ocenę skuteczności podejmowanych działań.

Pierwszym podetapem w tym etapie jest organizacja szkoleń, które mają na celu edukację pracowników w zakresie identyfikacji zagrożeń, takich jak phishing czy ataki socjotechniczne. Wykorzystuje się warsztaty, kursy e-learningowe oraz symulacje incydentów, co pozwala na przetestowanie umiejętności w praktycznych warunkach. Dostosowanie szkoleń do różnych grup docelowych, takich jak pracownicy IT czy kadra zarządzająca, zapewnia ich skuteczność. Wynikiem tego działania jest poprawa poziomu wiedzy pracowników, co mierzy się m.in. poprzez wskaźniki zmiany wyników testów wiedzy.

Drugim podetapem jest wdrożenie zaawansowanych narzędzi ochronnych, takich jak systemy SIEM, które umożliwiają monitorowanie oraz szybkie reagowanie na zagrożenia. Wprowadza się również wielopoziomowe uwierzytelnianie (MFA) dla krytycznych systemów oraz modernizuje zabezpieczenia fizyczne, w tym systemy kontroli dostępu i monitoring wizyjny. Te działania są mierzone poprzez wskaźniki modernizacji systemów oraz liczbę skutecznie zneutralizowanych zagrożeń, co pozwala na ocenę ich efektywności.

Trzecim podetapem jest uruchomienie procedur weryfikacyjnych, które obejmują automatyzację procesu sprawdzania pracowników oraz dostawców za pomocą specjalistycznych narzędzi. Regularne audyty dostawców oraz systematyczna weryfikacja nowych pracowników pozwalają na eliminację potencjalnych zagrożeń związanych z ludzkim czynnikiem. Efektywność tego działania monitoruje się przez wskaźniki procentowe zweryfikowanych osób oraz czas trwania weryfikacji, co umożliwia optymalizację procesów.

Czwarty podetap obejmuje systematyczne monitorowanie postępów realizacji harmonogramu oraz analizę wskaźników efektywności (KPI). Dane pozyskiwane z systemów SIEM oraz wyniki szkoleń są podstawą do raportowania do zarządu, co umożliwia identyfikację obszarów wymagających korekt. Czas reakcji na zagrożenia oraz zgodność działań z harmonogramem stanowią kluczowe wskaźniki oceny tego etapu, co pozwala na bieżące dostosowanie strategii wdrożeniowej.

W celu monitorowania postępów i identyfikacji obszarów wymagających poprawy w trakcie realizacji etapu 2, proponuje się wykorzystanie następujących wskaźników przedstawionych w tabeli nr 25.

Tabela 25 Kluczowe wskaźniki dla realizacji etapu 2

Wskaźnik	Podetap	Opis	Znaczenie
Procent przeszkolonych pracowników	1	Mierzy udział pracowników, którzy ukończyli szkolenia	Ocena zasięgu realizacji działań edukacyjnych
Zmiana poziomu wiedzy uczestników szkoleń	1	Różnica między wynikami testów wiedzy przed i po szkoleniu	Ocena skuteczności szkoleń
Procent systemów objętych modernizacją zabezpieczeń	2	Mierzy udział zmodernizowanych systemów w stosunku do wszystkich systemów	Ocenia poziom zabezpieczenia infrastruktury
Liczba zneutralizowanych zagrożeń	2	Liczba skutecznie wykrytych i zneutralizowanych zagrożeń	Ocenia efektywność narzędzi ochronnych
Procent zweryfikowanych pracowników i dostawców	3	Mierzy odsetek osób poddanych weryfikacji	Ocena realizacji procesów weryfikacyjnych
Czas weryfikacji pracowników i dostawców	3	Średni czas potrzebny na weryfikację	Efektywność procesu weryfikacyjnego
Procent działań realizowanych zgodnie z harmonogramem	4	Mierzy stopień zgodności działań z harmonogramem	Monitorowanie postępu prac wdrożeniowych
Czas reakcji na zagrożenia	4	Średni czas potrzebny na wykrycie i neutralizację zagrożenia	Ocena szybkości reagowania na incydenty

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Procent przeszkolonych pracowników (Percentage of trained employees, PTE)

$$PTE = \frac{Liczba\ przeszkolonych\ pracowników}{Całkowita\ liczba\ pracowników} \times 100\%$$

Opis:

Cel: pozwala ocenić stopień realizacji planów szkoleniowych oraz zasięg działań edukacyjnych w organizacji. Wysoki wskaźnik wskazuje na szerokie zaangażowanie pracowników w procesy szkoleniowe,

Interpretacja: jeśli w organizacji zatrudnionych jest 1000 pracowników, a szkolenia ukończyło 750 z nich, wskaźnik wynosi 75%. Oznacza to, że działania szkoleniowe są realizowane, ale konieczne jest dalsze zaangażowanie pozostałych osób.

Zmiana poziomu wiedzy uczestników szkoleń (Knowledge improvement score, KIS)

$$KIS = Średni\ wynik\ testu\ końcowego - Średniw\ wynik\ testu\ początkowego$$

Opis:

Cel: pokazuje, czy przeprowadzone szkolenia były skuteczne i czy pracownicy zrozumieli przekazane informacje. Wysoki wynik wskazuje na skuteczność programów szkoleniowych,

Interpretacja: jeśli średni wynik testu początkowego wynosił 50%, a po szkoleniu wynosi 85%, różnica 35% wskazuje na istotne zwiększenie poziomu wiedzy.

Procent systemów objętych modernizacją zabezpieczeń (Percentage of updated systems, PUS)

$$PUS = \frac{Liczba\ zmodernizowanych\ systemów}{Całkowita\ liczba\ systemów} \times 100\%$$

Opis:

- Cel: pozwala ocenić postęp we wdrażaniu narzędzi ochronnych i poziom zabezpieczenia infrastruktury organizacji. Wyższy wskaźnik wskazuje na lepszą gotowość organizacji do reagowania na zagrożenia,
- Interpretacja: jeśli organizacja posiada 200 systemów IT, z czego 160 zostało zmodernizowanych, wskaźnik wynosi 80%. Oznacza to, że większość infrastruktury została dostosowana do nowych standardów.

Liczba zneutralizowanych zagrożeń w czasie rzeczywistym (Number of neutralized threats, NNT)

$$NNT = \frac{Liczba\ zagrożeń\ wykrytych\ i\ zneutralizowanych}{Całkowita\ liczba\ wykrutych\ zagrożeń} \times 100\%$$

Opis:

Cel: ocenia efektywność wdrożonych narzędzi ochronnych, takich jak systemy SIEM czy firewalle, w ochronie infrastruktury organizacji,

Interpretacja: wysoki wskaźnik (bliski 100%) wskazuje na skuteczność wdrożonych narzędzi bezpieczeństwa, takich jak systemy SIEM (Security Information and Event Management), firewalle czy narzędzia IDS/IPS (Intrusion Detection/Prevention Systems). Niski wskaźnik może wskazywać na braki w konfiguracji systemów ochronnych, niewystarczającą szybkość reakcji lub nieadekwatność stosowanych technologii w stosunku do charakteru zagrożeń.

Procent zweryfikowanych pracowników i dostawców (Percentage of verified employees and suppliers, PVES)

$$PVES = \frac{Liczba\ zweryfikowanych\ osób}{Całkowita\ liczba\ osób\ wymagających\ weryfikacji} \times 100\%$$

Opis:

Cel: pozwala ocenić, w jakim stopniu organizacja realizuje procesy weryfikacyjne, które są kluczowe dla minimalizacji ryzyka wewnętrznego i zewnętrznego,

Interpretacja: jeśli z 500 pracowników i dostawców, którzy powinni zostać zweryfikowani, proces przeszedł 350 osób, wskaźnik wynosi 70%. Należy skupić się na weryfikacji pozostałych 30%.

Czas weryfikacji pracowników i dostawców (Verification time, VT)

$$VT = \frac{Łączny\ czas\ weryfikacji\ (godziny/dni)}{Liczba\ zweryfikowanych\ osób\ (pracowmników/dostawców)}$$

Opis:

Cel: ocenia efektywność i szybkość realizacji procedur weryfikacyjnych. Krótszy czas wskazuje na bardziej wydajny proces,

Interpretacja: niski wskaźnik VT wskazuje na wysoką efektywność procesu weryfikacyjnego. Może również sugerować dobrą automatyzację i organizację pracy. Wysoki wskaźnik VT może świadczyć o skomplikowanych procedurach, niedostatecznej liczbie zasobów lub braku odpowiednich narzędzi wspierających weryfikację.

Procent działań realizowanych zgodnie z harmonogramem (Schedule adherence rate, SAR)

$$SAR = \frac{Zrealizowane\ działania}{Działania\ zaplanowane} \times 100\%$$

Opis:

Cel: pozwala monitorować postęp prac i identyfikować obszary, w których mogą wystąpić opóźnienia. Wyższy wskaźnik wskazuje na dobrą organizację działań,

Interpretacja: jeśli zaplanowano 20 działań na dany tydzień, a zrealizowano 18, wskaźnik wynosi 90%. Organizacja może ocenić, czy brakujące 10% wymaga dodatkowych zasobów lub interwencji.

Czas reakcji na zagrożenia (Threat response time, TRT)

$$TRT = \frac{Suma\ czasu\ reakcji\ na\ wszystkie\ zagrożenia\ (minuty/godziny)}{Liczba\ obsłużonych\ zagrożeń}$$

Opis:

Cel: jest kluczowym wskaźnikiem efektywności systemów ochronnych i gotowości organizacji do szybkiego reagowania na incydenty,

Interpretacja: niski wskaźnik TRT oznacza szybkie i sprawne reagowanie na zagrożenia, co świadczy o efektywności systemów bezpieczeństwa oraz dobrze zorganizowanych procedurach. Wysoki wskaźnik TRT może wskazywać na problemy w procesie reakcji, takie jak niewydolność systemów monitorujących, brak zasobów ludzkich lub brak jasno określonych procedur.

Każdy z tych wskaźników pełni kluczową rolę w monitorowaniu efektywności wdrożenia modelu zarządzania bezpieczeństwem w organizacji. Regularne mierzenie i analiza tych wskaźników zapewniają pełną kontrolę nad postępami prac oraz umożliwiają wprowadzanie działań korygujących.

Na potrzeby wdrożenia etapu 2 przygotowano przykładowy harmonogram przedstawiony w tabeli nr 26.

Tabela 26 Przykładowy harmonogram wdrożenia etapu 2

Tydzień	Działanie	Opis	Odpowiedzialny
1	Implementacja szkoleń	Organizacja warsztatów i uruchomienie kursów online	Zespół ds. szkoleń
2	Wdrożenie narzędzi ochronnych	Konfiguracja systemów SIEM i MFA	Dział IT
3	Uruchomienie procedur weryfikacyjnych	Wdrożenie narzędzi do sprawdzania przeszłości	Dział HR
4	Monitorowanie postępów	Analiza wyników KPI i raportowanie	Menedżer projektu

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Harmonogram realizacji drugiego etapu wdrożenia modelu zarządzania bezpieczeństwem organizacji został podzielony na cztery tygodniowe cykle, z jasno określonym zakresem działań i przypisaniem odpowiedzialności odpowiednim zespołom. Strukturalne podejście umożliwia efektywne wykorzystanie dostępnych zasobów oraz monitorowanie postępów w czasie rzeczywistym, co pozwala na bieżące podejmowanie decyzji korygujących w przypadku potrzeby.

Pierwszy tydzień harmonogramu skupia się na implementacji szkoleń, które mają na celu zwiększenie świadomości pracowników w zakresie identyfikacji i przeciwdziałania zagrożeniom bezpieczeństwa. Działania obejmują organizację warsztatów, wdrożenie kursów e-learningowych oraz przeprowadzanie sesji edukacyjnych dostosowanych do specyfiki różnych grup docelowych, takich jak zespoły IT, kadra kierownicza i kontrahenci. Efektem tych działań jest lepsza świadomość zagrożeń oraz przygotowanie uczestników do skutecznego reagowania na potencjalne incydenty.

Drugi tydzień harmonogramu poświęcony jest wdrażaniu i optymalizacji narzędzi ochronnych, zarówno cyfrowych, jak i fizycznych. Działania obejmują implementację systemów SIEM, konfigurację wielopoziomowego uwierzytelniania (MFA) oraz instalację zabezpieczeń fizycznych, takich jak systemy kontroli dostępu i monitoring wizyjny. Testowanie nowych rozwiązań w środowisku produkcyjnym pozwala na identyfikację obszarów wymagających optymalizacji. W rezultacie organizacja zyskuje większą odporność na zagrożenia oraz lepszą kontrolę dostępu do zasobów krytycznych.

Trzeci tydzień koncentruje się na wdrożeniu ustandaryzowanych procedur weryfikacyjnych. Działania te obejmują zastosowanie automatycznych systemów do sprawdzania pracowników i dostawców, takich jak HireRight, oraz regularne przeprowadzanie audytów dostawców w celu zapewnienia zgodności z politykami bezpieczeństwa organizacji. Harmonogram obejmuje również ustanowienie regularnych cykli weryfikacyjnych dla nowych

i obecnych pracowników. Rezultatem jest minimalizacja ryzyka związanego z zagrożeniami wewnętrznymi i zewnętrznymi oraz ujednolicenie procesów kontroli.

Czwarty tydzień zakłada systematyczne monitorowanie postępów działań wdrożeniowych oraz analizę efektywności wdrożonych rozwiązań. Główne działania obejmują przygotowanie raportów dla zarządu na podstawie kluczowych wskaźników efektywności (KPI), takich jak odsetek przeszkolonych pracowników czy czas reakcji na zagrożenia. Na podstawie tych danych identyfikuje się obszary wymagające działań korygujących oraz opracowuje strategie ich implementacji.

Harmonogram Etapu 2 stanowi spójny i uporządkowany plan działań, który umożliwia realizację nadrzędnego celu, jakim jest zwiększenie poziomu bezpieczeństwa organizacji. Każdy tydzień realizacji w sposób konsekwentny buduje fundament dla poprawy bezpieczeństwa operacyjnego. Regularne monitorowanie postępów oraz zastosowanie wskaźników KPI pozwala na pełną kontrolę nad procesem wdrożeniowym, a także na szybkie reagowanie w przypadku wystąpienia niezgodności z założeniami.

Etap wdrożenia i realizacji, poprzez synergiczne działania szkoleniowe, techniczne oraz kontrolne, umożliwia organizacji skuteczne budowanie odporności na zagrożenia. Systematyczna realizacja działań w ramach jasno określonych procedur i harmonogramów pozwala na osiągnięcie zgodności z przyjętym modelem zarządzania bezpieczeństwem oraz zwiększenie efektywności funkcjonowania organizacji w obszarze ochrony danych i zasobów.

Etap ten, integrując wielowymiarowe działania i opierając się na bieżącej analizie wyników, stanowi fundament dla skutecznego zarządzania bezpieczeństwem organizacji. Podnosi poziom gotowości organizacji na wypadek wystąpienia incydentów, a jednocześnie pozwala na ciągłe doskonalenie strategii ochrony w dynamicznie zmieniającym się otoczeniu biznesowym i technologicznym.

Trzeci etap procesu wdrażania modelu zarządzania bezpieczeństwem koncentruje się na ocenie efektywności zastosowanych rozwiązań oraz ich ciągłym doskonaleniu. Kluczowym celem tego etapu jest utrzymanie wysokiego poziomu gotowości organizacji na dynamicznie zmieniające się zagrożenia oraz dostosowywanie się do nowych wymagań regulacyjnych i technologicznych. Proces ten wspiera systematyczna ewaluacja oraz odpowiedzialne podejście do poprawy zidentyfikowanych obszarów.

Pierwszym podetapem (1) jest regularne monitorowanie wskaźników efektywności (KPI), co obejmuje analizę danych operacyjnych, takich jak raporty z systemów SIEM, logi incydentów oraz wyniki audytów. Istotne jest także systematyczne porównywanie bieżących wyników z wcześniej ustalonymi wskaźnikami, co pozwala ocenić skuteczność działań, np. czas reakcji na zagrożenia (TRT) czy realizację harmonogramu. Analiza trendów w danych

umożliwia identyfikację potencjalnych problemów oraz obszarów wymagających interwencji, co skutkuje przygotowaniem raportów z wynikami oraz wskazaniami do dalszych działań doskonalących.

Kolejnym podetapem (2) jest przeprowadzenie szczegółowych audytów, zarówno wewnętrznych, jak i zewnętrznych, w celu oceny zgodności wdrożonych działań z regulacjami. Działania te są uzupełniane o benchmarking, który porównuje wyniki organizacji z najlepszymi praktykami branżowymi oraz osiągnięciami konkurencji. Dzięki temu możliwe jest określenie niezgodności oraz identyfikacja luk w istniejącym systemie, co przekłada się na stworzenie listy rekomendacji, mających na celu zwiększenie skuteczności systemu zarządzania bezpieczeństwem.

Zidentyfikowane podczas audytów i benchmarkingu problemy wymagają opracowania działań korygujących. (podetap 3) W tym kontekście istotne jest zaplanowanie i wdrożenie rozwiązań eliminujących wykryte niedoskonałości, takich jak dodatkowe szkolenia dla pracowników czy zmiana konfiguracji systemów zabezpieczających. Jednocześnie działania doskonalące, ukierunkowane na wprowadzenie nowych standardów lub technologii, zapewniają ciągłe podnoszenie poziomu bezpieczeństwa. Rezultaty tych działań są monitorowane w celu oceny ich efektywności oraz dostosowania przyszłych strategii.

Zastosowanie wskaźników efektywności umożliwia precyzyjne monitorowanie postępów w realizacji działań korygujących i doskonalących (podetap 4). Kluczowe wskaźniki obejmują m.in. procent zrealizowanych działań korygujących oraz czas potrzebny na ich ukończenie. Te mierniki pozwalają nie tylko na bieżące śledzenie realizacji celów, ale także na ocenę skuteczności podejmowanych działań oraz identyfikację obszarów wymagających dalszych usprawnień.

W celu monitorowania postępów i identyfikacji obszarów wymagających poprawy w trakcie realizacji etapu 3, proponuje się wykorzystanie następujących wskaźników przedstawionych w tabeli nr 27.

Tabela 27 Kluczowe wskaźniki dla realizacji etapu 3

Wskaźnik	Podetap	Opis	Znaczenie
Procent realizacji wskaźników KPI	1	Ocena skuteczności realizacji wyznaczonych celów	Wysoki wskaźnik świadczy o efektywnym wdrożeniu
Procent poprawy wyników KPI	1	Monitorowanie wzrostu efektywności działań	Wzrost wskazuje na poprawę procesów
Procent zgodności z regulacjami	2	Ocena przestrzegania wymagań prawnych i standardów	Niski wskaźnik wskazuje na ryzyko niezgodności

Wskaźnik	Podetap	Opis	Znaczenie
Procent niezgodności wykrytych podczas audytu	2	Identyfikacja obszarów wymagających poprawy	Wysoki wskaźnik wymaga pilnych działań korygujących
Procent zrealizowanych działań korygujących	3	Monitorowanie efektywności wprowadzanych poprawek	Niski wskaźnik oznacza opóźnienia w działaniach
Czas realizacji działań korygujących	3	Ocena szybkości realizacji działań korygujących	Długi czas może wskazywać na brak zasobów

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Procent realizacji wskaźników KPI (Percentage of achieved KPIs, PAK)

$$PAK = \frac{Liczba\ osiągniętych\ wskaźników}{Całkowita\ liczba\ zdefiniowanych\ wskaźników} \times 100\%$$

Opis:

Cel: ocena skuteczności realizacji kluczowych celów wyznaczonych dla wdrożenia działań w systemie zarządzania bezpieczeństwem,

Interpretacja: wysoki wynik (bliski 100%) wskazuje na skuteczną realizację założeń wdrożenia. Niski wynik sugeruje, że istnieją obszary wymagające interwencji i poprawy w procesach zarządzania

Procent poprawy wyników KPI względem poprzedniego okresu (Improvement in KPI performance, IKP)

$$IKP = \frac{Wynik\ obecny - Wynik\ poprzedni}{Wynik\ poprzedni} \times 100\%$$

Opis:

Cel: zapewnienie ciągłej poprawy w systemie zarządzania bezpieczeństwem poprzez ocenę zmian w wynikach kluczowych wskaźników,

Interpretacja: wzrost wskaźnika wskazuje na poprawę efektywności działań. Spadek wskaźnika może sygnalizować nowe problemy lub nieskuteczność wdrożonych działań.

Procent zgodności z regulacjami (Compliance rate, CR)

$$CR = \frac{Liczba\ zgodnych\ wymagań}{Całkowita\ liczba\ wymagań} \times 100\%$$

Opis:

Cel: zapewnienie, że działania organizacji są zgodne z obowiązującymi przepisami i wymaganiami, co minimalizuje ryzyko prawne i reputacyjne,

Interpretacja: wysoki wskaźnik (bliski 100%) świadczy o pełnej zgodności z wymaganiami. Niski wskaźnik wskazuje na potencjalne ryzyka związane z niezgodnością.

Procent niezgodności wykrytych podczas audytu (Non-compliance rate, NCR)

$$NCR = \frac{Liczba\ wykrytych\ niezgodności}{Całkowita\ liczba\ audytowanych\ obszarów} \times 100\%$$

Opis:

Cel: identyfikacja luk w systemie zarządzania bezpieczeństwem i określenie zakresu działań korygujących,

Interpretacja: wysoki wskaźnik wskazuje na potrzebę pilnych działań korygujących. Niski wskaźnik świadczy o wysokim poziomie zgodności z założeniami i standardami.

Procent zrealizowanych działań korygujących (Corrective actions completion rate CACR)

$$CACR = \frac{Liczba\ zrealizowanych\ działań\ korygujących}{Całkowita\ liczba\ działań\ korygujących} \times 100\%$$

Opis:

Cel: ocena skuteczności realizacji działań naprawczych w odpowiedzi na wykryte niezgodności,

Interpretacja: wysoki wskaźnik wskazuje na efektywność działań korygujących. Niski wskaźnik może oznaczać opóźnienia w realizacji działań lub niewystarczające zasoby.

Czas realizacji działań korygujących (Time to complete corrective actions, TCCA)

$$TCCA = \frac{Czas\ realizacji\ działań\ korygujących\ (dni/godziny)}{Liczba\ zrealizowanych\ działań\ korygujących}$$

Opis:

Cel: ocena szybkości, z jaką organizacja wprowadza niezbędne poprawki w odpowiedzi na wykryte problemy,

Interpretacja: krótki czas realizacji wskazuje na wysoką zdolność organizacji do szybkiego reagowania na wykryte problemy. Długi czas realizacji może sugerować problemy z zasobami lub złożoność działań korygujących.

Każdy z tych wskaźników pełni kluczową rolę w monitorowaniu efektywności wdrożenia modelu zarządzania bezpieczeństwem w organizacji. Regularne mierzenie i analiza tych wskaźników zapewniają pełną kontrolę nad postępami prac oraz umożliwiają wprowadzanie działań korygujących.

Na potrzeby wdrożenia etapu 3 przygotowano przykładowy harmonogram przedstawiony w tabeli nr 28.

Tabela 28 Przykładowy harmonogram wdrożenia etapu 3

Tydzień	Działanie	Opis	Odpowiedzialny
1	Monitoring wskaźników efektywności	Analiza danych operacyjnych i wyników KPI	Zespół ds. analizy danych
2	Audyt i benchmarking	Audyt wewnętrzny i porównanie z najlepszymi praktykami	Dział audytu
3	Planowanie działań korygujących	Przygotowanie listy działań naprawczych	Menedżer ds. bezpieczeństwa
4	Wdrożenie działań korygujących	Realizacja działań naprawczych i doskonalących	Zespół projektowy

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Podział harmonogramu na cztery tygodniowe cykle działań stanowi podstawę systematycznego podejścia do ewaluacji i doskonalenia systemu zarządzania bezpieczeństwem. Kluczowe etapy obejmują monitoring wskaźników efektywności, audyt i benchmarking, planowanie działań korygujących oraz ich wdrożenie. Taka struktura pozwala na efektywne wykorzystanie zasobów organizacyjnych oraz maksymalizację osiąganych rezultatów, wspierając proces adaptacji organizacji do dynamicznych zmian w otoczeniu.

Pierwszy tydzień cyklu koncentruje się na analizie danych operacyjnych pochodzących z zaawansowanych systemów, takich jak SIEM, logi incydentów czy wyniki audytów. Monitorowane są kluczowe wskaźniki efektywności (KPI), w tym czas reakcji na zagrożenia

(TRT) oraz liczba zneutralizowanych zagrożeń w czasie rzeczywistym (NNT). Narzędzia analityczne wspierają identyfikację trendów i anomalii, co umożliwia organizacji bieżącą ocenę skuteczności działań. Rezultatem tego etapu jest szczegółowy raport z bieżącego stanu KPI, który stanowi fundament dla planowania kolejnych działań.

Drugi tydzień obejmuje audyt wewnętrzny i zewnętrzny, których celem jest ocena zgodności wdrożonych działań z regulacjami prawnymi oraz standardami organizacyjnymi. Benchmarking wyników z najlepszymi praktykami branżowymi oraz porównanie z osiągnięciami konkurencji dostarczają obiektywnej perspektywy na skuteczność procesów. Efektem działań audytowych jest raport wskazujący mocne strony systemu oraz obszary wymagające poprawy. Na tej podstawie opracowywane są rekomendacje mające na celu dalszą optymalizację systemu zarządzania bezpieczeństwem.

Trzeci tydzień skupia się na opracowaniu planu działań, który uwzględnia wyniki wcześniejszych etapów. Lista działań korygujących może obejmować wprowadzenie dodatkowych szkoleń, modernizację systemów zabezpieczeń czy aktualizację procedur. Jednocześnie planowane są inicjatywy doskonalące, takie jak wdrażanie nowych technologii lub reorganizacja procesów. Kluczowym elementem tego etapu jest określenie harmonogramu działań oraz przypisanie odpowiedzialności zespołom, co zapewnia jasność w realizacji założonych celów. Rezultatem jest zatwierdzony plan działań z określonymi ramami czasowymi i alokacją zasobów.

Czwarty tydzień obejmuje realizację zaplanowanych działań, zarówno korygujących, jak i doskonalących. Kluczowym elementem jest bieżące monitorowanie efektów wdrożonych zmian oraz ocena ich skuteczności. Przygotowywany raport końcowy podsumowuje efekty zrealizowanych działań i wskazuje na osiągnięte rezultaty, takie jak poprawa wskaźników KPI, zwiększenie zgodności z regulacjami oraz wzrost odporności organizacji na potencjalne zagrożenia.

Harmonogram wdrożenia Etapu 3 odzwierciedla systematyczne podejście do oceny i doskonalenia systemu zarządzania bezpieczeństwem. Kluczową rolę odgrywa analiza wskaźników efektywności, przeprowadzanie audytów oraz wdrażanie działań naprawczych i ulepszających. Regularne monitorowanie i benchmarking umożliwiają dynamiczne reagowanie na zmieniające się warunki, co pozwala organizacji na skuteczne zarządzanie bezpieczeństwem i minimalizację ryzyka w długoterminowej perspektywie.

Podsumowując, etap ewaluacji i doskonalenia systemu zarządzania bezpieczeństwem stanowi kluczowy element długoterminowej strategii organizacji. Dzięki regularnej analizie danych, audytom, benchmarkingu oraz wdrażaniu działań korygujących i doskonalących, organizacja jest w stanie dynamicznie reagować na zmieniające się warunki otoczenia. To

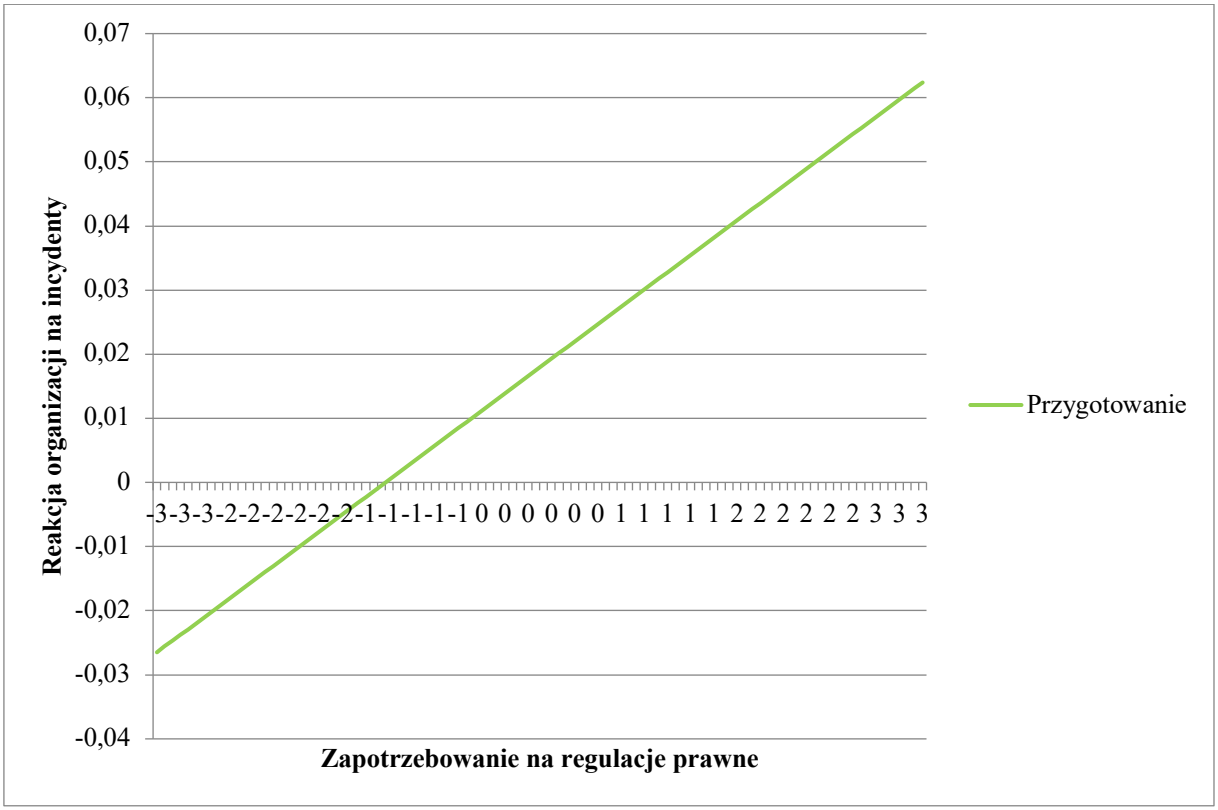
podejście umożliwia nie tylko minimalizację ryzyka, ale także zwiększenie odporności na przyszłe zagrożenia. Rezultaty tych działań potwierdzają skuteczność systemu zarządzania bezpieczeństwem oraz stanowią podstawę dla jego dalszego rozwoju.

6.2 Symulacja procedury wdrożenia modelu w strukturze organizacyjnej

Biorąc pod uwagę główne założenia przewidziane w modelu, które mają zwiększyć poziom przygotowania na incydenty bezpieczeństwa w kontekście zagrożenia szpiegostwem korporacyjnym, postanowiono przeprowadzić symulację komputerową. W celu przeprowadzenia symulacji modelu zarządzania bezpieczeństwem w sektorze ICT wykorzystano oprogramowanie AnyLogic, które umożliwia implementację złożonych modeli opartych na agentach. Zastosowanie tego narzędzia pozwoliło na dynamiczną analizę interakcji między kluczowymi komponentami systemu, w tym pracownikami, dostawcami i organizacją, co przyczyniło się do lepszego zrozumienia zależności w badanym środowisku.

Przedmiotowa symulacja miała na celu przedstawienie potencjalnych ścieżek implementacji modelu w ramach struktury organizacyjnej, mając na uwadze główne cechy modelu, tj. znaczenie szkoleń instytucji państwowych, postrzeganie szpiegostwa korporacyjnego jako zagrożenia, zapotrzebowanie na regulacje prawne, ocena wystarczalności szkoleń i profilaktyki, ocena kontroli przeszłości pracowników i dostawców, ocena środków ochronnych, wystarczalność zabezpieczeń fizycznych i cyfrowych oraz skuteczność regulacji w wykrywaniu szpiegostwa.

Wobec powyższego skupiono się na dalszej analizie trzech głównych czynników, które są bezpośrednio zależne od organizacji – zapotrzebowania na regulacje prawne dotyczące szpiegostwa korporacyjnego, znaczenia szkoleń instytucji państwowych oraz postrzegania szpiegostwa jako zagrożenia. Na wykresie nr 20 przedstawiono wpływ zapotrzebowania na regulacje prawne na poziom przygotowanie organizacji do reagowania na incydenty.

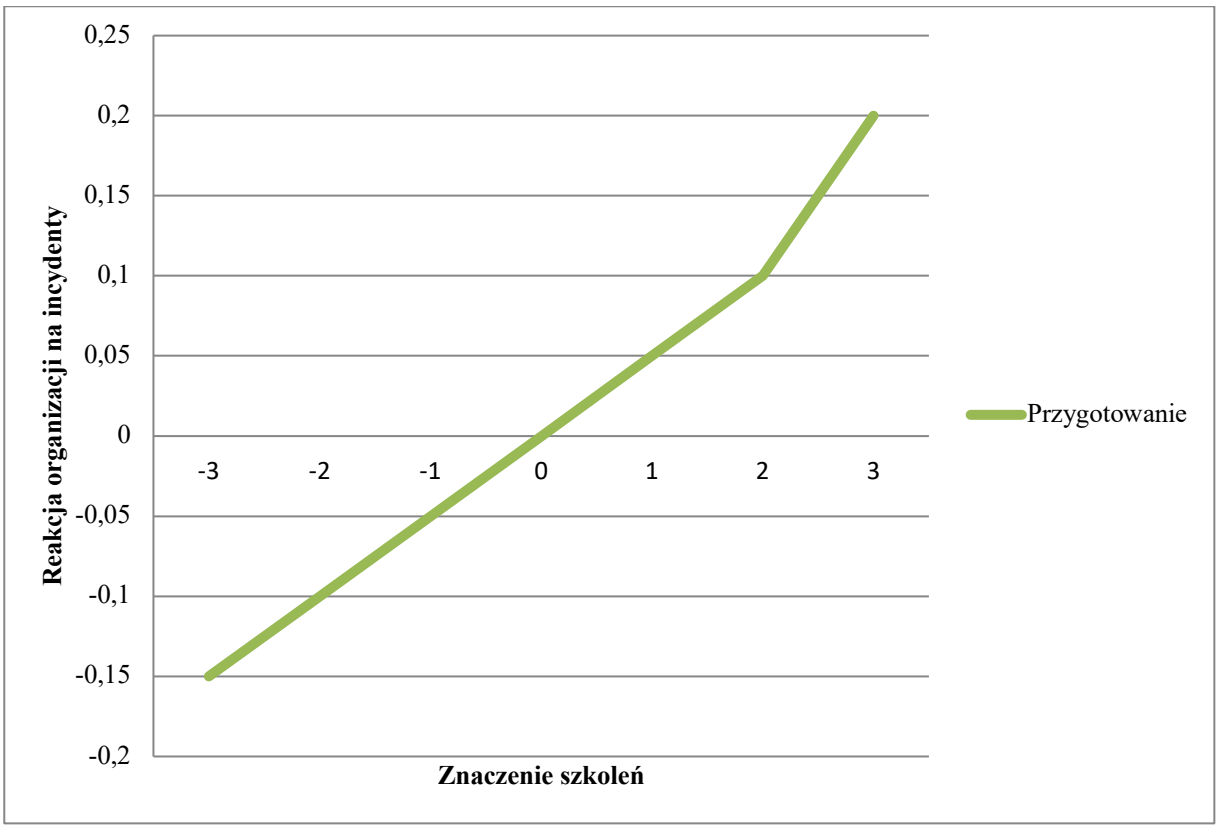


Wykres 20 Wpływ zapotrzebowania na regulacje prawne na poziom przygotowania organizacji do reagowania na incydenty

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Wykres liniowy ilustruje relację pomiędzy zapotrzebowaniem na regulacje prawne a poziomem przygotowania organizacji do reagowania na incydenty. Wraz ze wzrostem zapotrzebowania na regulacje prawne (od -3 do +3 odchyleń standardowych), poziom przygotowania do reagowania na incydenty ulega poprawie. Zjawisko to odzwierciedla istotną rolę ram prawnych w tworzeniu środowiska sprzyjającego gotowości organizacyjnej do przeciwdziałania zagrożeniom związanym ze szpiegostwem. Trend liniowy wskazuje, że zwiększenie regulacji prawnych konsekwentnie podnosi poziom przygotowania, jednak wielkość tego efektu może się różnić w zależności od innych czynników, takich jak adekwatność szkoleń czy kontrola przeszłości pracowników.

Na podstawie dokonanych sprawdzeń, uzyskano następujące wyniki, dotyczące wpływu znaczenia szkoleń na poziom przygotowania organizacji do reagowania na incydenty, które przedstawiono na wykresie nr 21.



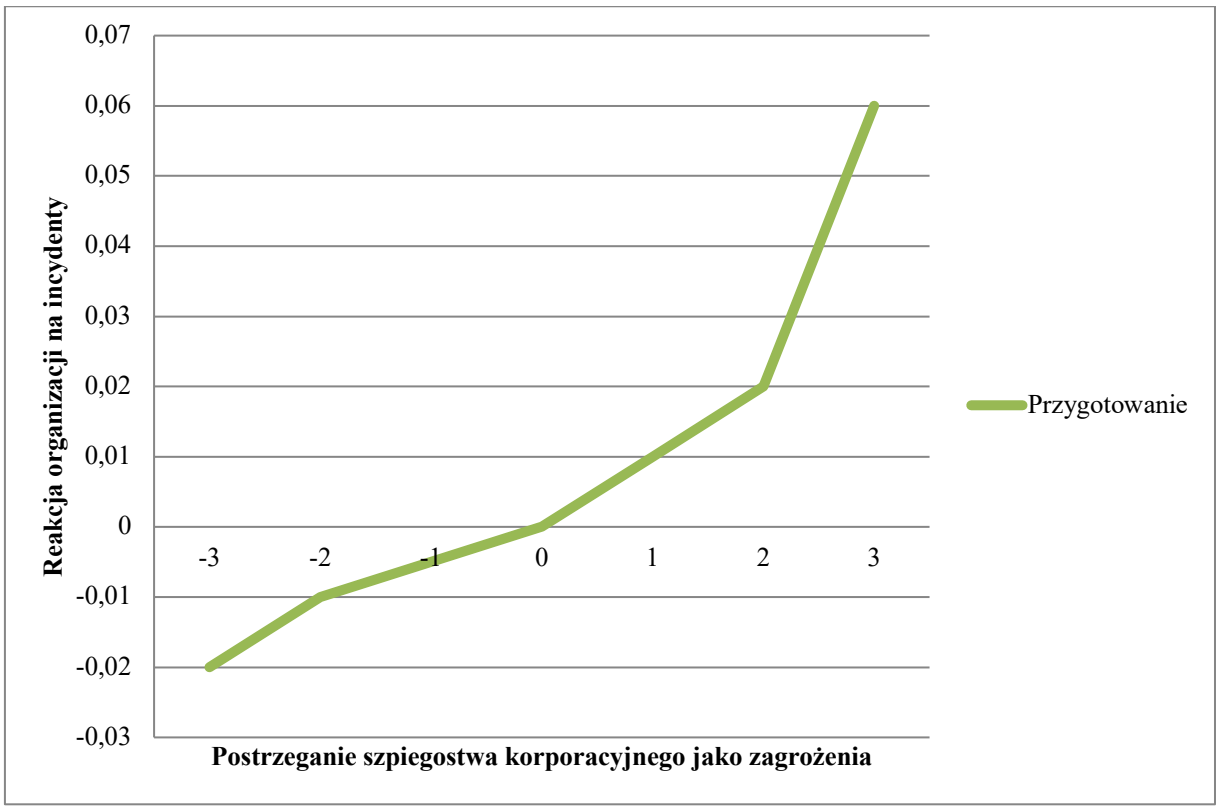
Wykres 21 Wpływ znaczenia szkoleń na poziom przygotowania organizacji do reagowania na incydenty

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Wykres przedstawia, w jaki sposób zmiany w **ocenie znaczenia szkoleń** wpływają na **gotowość organizacji do reagowania na incydenty**. Wraz ze wzrostem adekwatności szkoleń (mierzonej w odchyleniach standardowych), **gotowość** rośnie w sposób liniowy. Sugeruje to, że poprawa postrzegania adekwatności szkoleń pozytywnie wpływa na przygotowanie organizacji do radzenia sobie z incydentami szpiegowskimi.

Wyższa **ocena znaczenia szkoleń** koreluje z większą **gotowością organizacji do reagowania na incydenty**. Oznacza to, że organizacje koncentrujące się na poprawie szkoleń i działań prewencyjnych są bardziej przygotowane do reagowania na zagrożenia szpiegowskie, Relacja ta ma charakter liniowy, co wskazuje na konsekwentny wzrost **gotowości organizacji do reagowania na incydenty** wraz z poprawą **znaczenia szkoleń**.

Następnie, w sposób analogiczny dokonano analizy postrzegania szpiegostwa korporacyjnego jako zagrożenia w kontekście gotowości organizacji do reagowania na incydenty. Wyniki przedstawiono na wykresie nr 22.



Wykres 22 Wpływ postrzegania szpiegostwa korporacyjnego jako zagrożenia na poziom przygotowania organizacji do reagowania na incydenty
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Wraz ze wzrostem **postrzegania szpiegostwa korporacyjnego jako zagrożenia** (mierzonego w odchyleniach standardowych), **gotowość organizacji do reagowania na incydenty** również wzrasta, choć efekt ten jest umiarkowany. Liniowa relacja wskazuje, że zwiększona świadomość zagrożenia ze strony szpiegostwa korporacyjnego prowadzi do nieznacznie lepszego przygotowania, jednak wpływ ten nie jest tak silny, jak w przypadku czynników bezpośrednio związanych z działaniami ochronnymi.

Porównując powyższe z **oceną znaczenia szkoleń**, wpływ **postrzegania szpiegostwa korporacyjnego jako zagrożenia** na **gotowość organizacji do reagowania na incydenty** jest relatywnie mniejszy. Wskazuje to, że choć świadomość zagrożeń jest istotna, konkretne ulepszenia w zakresie szkoleń i środków ochronnych mają silniejszy wpływ na poziom gotowości organizacji.

Następnie, na podstawie wyników poszczególnych elementów, zobrazowanych w podrozdziale 5.4 dysertacji, przygotowano skalę gotowości organizacji do reagowania na incydenty szpiegostwa korporacyjnego. Przedmiotowa skala ma charakter numeryczny i obejmuje wartości od 0 do 1,100. Poniżej przedstawiono podstawy konstrukcji i interpretacji tej skali:

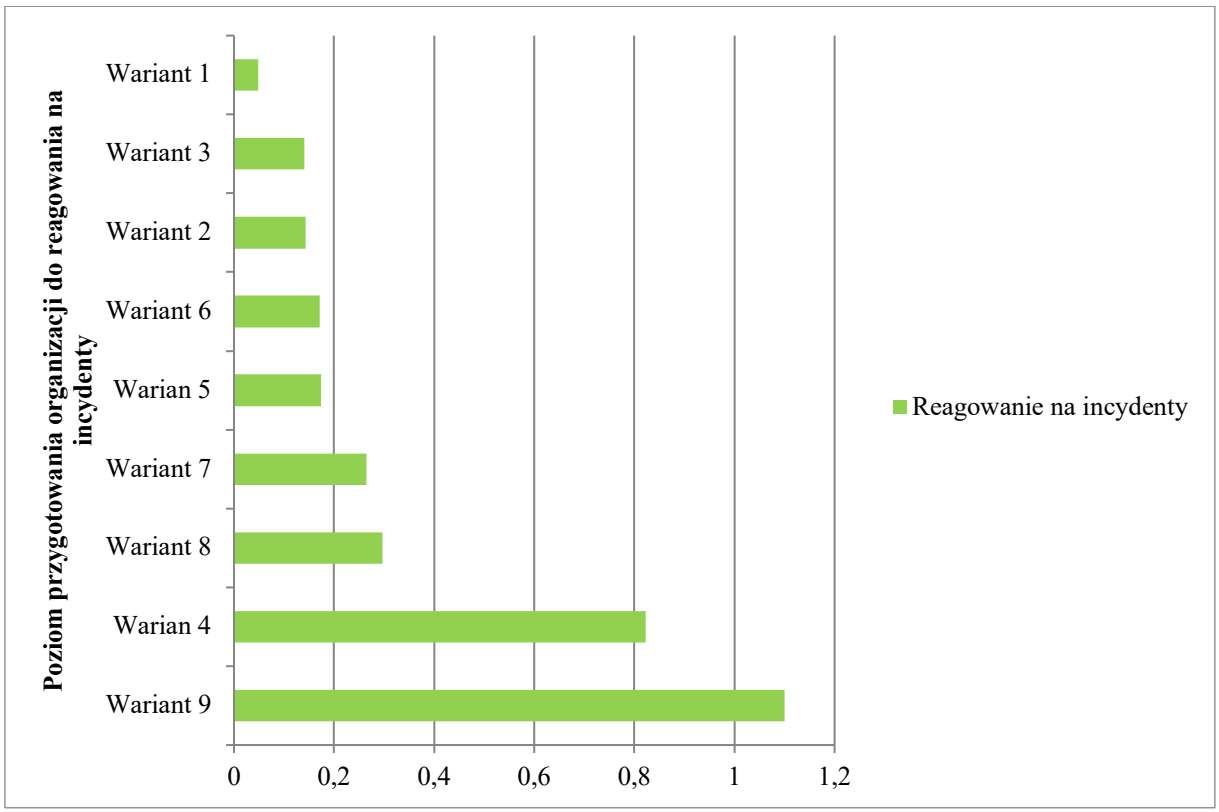
1. Podstawa konstrukcji skali

a. Analiza wpływu wariantów:
    i. gotowość do reagowania na incydenty dla każdej ścieżki obliczono na podstawie kombinacji trzech wskaźników oraz ich względnego wkładu w poprawę gotowości,
    ii. wpływ na poziom gotowości mają współczynniki oraz jakościowe dane.

2. Kluczowe zmienne uwzględnione:
    a. znaczenie szkoleń instytucji państwowych,
    b. postrzeganie szpiegostwa korporacyjnego jako zagrożenia,
    c. zapotrzebowanie na regulacje prawne,
    d. ocena wystarczalności szkoleń i profilaktyki,
    e. ocena kontroli przeszłości pracowników i dostawców,
    f. ocena środków ochronnych,
    g. wystarczalność zabezpieczeń fizycznych i cyfrowych,
    h. skuteczność regulacji w wykrywaniu szpiegostwa.
3. Definicja zakresów:
    a. minimalny poziom (0,049): reprezentuje podejście reaktywne i minimalne, koncentrujące się wyłącznie na świadomości zagrożeń, bez wprowadzania zmian strukturalnych lub działań prewencyjnych,
    b. maksymalny poziom (1,100): odzwierciedla w pełni zintegrowane i kompleksowe podejście, obejmujące wszystkie kluczowe czynniki: percepcję zagrożeń, szkolenia, weryfikację pracowników oraz zabezpieczenia fizyczne i cyfrowe.
4. Poziomy gotowości na skali:
    a. 0,00 – 0,25 (Niska gotowość),
    b. 0,26 – 0,50 (Umiarkowana gotowość),
    c. 0,51 – 0,75 (Wysoka gotowość),
    d. 0,76 – 1,10 (Optymalna gotowość):

Skala gotowości reagowania organizacji na incydenty jest narzędziem umożliwiającym ocenę zdolności przedsiębiorstwa do reagowania na zagrożenia związane ze szpiegostwem korporacyjnym.

Wobec powyższego, przygotowano 9 wariantów wdrożenia modelu zarządzania bezpieczeństwem organizacji, przy których wykorzystaniu, przedsiębiorstwo może zwiększać swój poziom reagowania na incydenty. Przedmiotowe warianty przedstawiono na wykresie nr 23.



Wykres 23 Warianty wdrożenia modelu zarządzania bezpieczeństwem organizacji i ich wpływ na poziom reagowania na incydenty

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Wariant 1 polega na skupieniu się wyłącznie na zwiększeniu percepcji pracowników w kontekście szpiegostwa korporacyjnego. Wdrożenie tego wariantu obejmuje przeprowadzenie regularnych kampanii dotyczących uświadamiania pracowników przy wykorzystaniu studium przypadków zdarzeń, które miały miejsce w rzeczywistości, aktualizację krajobrazu zagrożeń oraz wykorzystanie ankiet pracowniczych do oceny poziomu percepcji zagrożeń.

Zastosowanie omawianego wariantu niesie ze sobą szereg korzyści dla organizacji. Przede wszystkim przyczynia się do zwiększenia poziomu świadomości pracowników w zakresie identyfikacji podejrzanych działań lub zachowań, co pozwala na wczesne wykrywanie potencjalnych zagrożeń. Ponadto, wdrożenie tego podejścia wspiera rozwój kultury organizacyjnej, opartej na ostrożności i odpowiedzialności, w której pracownicy postrzegają siebie jako istotnych uczestników procesu ochrony organizacji. Dodatkowo, budowanie świadomości zagrożeń staje się solidną podstawą do wprowadzania bardziej zaawansowanych działań, takich jak programy szkoleniowe czy kompleksowe systemy bezpieczeństwa.

Jednakże, wariant ten ma również swoje ograniczenia. Jego kluczową słabością jest dominująco reaktywne podejście, które mimo rozpoznawania zagrożeń nie obejmuje

aktywnych działań prewencyjnych. Pracownicy, choć świadomi ryzyk, mogą nie posiadać wystarczających narzędzi lub wiedzy, aby skutecznie na nie reagować. Wariant charakteryzuje się również niskim poziomem gotowości operacyjnej (0,049), wynikającym z braku zmian strukturalnych i operacyjnych w zabezpieczeniach. Dodatkowo, skuteczność wdrożenia w dużej mierze zależy od stopnia zaangażowania pracowników oraz ich chęci do zgłaszania i przeciwdziałania potencjalnym zagrożeniom, co czyni sukces inicjatywy zależnym od czynników ludzkich.

Wykorzystanie wariantu nr 1 przez organizacje może nastąpić w przypadku, gdy przedsiębiorstwo jest zainteresowane wykorzystaniem niskokosztowego sposobu na budowanie podstawowej świadomości. Ponadto, wariant ten może stanowić punkt wyjścia do wdrożenia bardziej kompleksowych działań, takich jak szkolenia czy inwestycje w systemy bezpieczeństwa.

W celu zwiększenia skuteczności wariantu 1, organizacje mogą połączyć działania zwiększające świadomość zagrożeń z podstawowymi modułami szkoleniowymi oraz stosować systemy motywacyjne w celu zachęcenia pracowników do aktywnego uczestnictwa w kampaniach podnoszących świadomość.

Wariant 2 polega na wykorzystaniu kompleksowych szkoleń w zakresie bezpieczeństwa i gotowości do reagowania na incydenty. Wdrożenie tego wariantu obejmuje opracowanie modułów szkoleniowych dostosowanych do konkretnych ról i koncentrujących się na identyfikacji i reagowaniu na incydenty. Następnie wymaga organizowania regularnych szkoleń przypominających w celu utrwalenia wiedzy oraz prowadzenia ćwiczeń praktycznych przy wykorzystaniu symulacji. Ograniczenia związane z implementacją tego wariantu dotyczą przede wszystkim kosztów oraz czasu niezbędnego do opracowania i wdrożenia kompleksowego programu szkoleniowego. Przygotowanie takiego programu wymaga znacznych nakładów finansowych oraz organizacyjnych, co może być wyzwaniem dla przedsiębiorstw o ograniczonych zasobach. Dodatkowo, skuteczność Wariantu 2 jest ograniczona, jeśli szkolenia nie są wspierane przez inne środki zapobiegawcze, takie jak zabezpieczenia fizyczne czy cyfrowe, co zmniejsza ogólny wpływ na gotowość organizacji. Ponadto wiedza zdobyta podczas jednorazowych szkoleń ma tendencję do szybkiego zanikania, jeśli nie jest regularnie utrwalana, co może prowadzić do spadku efektywności działań prewencyjnych w dłuższym okresie.

Wariant 2 powinien być wybierany w sytuacjach, gdy priorytetem jest zwiększenie kompetencji pracowników w zakresie reagowania na incydenty. Jest to szczególnie ważne w organizacjach, które posiadają rozwinięte zabezpieczenia techniczne, ale ich pracownicy nie są odpowiednio przeszkoleni w ich efektywnym wykorzystaniu. Implementacja Ścieżki 2 jest

również wskazana w przypadku dostępności zasobów finansowych i czasowych, które pozwalają na realizację wysokiej jakości programów szkoleniowych. Dodatkowo, może być ona stosowana jako uzupełnienie innych wariantów, takich jak Wariant 4 lub Wariant 3, aby zwiększyć ich skuteczność poprzez lepsze przygotowanie personelu.

W celu zwiększenia efektywności wariantu 2 zaleca się jej połączenie z kampaniami zwiększającymi świadomość zagrożeń, co pozwoli na lepsze osadzenie treści szkoleniowych w kontekście funkcjonowania organizacji. Wdrożenie systemów zarządzania nauczaniem (LMS) może również przyczynić się do poprawy efektywności poprzez monitorowanie postępów pracowników, automatyczne przypominanie o konieczności odbycia kolejnych szkoleń oraz dostęp do zróżnicowanych materiałów edukacyjnych. Regularne analizy wyników testów, raportów o incydentach oraz poziomu zaangażowania uczestników szkoleń pozwolą na bieżące monitorowanie skuteczności wdrożonych programów i umożliwią ich dynamiczne dostosowanie do zmieniających się potrzeb organizacji.

Wariant 3 skupia się na wzmocnieniu procesów weryfikacji pracowników i podwykonawców. W tym wariancie, kluczową rolę odgrywa przegląd procesów weryfikacyjnych i opracowanie optymalnych narzędzi do jego prowadzenia, regularnych przegląd relacji z podwykonawcami oraz integracja procedur weryfikacji w ramach procesu wprowadzania nowych pracowników. Oczekiwane korzyści z wdrożenia wariantu 3 obejmują znaczące zmniejszenie ryzyka związanego z zagrożeniami wewnętrznymi. Rygorystyczne sprawdzanie przeszłości pracowników pozwala ograniczyć zatrudnianie osób o potencjalnie złych intencjach, co wpływa na zwiększenie bezpieczeństwa organizacji. Dodatkowo weryfikacja dostawców minimalizuje ryzyko naruszenia bezpieczeństwa przez strony trzecie, co jest szczególnie istotne w sektorach współpracujących z wieloma partnerami zewnętrznymi. Kolejnym kluczowym benefitem jest zgodność z przepisami prawa, która eliminuje ryzyko kar za naruszenie regulacji takich jak RODO, przyczyniając się do budowy wiarygodności i odpowiedzialności organizacji.

Wariant 3 może wiązać się jednak z pewnymi ograniczeniami, w tym wysokimi kosztami wdrożenia kompleksowych systemów weryfikacyjnych, co może być szczególnie odczuwalne w większych organizacjach. Dodatkowym wyzwaniem są ograniczenia technologiczne – automatyczne narzędzia weryfikacyjne mogą nie wychwycić wszystkich potencjalnych zagrożeń, co zwiększa konieczność stosowania manualnych procesów kontrolnych. Ponadto efektywność tej ścieżki jest ograniczona, jeśli nie jest wsparta innymi środkami ochrony, takimi jak szkolenia pracowników czy zabezpieczenia techniczne, które mogą lepiej odpowiadać na dynamicznie zmieniające się zagrożenia, np. nowe techniki szpiegowskie.

Wariant 3 znajduje zastosowanie w sytuacjach, gdy priorytetem organizacji jest zwiększenie bezpieczeństwa personalnego, szczególnie w organizacjach, które już wdrożyły podstawowe zabezpieczenia techniczne i szkoleniowe. Jest szczególnie zalecana w sektorach o podwyższonym ryzyku, takich jak sektor finansowy, technologiczny czy obronny, gdzie zagrożenia wewnętrzne mogą mieć poważne konsekwencje. Aby zwiększyć skuteczność tej ścieżki, organizacje mogą zintegrować ją z innymi metodami ochrony, takimi jak regularne szkolenia (Wariant 2), co wzmacnia przygotowanie pracowników. Dodatkowo inwestowanie w automatyzację procesów weryfikacyjnych oraz prowadzenie regularnych audytów zgodności z aktualnymi standardami bezpieczeństwa pozwala na bieżąco optymalizować działanie procesów weryfikacyjnych, zapewniając kompleksową ochronę organizacji.

Wariant 4 polega na wzmocnieniu fizycznych i cyfrowych zabezpieczeń organizacji. Wdrożenie tego wariantu obejmuje implementację efektywnych systemów kontroli dostępu fizycznego, wzmacnianie cyberbezpieczeństwa poprzez zastosowanie narzędzi uwzględniających ewolucję i zmienność zagrożeń oraz regularne prowadzenie audytów bezpieczeństwa oraz ocenę podatności na zagrożenia. Zabezpieczenia fizyczne i cyfrowe pełnią kluczową rolę w minimalizowaniu ryzyka incydentów, takich jak włamania czy szpiegostwo przemysłowe. Stanowią one pierwszą linię obrony, ograniczając potencjalny dostęp do krytycznych zasobów organizacji. Dodatkowo, zintegrowane systemy bezpieczeństwa umożliwiają szybsze wykrywanie i reagowanie na zagrożenia, co przyczynia się do ograniczenia negatywnych skutków incydentów. Inwestycje w zabezpieczenia podnoszą również zaufanie interesariuszy – klientów, partnerów i pracowników, którzy postrzegają organizację jako bardziej odpowiedzialną i bezpieczną.

Pomimo istotnych korzyści, wdrożenie zaawansowanych systemów ochrony wiąże się z pewnymi ograniczeniami. Wysokie koszty instalacji i utrzymania nowoczesnych technologii mogą być znaczącym obciążeniem, szczególnie dla mniejszych organizacji. Ponadto integracja systemów fizycznych i cyfrowych wymaga zaawansowanych kompetencji technologicznych, co może stanowić wyzwanie dla zespołów odpowiedzialnych za wdrożenie. Zależność od technologii oznacza również konieczność ciągłego monitorowania, aktualizacji oraz konserwacji systemów, aby uniknąć przestojów lub awarii mogących zagrozić bezpieczeństwu.

Wariant 4 jest szczególnie zalecany dla organizacji, które przechowują dane o wysokiej wartości lub posiadają zasoby wymagające szczególnej ochrony, takie jak laboratoria, patenty czy dane klientów. Znajduje ona również zastosowanie w sektorach narażonych na wysokie ryzyko szpiegostwa, takich jak obrona, badania i rozwój czy sektor finansowy. Aby zwiększyć skuteczność tej ścieżki, organizacje mogą połączyć zaawansowane zabezpieczenia z edukacją pracowników, szkoląc ich w obsłudze systemów ochrony oraz procedur dotyczących dostępu.

Regularne testy i symulacje, takie jak ćwiczenia dotyczące cyberataków czy prób włamań fizycznych, pomogą w identyfikacji słabych punktów systemu. Dodatkowo kluczowe jest monitorowanie miejsc o największym ryzyku, takich jak serwerownie, laboratoria czy systemy przetwarzania danych, aby skupić zasoby na najważniejszych obszarach ochrony.

Wariant 5 stanowi kompilację wariantu 1 oraz 2 i polega na połączeniu świadomości zagrożeń z odpowiednim szkoleniem pracowników. W celu wdrożenia tego wariantu, organizacja powinna uwzględnić elementy przewidziane dla wariantu 1 oraz 2, jak również skupić się na realizacji zintegrowanych programów obejmujących kampanie uświadamiające połączone z interaktywnymi szkoleniami oraz monitorowanie poziomu zdolności reagowania na incydenty po zakończeniu działania programu. Budowanie gotowości zespołów do reagowania na zagrożenia, w tym szpiegostwo korporacyjne, jest kluczowym elementem Wariantu 5. Połączenie edukacji z zaawansowanymi programami szkoleniowymi umożliwia pracownikom nie tylko rozpoznanie potencjalnych zagrożeń, ale także odpowiednią reakcję w sytuacjach kryzysowych. Wdrożenie tych działań znacząco zmniejsza ryzyko sukcesu ataków poprzez podniesienie poziomu świadomości oraz umiejętności praktycznych w organizacji. Co więcej, rozwijanie kultury bezpieczeństwa jako integralnej części codziennej pracy wzmacnia zaangażowanie wszystkich interesariuszy w działania na rzecz ochrony danych i zasobów.

Pomimo korzyści, wdrożenie wariantu 5 wiąże się z pewnymi wyzwaniami. Zintegrowanie kampanii edukacyjnych i szkoleń wymaga znacznych nakładów finansowych oraz czasu, co może stanowić barierę dla organizacji o ograniczonym budżecie. Sukces programu zależy również od aktywnego zaangażowania pracowników, co w dużych lub zdecentralizowanych strukturach może być trudne do osiągnięcia. Dodatkowo, ta ścieżka nie obejmuje bezpośrednich zabezpieczeń fizycznych ani cyfrowych, co sprawia, że jest mniej skuteczna w obliczu zaawansowanych i technologicznie złożonych ataków.

Wariant 5 jest najbardziej odpowiedni dla organizacji posiadających wykwalifikowaną kadrę, która potrzebuje jedynie ukierunkowanego wsparcia w zakresie bezpieczeństwa. To także rozwiązanie dla firm, które dopiero zaczynają rozwijać kulturę bezpieczeństwa, zanim zdecydują się na inwestycje w techniczne zabezpieczenia. W branżach charakteryzujących się wysokim ryzykiem wystąpienia zagrożeń, ale bez dotychczasowych incydentów, wariant 5 pozwala zbudować fundament dla dalszych działań. W celu zwiększenia jej skuteczności warto rozważyć połączenie z inwestycjami technicznymi, takimi jak podstawowe zabezpieczenia fizyczne czy cyfrowe. Regularna aktualizacja materiałów szkoleniowych i kampanii edukacyjnych w oparciu o nowe zagrożenia, jak również wdrożenie systemów motywacyjnych

dla pracowników, może znacząco poprawić efektywność działań i utrzymać zaangażowanie zespołów w dłuższej perspektywie.

Wariant 6 również stanowi kompilację przedstawionych wcześniej wariantów. W tym przypadku, jest to połączenie wariantu 1 oraz 3. Celem wdrożenia, oprócz przeprowadzenia czynności wskazanych w przedmiotowych wariantach, organizacja powinna skupić się na łączeniu działań uświadamiających z rygorystycznymi procesami weryfikacji. Kluczowymi elementami tego wariantu są edukacja pracowników w zakresie identyfikacji natury incydentu oraz uzupełnienie procesu rekrutacyjnego w zakresie efektywnych metod i form weryfikacji. Połączenie działań edukacyjnych i weryfikacyjnych w ramach wariantu 6 oferuje znaczące korzyści w zakresie zarządzania bezpieczeństwem organizacji. Przede wszystkim, integracja tych dwóch elementów pozwala na zwiększenie ochrony zarówno przed zagrożeniami wewnętrznymi, jak i zewnętrznymi. Pracownicy, dzięki szkoleniom, zyskują niezbędną wiedzę i umiejętności w zakresie identyfikacji oraz zgłaszania potencjalnych zagrożeń, podczas gdy procesy weryfikacyjne minimalizują ryzyko zatrudnienia osób nieodpowiednich lub współpracy z nierzetelnymi dostawcami. Co więcej, takie podejście przyczynia się do wzrostu zaufania interesariuszy, którzy postrzegają organizację jako odpowiedzialnego i wiarygodnego partnera, szczególnie istotnego w sektorach wymagających wysokiego poziomu bezpieczeństwa.

Jednakże, wdrożenie wariantu 6 może wiązać się z pewnymi ograniczeniami, które należy wziąć pod uwagę. Największym wyzwaniem jest koszt i złożoność związana z równoczesnym prowadzeniem działań edukacyjnych i weryfikacyjnych. Opracowanie i utrzymanie obu tych komponentów wymaga znacznych nakładów finansowych, a ich sukces zależy od aktywnego zaangażowania pracowników, co może być trudne w dużych lub zdecentralizowanych organizacjach. Ponadto brak technicznych środków ochrony, takich jak zabezpieczenia fizyczne czy cyfrowe, ogranicza skuteczność tej ścieżki w przypadku zaawansowanych technik szpiegowskich, które mogą wykorzystać luki w infrastrukturze technicznej organizacji.

Wariant 6 jest szczególnie rekomendowana dla organizacji posiadających silne zespoły oraz strukturę wspierającą wdrażanie działań edukacyjnych i weryfikacyjnych. Wysoką użyteczność znajduje w sektorach wysokiego ryzyka, takich jak technologie, sektor finansowy czy obrona, gdzie zagrożenia szpiegowskie są powszechne. Przedsiębiorstwa korzystające z usług wielu dostawców również mogą odnieść korzyści z rygorystycznych procesów weryfikacyjnych. Aby zwiększyć skuteczność Ścieżki 6, warto połączyć edukację z praktycznymi warsztatami, co pozwoli na lepsze zrozumienie i wdrożenie nabytych umiejętności. Automatyzacja procesów weryfikacyjnych przy użyciu zaawansowanych

narzędzi, takich jak HireRight czy Checkr, może znacząco przyspieszyć i usprawnić procesy oceny kandydatów i dostawców. Regularne aktualizacje i audyty pozwolą natomiast na dostosowanie systemów do zmieniających się zagrożeń, zapewniając skuteczność i bezpieczeństwo organizacji.

Wariant 7 ponownie stanowi kompilację wcześniej przedstawionych wariantów. Tym razem jest to połączenie wariantu 2 i 3. W celu wdrożenia tego wariantu, organizacja powinna uwzględnić elementy przewidziane dla przedmiotowych wariantów, a ponadto skupić się ma zapewnianiu odpowiedniego szkolenia dla pracowników i efektywną weryfikację kandydatów i podwykonawców. Kluczowymi elementami wariantu 7 są synchronizacja harmonogramu szkoleń z procesem wprowadzania nowych pracowników oraz ich szkolenie w zakresie współdziałania z wcześniej zweryfikowanymi podwykonawcami. Zintegrowane zarządzanie ryzykiem, będące kluczowym elementem Ścieżki 7, przynosi organizacjom istotne korzyści w zakresie minimalizowania zagrożeń związanych zarówno z czynnikami ludzkimi, jak i systemowymi. Dzięki połączeniu szkoleń i weryfikacji, pracownicy oraz dostawcy stają się bardziej świadomi potencjalnych zagrożeń, co przekłada się na ich większą niezawodność. Procesy weryfikacyjne eliminują ryzykowne elementy, zmniejszając szansę na dostęp osób o złych intencjach do kluczowych zasobów organizacji. Takie podejście nie tylko zwiększa gotowość organizacji do reagowania na incydenty, ale również buduje zaufanie partnerów biznesowych i klientów.

Wdrożenie wariantu 7 wiąże się jednak z pewnymi ograniczeniami, które mogą wpływać na jej efektywność. Najważniejszym wyzwaniem są wysokie koszty związane z opracowaniem oraz realizacją kompleksowych programów szkoleniowych i weryfikacyjnych. Dodatkowo, procesy te są czasochłonne, szczególnie w przypadku dużych organizacji z rozbudowaną strukturą lub wysoką rotacją pracowników. Istotnym ograniczeniem jest również brak uwzględnienia inwestycji w techniczne środki ochrony, takie jak zabezpieczenia cyfrowe czy fizyczne, co czyni tę ścieżkę mniej skuteczną w przypadku zaawansowanych ataków, wymagających interdyscyplinarnych metod przeciwdziałania.

Wariant 7 jest szczególnie zalecany dla organizacji, które stawiają na odpowiednio przygotowanych pracowników i współpracowników jako fundament swojego bezpieczeństwa. Branże takie jak logistyka czy produkcja, gdzie współpraca z wieloma partnerami zewnętrznymi jest nieodzowna, mogą znacząco skorzystać z wdrożenia efektywnych procesów weryfikacyjnych. Również organizacje z wysoką rotacją pracowników, np. w sektorze handlu detalicznego, znajdą w tym wariancie narzędzie do usprawnienia procedur przyjmowania nowych pracowników i podniesienia standardów bezpieczeństwa. Aby zwiększyć skuteczność wariantu 7, warto połączyć go z kampaniami świadomości, które zwiększą zaangażowanie

pracowników, oraz zautomatyzować procesy weryfikacji za pomocą narzędzi technologicznych. Regularne testy i ćwiczenia praktyczne mogą dodatkowo poprawić efektywność szkoleń, identyfikując luki w kompetencjach i umożliwiając ich bieżące eliminowanie.

Wariant 8 jest pierwszym z dwóch działań kompleksowych organizacji. Obejmuje kompilację wariantu 1, 2 oraz 3. W swoim działaniu skupia się na integracji procesów uświadamiających, szkoleń oraz procesów weryfikacyjnych. W celu wdrożenia tego wariantu, organizacja, oprócz wykorzystania elementów przewidzianych dla przedmiotowych trzech wariantów, powinna skupić się na łączeniu podejmowanych wysiłków w jednolity program kultury bezpieczeństwa organizacyjnego oraz wdrożyć efektywne narzędzia do monitorowania postępów we wskazanych obszarach działania. Kompleksowa ochrona oferowana przez wariant 8 wynika z integracji trzech kluczowych elementów: edukacji, szkoleń oraz weryfikacji pracowników i dostawców. Dzięki takiemu podejściu organizacja skutecznie minimalizuje ryzyko wynikające zarówno z zagrożeń wewnętrznych, jak i zewnętrznych. Świadomi i przeszkoleni pracownicy, którzy przeszli szczegółową weryfikację, są w stanie szybko i adekwatnie reagować na różne zagrożenia. Dodatkowo, taki model działania wzmacnia zaufanie interesariuszy, klientów i partnerów, którzy postrzegają organizację jako odpowiedzialną i godną zaufania, co może pozytywnie wpłynąć na jej reputację i pozycję rynkową.

Pomimo licznych korzyści, wdrożenie wariantu 8 niesie ze sobą znaczące wyzwania. Najistotniejszymi ograniczeniami są wysokie koszty oraz czasochłonność działań obejmujących realizację programów szkoleniowych, procesów weryfikacyjnych oraz kampanii zwiększających świadomość pracowników. Szczególnie w dużych organizacjach, gdzie struktura jest bardziej rozbudowana, konieczność skoordynowania tych działań między różnymi działami może stanowić dodatkowe wyzwanie. Brak efektywnej koordynacji i spójności w implementacji może obniżyć skuteczność programu, co w konsekwencji ograniczy jego wpływ na bezpieczeństwo organizacji.

Wariant 8 jest szczególnie rekomendowana dla dużych organizacji. Ze względu na koszty, jej wdrożenie jest najbardziej uzasadnione w firmach dysponujących znacznymi budżetami na bezpieczeństwo. Aby zwiększyć efektywność tej ścieżki, warto ją uzupełnić o elementy fizycznych i cyfrowych zabezpieczeń, takich jak systemy dostępu czy zaawansowane zapory sieciowe, oferowane w ramach wariantu 4. Wprowadzenie systemów motywacyjnych, w tym nagród za zaangażowanie w kwestie bezpieczeństwa, może zachęcić pracowników do większej aktywności i współodpowiedzialności za ochronę organizacji. Automatyzacja, np. przy użyciu narzędzi typu SIEM (Security Information and Event

Management), pozwala na zintegrowanie danych o zagrożeniach i zwiększenie szybkości oraz precyzji reakcji na incydenty, co dodatkowo wzmacnia kompleksowy system ochrony.

Wariant 9 jest drugim kompleksowym działaniem organizacji. Stanowi połączenie czterech wariantów podstawowych (1-4). W swoim działaniu, skupia się na przygotowaniu kompleksowej strategii obejmującej wszystkie kluczowe czynniki przewidziane w przedmiotowych wariantach podstawowych. Celem wdrożenia tego wariantu, organizacja powinna skupić się na połączeniu wszystkich działań w jednolitą strategię bezpieczeństwa organizacyjnego, przydzielenia środków finansowych na równoczesne inwestycje we wskazane obszary oraz wykorzystanie kluczowych wskaźników efektywności (Key Performance Indicators) do ciągłej ewaluacji i wdrażania ulepszeń uwzględniając zmiany w środowisku bezpieczeństwa. Najwyższy poziom bezpieczeństwa, jaki oferuje wariant 9, wynika z pełnej integracji wszystkich kluczowych elementów: edukacji, szkoleń, weryfikacji oraz zaawansowanych systemów zabezpieczeń fizycznych i cyfrowych. Dzięki takiemu podejściu organizacja jest przygotowana na różnorodne zagrożenia, zarówno wewnętrzne, jak i zewnętrzne, minimalizując ryzyko operacyjne. Jednocześnie, skuteczne wdrożenie tej ścieżki wzmacnia zaufanie interesariuszy, w tym klientów i partnerów, którzy postrzegają organizację jako profesjonalną, odpowiedzialną i zapewniającą najwyższy poziom ochrony. Połączenie tych elementów umożliwia stworzenie kompleksowego systemu bezpieczeństwa, który nie tylko reaguje na zagrożenia, ale również proaktywnie im zapobiega.

Pomimo licznych korzyści, wdrożenie wariantu 9 wiąże się z istotnymi ograniczeniami. Największym wyzwaniem są wysokie koszty, wynikające z konieczności inwestowania w zaawansowane technologie, kompleksowe szkolenia oraz rozbudowane systemy weryfikacyjne. Ponadto, złożoność operacyjna związana z koordynacją i zarządzaniem wszystkimi elementami wymaga odpowiednich zasobów ludzkich oraz zaawansowanych kompetencji zarządczych. Proces ten jest również czasochłonny, szczególnie w dużych organizacjach, gdzie opracowanie i wdrożenie wszystkich komponentów wymaga wielomiesięcznych, a nawet wieloletnich działań. Niemniej jednak, organizacje o krytycznym znaczeniu, takie jak te działające w sektorach obrony, finansów, technologii czy medycyny, powinny rozważyć implementację tej ścieżki ze względu na wysokie ryzyko, jakie niosą zagrożenia w ich branżach.

Aby zwiększyć efektywność wariantu 9, warto wdrożyć systemy monitorowania w czasie rzeczywistym, które umożliwiają natychmiastową reakcję na potencjalne incydenty. Kluczowe jest również budowanie kultury bezpieczeństwa, w której każdy pracownik czuje się współodpowiedzialny za ochronę organizacji. Taki model zarządzania wymaga regularnych testów i ćwiczeń, w tym symulacji sytuacji awaryjnych, które pozwalają na ocenę skuteczności

systemu i identyfikację potencjalnych luk. Kompleksowe podejście do zarządzania bezpieczeństwem w ramach wariantu 9 może stanowić wzorcowy model ochrony w organizacjach o strategicznym znaczeniu.

Efektywność działania poszczególnych wariantów można ocenić za pomocą proponowanych wskaźników KPI przedstawionych poniżej.

Poziom Świadomości Zagrożeń (Threat Awareness Level, TAL)

$$TAL = \frac{Liczba\ pracowników, którzy\ poprawnie\ zidentyfikowali\ zagrożenie}{Całkowita\ liczba\ przeszkolonych\ pracowników} \times 100\ \%$$

Opis:

Cel: ocena, ilu pracowników potrafi skutecznie rozpoznać zagrożenie,

Interpretacja: wysoka wartość wskazuje na wysoki poziom świadomości zagrożeń w organizacji.

Efektywność Szkolenia (Training Effectiveness, TE)

$$TE = \frac{Średni\ wynik\ testu\ po\ szkoleniu - Średni\ wynik\ testu\ przed\ szkoleniem}{Maksymalny\ możliwy\ wynik\ testu} \times 100\%$$

Opis:

Cel: pomiar przyrostu wiedzy pracowników w wyniku szkolenia,

Interpretacja: wyższe wartości wskazują na większy przyrost wiedzy i skuteczność szkolenia.

Skuteczność Weryfikacji Pracowników i Dostawców (Verification Effectiveness, VE)

$$VE = \frac{Liczba\ zweryfikowanych\ pracowników\ (dostawców)\ bez\ incydentów}{Całkowita\ liczba\ zweryfikiowanych\ pracowników\ (dostawców)} \times 100\%$$

Opis:

Cel: ocena skuteczności procesów weryfikacyjnych w eliminacji ryzykownych osób lub podmiotów,

Interpretacja: wartości bliskie 100% oznaczają wysoką skuteczność weryfikacji.

Liczba Wykrytych i Zneutralizowanych Zagrożeń (Threat Detection Rate, TDR)

$$TDR = \frac{Liczba\ wykrytych\ i\ zneutralizowanych\ zagrożeń}{Całkowita\ liczba\ zidentyfikowanych\ prób\ incydentów} \times 100\%$$

Opis:

Cel: ocena skuteczności systemów bezpieczeństwa w wykrywaniu i neutralizacji zagrożeń,

Interpretacja: wysoka wartość wskazuje na dobrą skuteczność systemów ochrony.

Średni Czas Reakcji na Incydenty (Incident Response Time, IRT)

$$IRT = \frac{Suma\ czasu\ reakcji\ na\ wszystki\ incydenty\ (w\ minutach)}{Liczba\ incydentów}$$

Opis:

Cel: pomiar efektywności organizacji w reagowaniu na zagrożenia,

Interpretacja: niższe wartości oznaczają szybsze reakcje na incydenty.

Zgodność z Polityką Bezpieczeństwa (Policy Compliance Rate, PCR)

$$PCR = \frac{Liczba\ pracowników\ (dostawców)\ zgodnych\ z\ polityką}{Całkowita\ liczba\ pracowników\ (dostawców)} \times 100\%$$

Opis:

Cel: ocena poziomu zgodności pracowników i dostawców z obowiązującymi politykami bezpieczeństwa,

Interpretacja: wartości bliskie 100% wskazują na wysoki poziom zgodności.

Wskaźnik Powtarzalności Incydentów (Incident Recurrence Rate, IRR)

$$IRR = \frac{Liczba\ powtarzających\ się\ incydentów}{Całkowita\ liczba\ incydentów} \times 100\%$$

Opis:

Cel: ocena zdolności organizacji do eliminacji przyczyn incydentów,

Interpretacja: niższe wartości wskazują na skuteczną eliminację przyczyn incydentów.

Koszt Reakcji na Incydenty (Incident Response Cost, IRC)

$$IRC = \frac{Całkowity\ koszt\ reakcji\ na\ incydenty\ (PLN)}{Liczba\ incydentów}$$

Opis:

Cel: oszacowanie kosztów finansowych związanych z obsługą incydentów,

Interpretacja: niższe wartości oznaczają bardziej efektywne zarządzanie zasobami podczas reakcji na incydenty.

Przedstawione powyżej wskaźniki KPI mogą posłużyć do oceny skuteczności wdrożenia modelu zarządzania bezpieczeństwem. Systematyczne monitorowanie kluczowych wskaźników efektywności (KPI) odgrywa istotną rolę w zarządzaniu jakością i bezpieczeństwem organizacji. Przede wszystkim umożliwia identyfikację obszarów wymagających poprawy, gdzie niskie wartości KPI sygnalizują konieczność aktualizacji istniejących procesów lub intensyfikacji działań ochronnych. Ponadto, precyzyjnie określone wskaźniki sprzyjają efektywnemu raportowaniu do zarządu, dostarczając przejrzystych i jednoznacznych danych na temat skuteczności realizowanych działań w zakresie bezpieczeństwa. Dodatkowo, analiza KPI wspiera optymalizację zarówno kosztów, jak i procesów operacyjnych, pozwalając na lepsze zarządzanie zasobami i usprawnienie czasu reakcji, co przekłada się na ogólną efektywność organizacyjną.

W celu przeprowadzenia symulacji, z wykorzystaniem programu AnyLogic, zastosowano dane wejściowe, przedstawione w tabeli nr 29.

Tabela 29 Dane do symulacji wdrożenia modelu zarządzania bezpieczeństwem

Kategoria	Parametr	Dane wejściowe
Pracownicy	Liczba pracowników	900 (100 na każdy z 9 wariantów)
	Poziom świadomości zagrożeń (TAL)	Początkowy: 40–70% (średnio 55%). Wzrost o 10–30% po szkoleniach
	Prawdopodobieństwo zgłoszenia	TAL ≥ 80% zwiększa szansę zgłoszenia incydentu o 50%
	Rotacja	10% pracowników zmienia się w trakcie symulacji (np. rotacja lub nieobecności)
	Testy wiedzy	Dwie rundy testów:

Kategoria	Parametr	Dane wejściowe
		Pierwsza: 900 pracowników (zaraz po szkoleniu) Druga: 800 pracowników (po 6 miesiącach, uwzględniając rotację)
Dostawcy	Liczba dostawców	900 (100 na każdy wariant)
	Status początkowy	50% dostawców zweryfikowanych na początku
	Częstotliwość kontaktu	Średnio 2 interakcje na dostawcę miesięcznie
	Weryfikacja	Skuteczność różna w zależności od wariantu (50–98%)
Zagrożenia	Liczba incydentów	Łącznie 850 w całej symulacji (95 średnio na każdy wariant).
	Typy zagrożeń	Phishing: 30%
		Nieautoryzowany dostęp: 25%
		Malware: 20%
		Anomalie w logach: 15%
		Ransomware: 10%
	Trudność neutralizacji	Rozkład trudności: łatwe (50%), średnie (30%), trudne (20%)
Systemy SIEM/PSIM	Zdolność wykrywania	Od 70% do 95%
	Czas reakcji	Najlepszy czas reakcji: 28 minut Najgorszy czas reakcji: 45 minut
	Neutralizacja zagrożeń	Efektywność neutralizacji NNT: od 70% do 95%
Szkolenia	Poziom TAL po szkoleniu	TAL wzrasta średnio o 20%
	Retencja wiedzy	68–90%
	Liczba uczestników	900 (100 na wariant) uczestników w pierwszej turze, 800 (~89 na wariant) w drugiej turze (rotacja)
KPI	TAL (Threat Awareness Level)	Docelowy poziom: ≥90%
	Retencja wiedzy	Docelowy poziom: ≥85%
	VE (Verification Effectiveness)	Docelowy poziom: ≥98%
	NNT (Neutralized Threats)	Docelowy poziom: ≥95%
	IRT (Incident Response Time)	Docelowy czas: ≤30 minut

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Pracownicy, reprezentujący różne działy – zarówno techniczne, jak i nietechniczne – są kluczowym źródłem danych o poziomie świadomości zagrożeń (TAL) i rotacji, które

umożliwiają analizę skuteczności działań szkoleniowych. Dostawcy, poprzez proces weryfikacji, mają bezpośredni wpływ na skuteczność weryfikacji (VE), co minimalizuje ryzyko zewnętrzne. W zakresie zagrożeń uwzględniono realistyczne scenariusze incydentów bezpieczeństwa o zróżnicowanym stopniu trudności neutralizacji, co pozwala na kompleksową ocenę zdolności organizacji do ich ograniczania. Wydajność systemów SIEM/PSIM pozostaje kluczowym elementem wpływającym na czas reakcji na incydenty (IRT) oraz liczbę zneutralizowanych zagrożeń (NNT), bezpośrednio przekładając się na skuteczność reagowania na niebezpieczeństwa. W kontekście szkoleń szczególną uwagę zwrócono na retencję wiedzy, która wpływa na długoterminową efektywność edukacji. Ostatecznie przyjęte wartości docelowe KPI stanowią istotny punkt odniesienia, umożliwiając ocenę i porównanie efektywności różnych wariantów działań organizacyjnych.

Przeprowadzona analiza wskaźników KPI dla dziewięciu wariantów modelu zarządzania bezpieczeństwem wykazała istotne różnice w skuteczności zastosowanych strategii, obejmujących szkolenia pracowników, weryfikację dostawców oraz procedury reagowania na incydenty. Wyniki analizy przedstawiono w tabeli nr 30.

Tabela 30 Podsumowanie wskaźników KPI dla 9 wariantów

	Wariant	TAL (%)	Retencja wiedzy (%)	VE (%)	NNT (%)	IRT (min)
	1	78	78	94	92	30.0
	2	74	75	92	90	30.0
	3	80	82	95	94	30.0
	4	68	70	90	89	40.0
	5	82	80	96	96	35.0
	6	85	85	97	97	45.0
	7	70	72	93	91	40.0
	8	72	68	92	89	45.0
	9	91	90	98	98	28.6

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Warianty charakteryzujące się wysokimi wartościami wskaźników, takich jak TAL i NNT, potwierdzają efektywność wdrożonych działań edukacyjnych oraz zastosowania zaawansowanych systemów ochronnych. Z kolei niższe wyniki w pozostałych wariantach wskazują na potrzebę udoskonalenia tych obszarów w celu podniesienia ogólnej efektywności modelu.

Proces ewaluacji skuteczności działań bezpieczeństwa opiera się na zbieraniu danych z różnych obszarów, analizie wskaźników KPI oraz ocenie realizacji założonych celów. Zebrane dane, takie jak raporty z audytów czy wyniki ankiet, są analizowane w celu identyfikacji trendów i luk w systemie. Następnie przeprowadzana jest ocena skuteczności wdrożonych środków, a na tej podstawie wprowadzane są zmiany w strategii, takie jak

aktualizacja programów szkoleniowych czy wzmocnienie procedur weryfikacyjnych. Proces ewaluacji stanowi cykliczny mechanizm umożliwiający organizacji nieustanne dostosowywanie swoich działań do zmieniających się warunków i zagrożeń.

6.3 Monitorowanie i ewaluacja skuteczności wdrożenia

Monitorowanie kluczowych obszarów działalności organizacji w zakresie bezpieczeństwa stanowi fundamentalny element skutecznego zarządzania ryzykiem. Jednym z kluczowych aspektów jest świadomość zagrożeń wśród pracowników, mierzona poprzez takie działania jak ankiety, analiza zgłoszeń incydentów czy uczestnictwo w kampaniach edukacyjnych. Kolejnym obszarem są szkolenia, które ocenia się na podstawie wyników testów wiedzy oraz opinii uczestników. Równie istotne są procedury weryfikacji pracowników i dostawców, które obejmują audyty i monitoring ciągły. Dodatkowo, zabezpieczenia fizyczne i cyfrowe, takie jak testy penetracyjne czy analiza zdarzeń, pozwalają na skuteczne identyfikowanie i neutralizowanie potencjalnych zagrożeń.

W procesie monitorowania oraz oceny realizacji wdrożenia kluczowe znaczenie ma zastosowanie odpowiednich narzędzi analitycznych, które umożliwią ocenę efektywności poszczególnych wariantów oraz identyfikację obszarów wymagających doskonalenia. Spośród proponowanych metod, najbardziej adekwatne na tym etapie są następujące techniki:

a) drzewa decyzyjne (decision trees) – jako narzędzie wspomagające identyfikację kluczowych czynników determinujących skuteczność wdrożenia,
b) las losowy (random forest) – w celu analizy trendów oraz hierarchizacji zmiennych wpływających na efektywność w różnych scenariuszach,
c) regresja logistyczna (logistic regression) – służąca prognozowaniu prawdopodobieństwa osiągnięcia sukcesu wdrożenia dla poszczególnych wariantów.

Tego typu podejście umożliwia precyzyjną ocenę wpływu różnych czynników na wyniki implementacji oraz wspiera proces podejmowania decyzji dotyczących koniecznych usprawnień.

Drzewa decyzyjne zostały zastosowane w celu identyfikacji hierarchii wpływu kluczowych wskaźników efektywności (KPI) na skuteczność monitorowania, definiowaną przez wysoki poziom świadomości zagrożeń (TAL ≥ 85%). Analiza wykazała, że najważniejszym czynnikiem determinującym efektywność monitorowania jest czas reakcji na incydenty (IRT), który wyprzedza takie wskaźniki jak retencja, skuteczność weryfikacji (VE) oraz liczba zneutralizowanych zagrożeń (NNT). Warianty charakteryzujące się niskim IRT (≤ 35 minut) osiągnęły wyższy poziom świadomości zagrożeń, co wskazuje na ich przewagę

nad innymi. Warianty z wysokim IRT (> 40 minut) wymagały usprawnień, takich jak lepsza integracja systemów SIEM/PSIM oraz wdrożenie automatycznych mechanizmów priorytetowych alertów.

Metoda Random Forest została wykorzystana do zidentyfikowania najważniejszych zmiennych wpływających na skuteczność wdrożenia oraz analizy trendów między różnymi wariantami. W analizie kluczową rolę odegrały TAL i IRT, podczas gdy retencja oraz skuteczność weryfikacji miały umiarkowane znaczenie. Liczba zneutralizowanych zagrożeń (NNT) okazała się najmniej istotnym czynnikiem. Lepsze wyniki osiągały warianty o wysokiej świadomości zagrożeń i krótkim czasie reakcji. Dla poprawy skuteczności w gorszych wariantach zaproponowano cykliczne przypomnienia e-learningowe, grywalizacyjne testy wiedzy oraz automatyzację procesów weryfikacyjnych, co pozwala na zwiększenie efektywności tych wskaźników.

Regresja logistyczna posłużyła do oszacowania prawdopodobieństwa sukcesu poszczególnych wariantów wdrożenia na podstawie wartości KPI. Warianty z wysokim poziomem TAL i niskim czasem reakcji na incydenty osiągnęły przewidywane prawdopodobieństwo sukcesu przekraczające 85%, natomiast warianty o niższych wynikach w tych obszarach miały szanse poniżej 50%. Analiza wykazała, że wzrost TAL o 1% zwiększa prawdopodobieństwo sukcesu o 0,5%, a skrócenie czasu reakcji o 5 minut podnosi je o 10%. W celu poprawy efektywności gorszych wariantów zasugerowano personalizowane kampanie edukacyjne oraz intensyfikację działań automatyzacyjnych i integracyjnych systemów, co ma na celu zoptymalizowanie wyników wdrożenia.

Na podstawie powyższych czynników, dokonano ewaluacji poszczególnych wariantów, a jej wyniki przedstawiono w tabeli nr 31.

Tabela 31 Podsumowanie ewaluacji wariantów

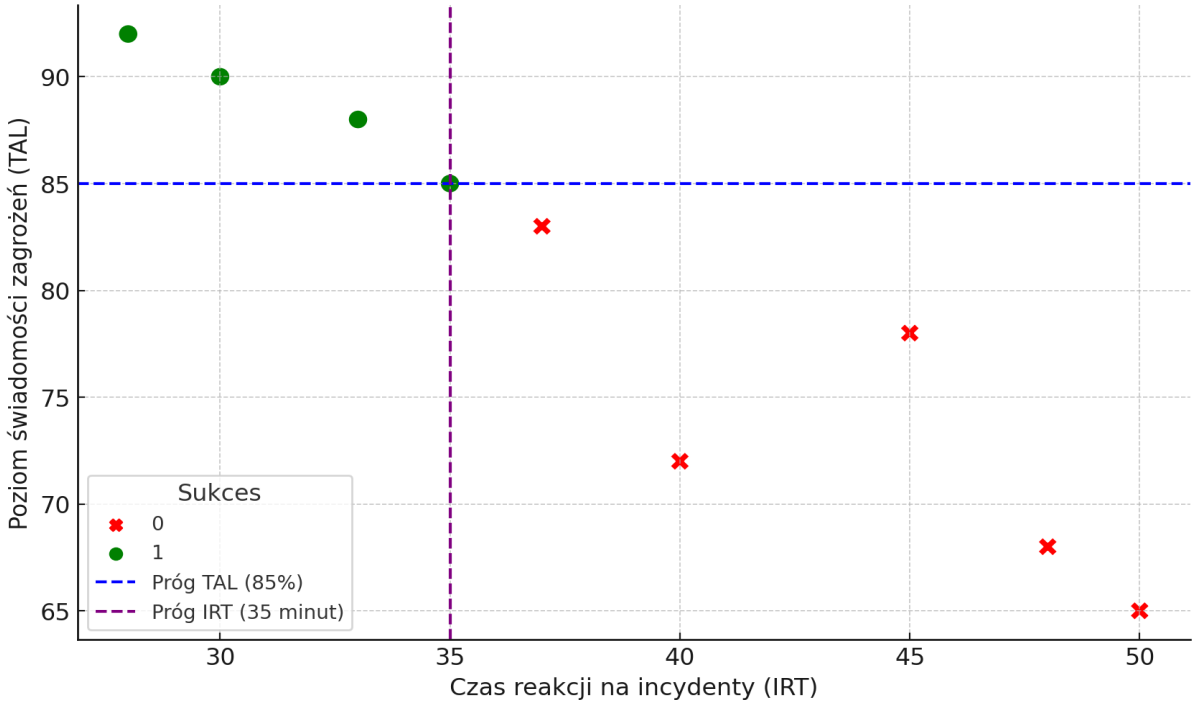
Wariant	Wynik	Ocena	Poprawa
1	Lepszy	Wysoki TAL, niski IRT, umiarkowana Retencja	Utrzymanie wyników
2	Gorszy	Niski TAL, wysoki IRT, niska Retencja	Poprawa Retencji (e-learning), skrócenie IRT (automatyzacja)
3	Lepszy	Bardzo wysoki TAL, niski IRT, wysoka VE	Optymalizacja VE (dalsza automatyzacja weryfikacji)
4	Gorszy	Niski TAL, wysoki IRT, umiarkowana VE	Poprawa VE (audyt regularny), edukacja dla podniesienia TAL
5	Lepszy	Wysoki TAL, niski IRT, wysoka Retencja	Dalsze wsparcie grywalizacji dla poprawy Retencji
6	Gorszy	Niski TAL, umiarkowany IRT, niska Retencja	Poprawa Retencji oraz TAL poprzez zindywidualizowane szkolenia
7	Lepszy	Wysoki TAL, umiarkowany IRT, wysoka Retencja	Optymalizacja Retencji poprzez krótkie testy powtórkowe

Wariant	Wynik	Ocena	Poprawa
8	Gorszy	Niski TAL, wysoki IRT, niska Retencja i VE	Poprawa wszystkich wskaźników – wprowadzenie regularnych audytów, automatyzacji i edukacji
9	Lepszy	Bardzo wysoki TAL, niski IRT, wysoka Retencja i VE	Kontynuacja działań optymalizacyjnych

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Zaleca się regularne monitorowanie kluczowych wskaźników efektywności (KPI), takich jak świadomość zagrożeń (TAL), czas reakcji na incydenty (IRT), poziom retencji oraz skuteczność weryfikacji (VE). Proces ten powinien być wspierany przez zaawansowane narzędzia analityczne umożliwiające bieżącą ocenę wyników. W celu zwiększenia efektywności działań edukacyjnych, należy je dostosować do specyficznych potrzeb działów wykazujących niższe wskaźniki efektywności. Personalizacja szkoleń pozwoli na lepsze dostosowanie treści do indywidualnych wymagań jednostek organizacyjnych, co może przyczynić się do poprawy wyników w tych obszarach.

Analiza relacji pomiędzy wskaźnikami świadomości zagrożeń (TAL) a czasem reakcji na incydenty (IRT) umożliwiła wyodrębnienie obszarów sukcesu i niepowodzenia. Powyższe zostało przedstawione na wykresie nr 24.

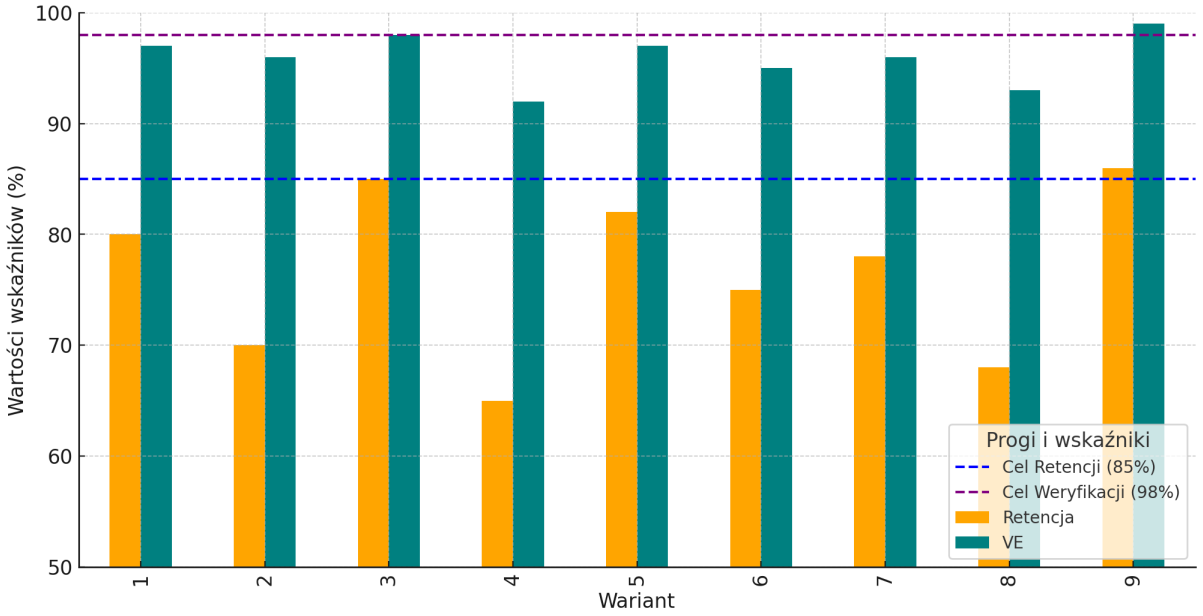


Wykres 24 TAL a IRT - klasyfikacja wyników

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Zielone punkty reprezentują sytuacje, w których wskaźniki osiągają założone wartości (TAL ≥ 85% oraz IRT ≤ 35 minut), natomiast czerwone punkty oznaczają przypadki niespełnienia tych kryteriów. Linie przerywane wyznaczają progi dla obu wskaźników, ułatwiając klasyfikację. Na tej podstawie stwierdzono, że warianty 1, 3, 5, 7 i 9 mieszczą się w obszarze sukcesu, podczas gdy warianty 2, 4, 6 i 8 nie spełniają wymogów, głównie ze względu na zbyt długi czas reakcji na incydenty (IRT).

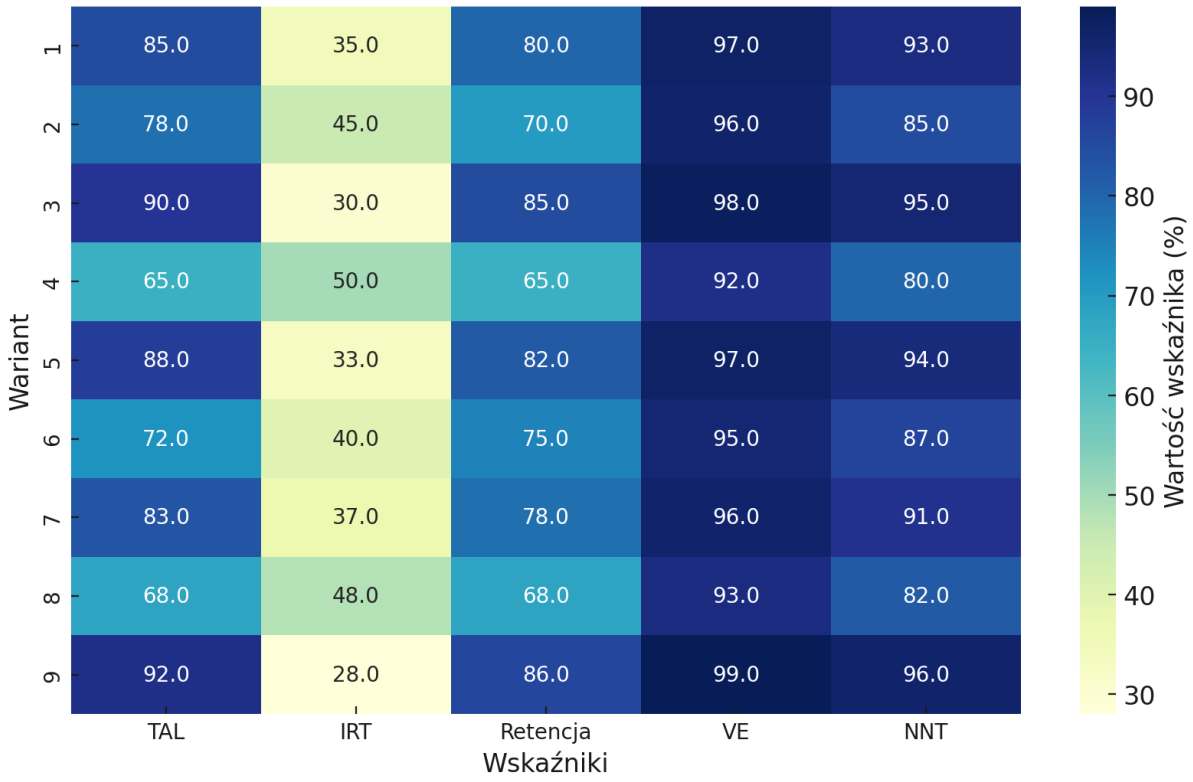
Retencja wiedzy oraz skuteczność weryfikacji (VE) zostały ocenione jako kluczowe wskaźniki efektywności, których wyniki przedstawiono na wykresie nr 25.



Wykres 25 Retencja i skuteczność weryfikacji (VE) a wariant wdrożenia
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Wyniki zilustrowano graficznie z wykorzystaniem linii przerywanych wyznaczających cele (Retencja ≥ 85% i VE ≥ 98%). Warianty 3 i 9 osiągnęły najwyższe wartości w obu kategoriach, co świadczy o ich wysokiej skuteczności. Z kolei warianty 4, 6 i 8 wykazały niskie wartości zarówno w zakresie Retencji, jak i VE, co wskazuje na konieczność wdrożenia działań naprawczych w celu poprawy wyników w tych obszarach. Kluczowym zaleceniem jest wdrożenie ukierunkowanych działań edukacyjnych i automatyzacji procesów weryfikacji.

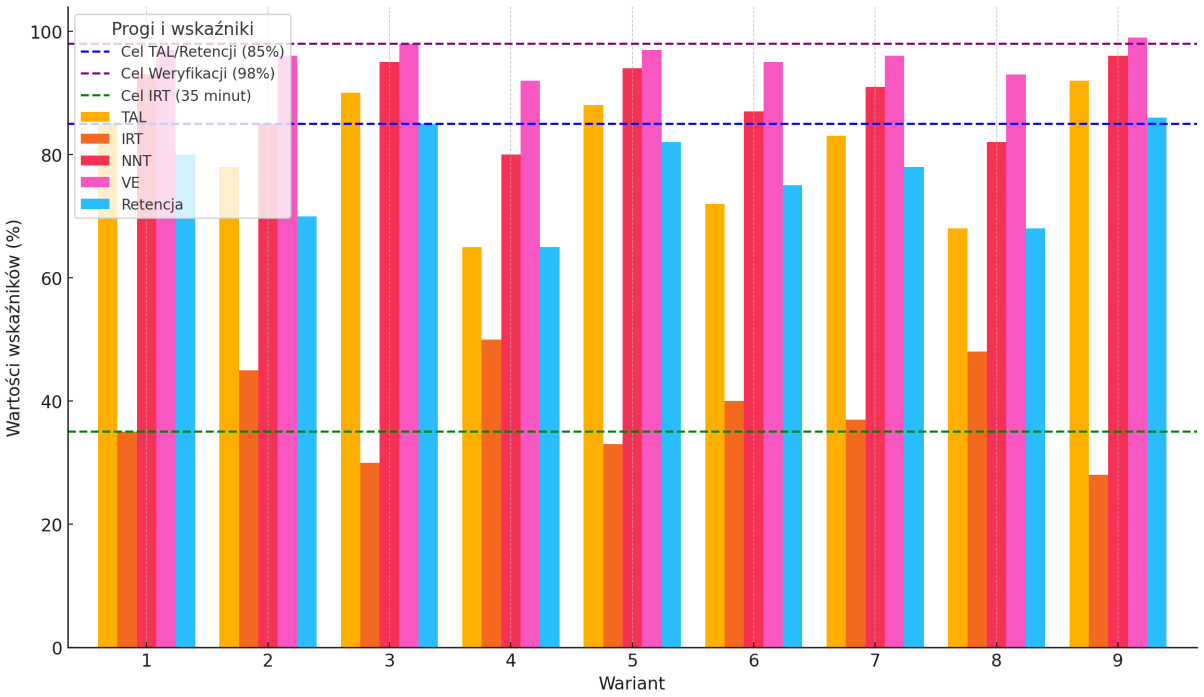
Mapa cieplna wskaźników, przedstawiona na wykresie nr 26, obrazuje szczegółowe wyniki dotyczące TAL, IRT, Retencji, VE oraz liczby zneutralizowanych zagrożeń (NNT) dla poszczególnych wariantów.



Wykres 26 Mapa cieplna wskaźników efektywności
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Wartości wskaźników zilustrowano za pomocą kolorów, gdzie jaśniejsze barwy oznaczają lepsze rezultaty. Wyniki wskazują, że warianty 3, 5, 7 i 9 charakteryzują się dominacją w większości wskaźników, szczególnie w TAL i VE, co potwierdza ich wysoką efektywność. Natomiast wariant 4 osiągnął najniższe wartości w badanych kategoriach, co sugeruje konieczność przeprowadzenia kompleksowej analizy i wdrożenia działań usprawniających.

Wykres nr 27 przedstawia szczegółowe porównanie wskaźników KPI (TAL, IRT, NNT, VE, Retencja) dla dziewięciu wariantów, ukazując różnice w wynikach i identyfikując, które z nich spełniają założone progi, a które pozostają poniżej oczekiwań.



Wykres 27 Porównanie kluczowych wskaźników w ramach wariantów wdrożenia
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

TAL (poziom świadomości zagrożeń) z celem wynoszącym ≥85% osiągnęły warianty 3, 5 i 9, co świadczy o ich skuteczności w budowaniu świadomości. Warianty 4 i 8 pozostają daleko poniżej wyznaczonego poziomu (≤70%), co wskazuje na potrzebę poprawy. W zakresie IRT (czas reakcji na incydenty), wyznaczono próg ≤35 minut, który zrealizowano w wariantach 3, 5 i 9, podczas gdy warianty 4 i 8 charakteryzują się znacznie wyższymi wartościami (≥48 minut), co osłabia efektywność odpowiedzi na zagrożenia. Dla NNT (zneutralizowane zagrożenia) celem było ≥95%, co osiągnęły warianty 3, 5 i 9, natomiast wariant 4 zanotował wynik 80%. Skuteczność weryfikacji (VE) z celem ≥98% została zrealizowana jedynie przez wariant 9, podczas gdy pozostałe warianty osiągnęły wyniki zbliżone do 95%-97%. W przypadku Retencji, gdzie celem było ≥85%, spełniły go warianty 3 i 9, natomiast warianty 4 i 8 charakteryzują się niskimi wartościami (65%-70%).

Średnie wartości wskaźników wskazują na przeciętny poziom TAL wynoszący 80,1%, IRT na poziomie 38,4 minuty, co przewyższa założony cel oraz NNT na poziomie 89,2%, poniżej oczekiwanego progu 95%. VE osiągnęło średnią wartość 95,9%, a Retencja 76,6%. Analiza odchyleń standardowych wskazuje, że wskaźniki TAL oraz Retencja charakteryzują się dużą zmiennością pomiędzy wariantami, co sugeruje brak spójności w strategiach budowania świadomości i retencji wiedzy w organizacjach. Dla wariantów 4 i 8 zaleca się skoncentrowanie działań na redukcji IRT poprzez integrację systemów i usprawnienie procedur reagowania na incydenty. W obszarze TAL i Retencji niezbędne są ukierunkowane szkolenia

oraz regularne działania utrwalające wiedzę. Warianty 3, 5 i 9, pomimo wysokich wyników, mogą zwiększyć skuteczność VE i NNT poprzez wdrożenie automatyzacji procesów neutralizacji zagrożeń. We wszystkich wariantach rekomenduje się standaryzację modułów szkoleniowych w celu zmniejszenia zmienności w TAL i Retencji oraz automatyzację wybranych procesów, co pozwoli na uzyskanie bardziej spójnych i przewidywalnych wyników w zakresie VE i IRT.

W realizacji monitorowania i ewaluacji kluczową rolę odgrywają nowoczesne narzędzia, takie jak systemy zarządzania bezpieczeństwem informacji (SIEM), które umożliwiają monitorowanie incydentów w czasie rzeczywistym. Platformy LMS pozwalają na bieżące śledzenie postępów pracowników w szkoleniach, a narzędzia do weryfikacji, takie jak HireRight, automatyzują procesy sprawdzania danych. Systemy PSIM integrują zabezpieczenia fizyczne i cyfrowe, co umożliwia bardziej kompleksowe podejście do zarządzania bezpieczeństwem. Z kolei aplikacje ankietowe, takie jak SurveyMonkey, pomagają zbierać opinie pracowników, które stanowią istotny element oceny efektywności działań.

Proces monitorowania i ewaluacji skuteczności wdrożenia modelu bezpieczeństwa w przedsiębiorstwie powinien uwzględniać dodatkowe czynniki, które pozwolą na kompleksową ocenę i optymalizację działań. Oto kluczowe elementy:

1. **Analiza ryzyka w czasie rzeczywistym** – regularne aktualizowanie matrycy ryzyka w oparciu o zmieniające się zagrożenia i wyniki monitoringu systemów bezpieczeństwa.
2. **Ocena zgodności z regulacjami** – ciągłe sprawdzanie zgodności z nowymi wymaganiami prawnymi oraz standardami branżowymi.
3. **Integracja systemów zarządzania** – stworzenie platformy integrującej dane z różnych narzędzi, takich jak SIEM, PSIM czy LMS, w celu zminimalizowania fragmentacji danych.
4. **Monitorowanie świadomości i zaangażowania pracowników** – badanie postaw i świadomości bezpieczeństwa wśród pracowników za pomocą ankiet i testów.
5. **Automatyzacja raportowania** – wykorzystanie narzędzi generujących regularne raporty dla zarządu, zawierające wyniki KPI oraz rekomendacje działań doskonalących.
6. **Analiza kosztów i efektywności** – ocena zwrotu z inwestycji (ROI) w systemy bezpieczeństwa w kontekście zredukowanego ryzyka i uniknięty kosztów związanych z incydentami.

Biorąc pod uwagę wyszczególnione czynniki, w tabeli nr 32 zaproponowano wskaźniki na potrzeby monitorowania i ewaluacji.

Tabela 32 Propozycja wskaźników monitorowania i ewaluacji

Obszar monitorowania	Wskaźnik KPI	Cel	Narzędzie
Zarządzanie incydentami	Średni czas reakcji na incydent (TRT)	Skrócenie czasu reakcji o 20%	SIEM
Świadomość pracowników	Procent pracowników przeszkolonych	100% przeszkolonych w ciągu 12 miesięcy	LMS
Zgodność z regulacjami	Procent zgodności z wymaganiami regulacyjnymi	Utrzymanie 100% zgodności	Audyty
Efektywność systemów	Liczba zneutralizowanych zagrożeń w czasie rzeczywistym	Zwiększenie skuteczności o 15% rocznie	PSIM
Koszty bezpieczeństwa	ROI z inwestycji w systemy bezpieczeństwa	Wzrost ROI o 10% rocznie	Narzędzia analizy finansowej

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Monitorowanie i ewaluacja skuteczności wdrożenia systemu zarządzania bezpieczeństwem wymaga kompleksowego podejścia, integrującego analizę danych, ocenę wskaźników KPI oraz ciągłą adaptację strategii. Dlatego też, można zastosować harmonogram monitorowania i ewaluacji. Przykładowy harmonogram, obejmujący wskazanie działań oraz pożądanych rezultatów wraz z wyszczególnieniem tygodniowym, przedstawiono w tabeli nr 33.

Tabela 33 Przykładowy harmonogram monitorowania i ewaluacji

Tydzień	Działanie	Rezultat
1	Zbieranie danych operacyjnych i analiza wskaźników KPI	Raport wstępny dotyczący skuteczności działań
2	Przeprowadzenie audytów wewnętrznych	Wskazanie mocnych i słabych stron systemu
3	Benchmarking wyników i analiza ryzyka	Lista obszarów wymagających poprawy
4	Opracowanie działań korygujących i aktualizacja strategii	Zatwierdzony plan działań doskonalących
5	Wdrożenie działań korygujących	Monitorowanie efektów i raport końcowy
6	Przygotowanie raportu końcowego i prezentacja zarządowi	Decyzje strategiczne dotyczące dalszych inwestycji

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Mimo zaawansowania technologicznego, wdrożenie skutecznych systemów monitorowania i ewaluacji wiąże się z pewnymi wyzwaniami. Fragmentacja danych z różnych systemów może utrudniać ich integrację i analizę. Dodatkowo, dynamicznie zmieniające się zagrożenia w sektorze ICT wymagają stałego aktualizowania modeli i strategii bezpieczeństwa.

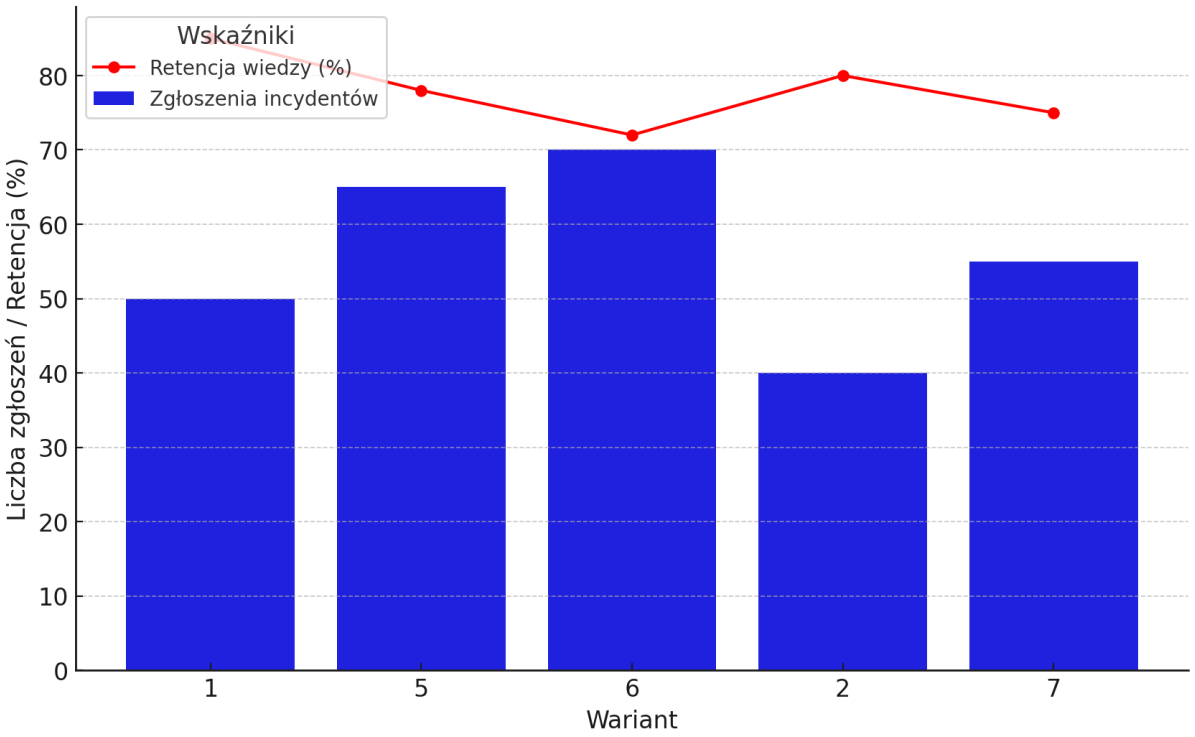
Koszty wdrożenia i utrzymania zaawansowanych narzędzi mogą być wysokie, a skuteczność monitorowania w dużej mierze zależy od zaangażowania pracowników, co wymaga dodatkowych działań motywacyjnych.

Aby sprostać tym wyzwaniom, organizacje powinny wdrażać zintegrowane podejście, umożliwiające analizę danych z różnych obszarów w jednym systemie. Kluczowe jest także ciągłe doskonalenie procesów poprzez aktualizację programów szkoleniowych i weryfikacyjnych oraz inwestycje w nowoczesne technologie automatyzujące monitorowanie i raportowanie. Regularne raportowanie wyników i rekomendacji do zarządu pozwala na bieżące monitorowanie skuteczności działań oraz podejmowanie strategicznych decyzji w celu dalszego doskonalenia systemu bezpieczeństwa.

6.4 Optymalizacja modelu w oparciu o wyniki wdrożenia

Optymalizacja modelu zarządzania bezpieczeństwem w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych (ICT) wymaga dokładnego przeglądu wyników wdrożenia oraz zidentyfikowania obszarów, które mogą zostać usprawnione. Poniżej przedstawiono szczegółowy plan optymalizacji oparty na wynikach 9 wariantów wdrożenia, wskaźnikach KPI oraz analizie monitorowania i ewaluacji skuteczności.

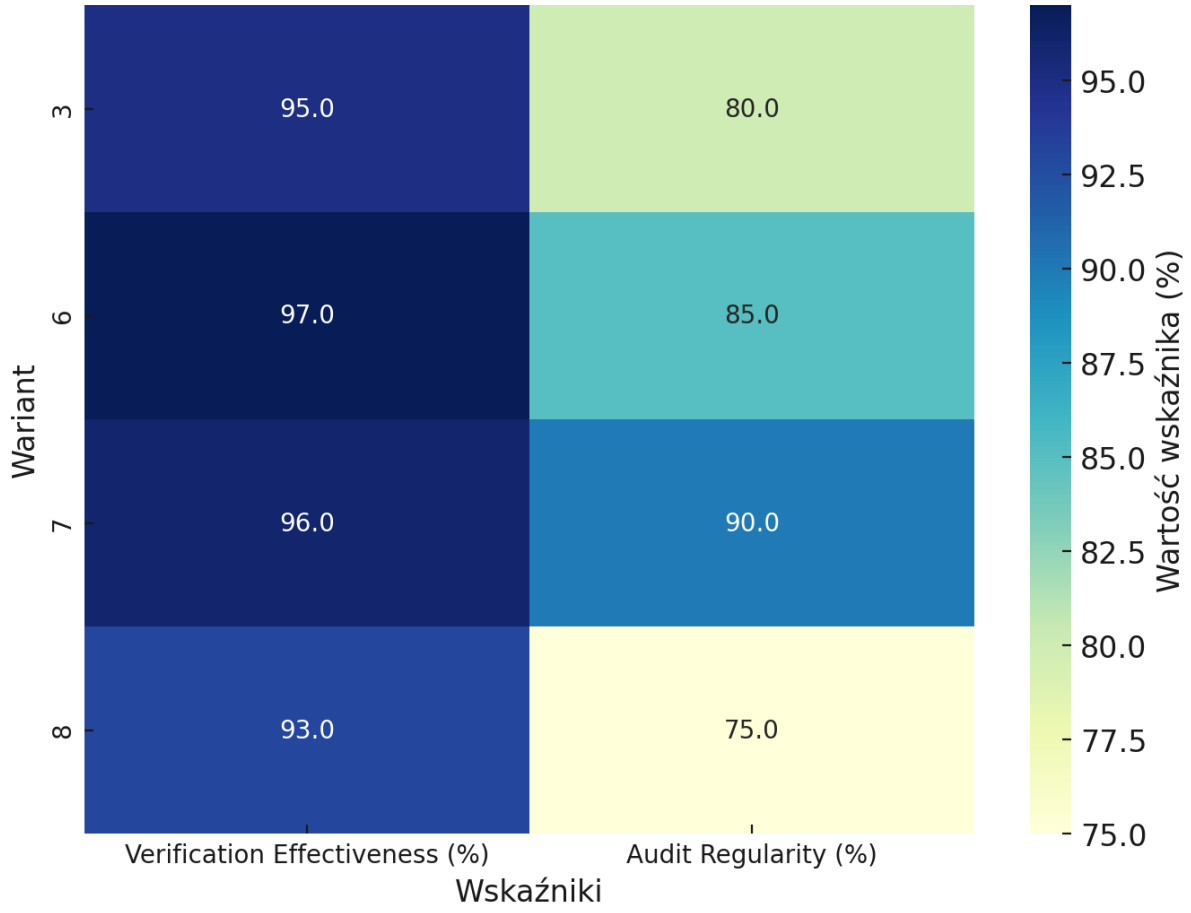
Symulacja wdrożenia różnych ścieżek zarządzania bezpieczeństwem ukazała istotne różnice w efektywności poszczególnych elementów systemu. Analiza świadomości zagrożeń wykazała wzrost liczby zgłaszanych incydentów wśród pracowników objętych kampaniami edukacyjnymi (warianty 1, 5, 6), co świadczy o wyższej czujności. Jednak ankiety ujawniły, że działy niezwiązane bezpośrednio z technologią, takie jak administracja, wykazują niższy poziom świadomości zagrożeń. Podobnie szkolenia (warianty 2, 5, 7) znacząco zwiększyły wiedzę pracowników, ale obserwowany spadek retencji wiedzy po sześciu miesiącach wskazuje na potrzebę wdrożenia mechanizmów przypominających, takich jak e-learning czy krótkie quizy. Powyższą obserwację przedstawiono na wykresie nr 28.



Wykres 28 Liczba zgłaszanych incydentów i retencja wiedzy
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Przedstawiony wykres ilustruje wzrost liczby raportowanych incydentów (przedstawionych za pomocą słupków) w tych wariantach, które zostały objęte działaniami edukacyjnymi, szczególnie w wariantach 1, 5 i 6. Jednocześnie widoczny jest trend spadkowy w zakresie retencji wiedzy w dłuższym okresie, co zostało zobrazowane za pomocą linii. Taka sytuacja wskazuje na konieczność wdrożenia dodatkowych mechanizmów wspomagających utrwalanie wiedzy, takich jak przypomnienia czy regularne szkolenia odświeżające.

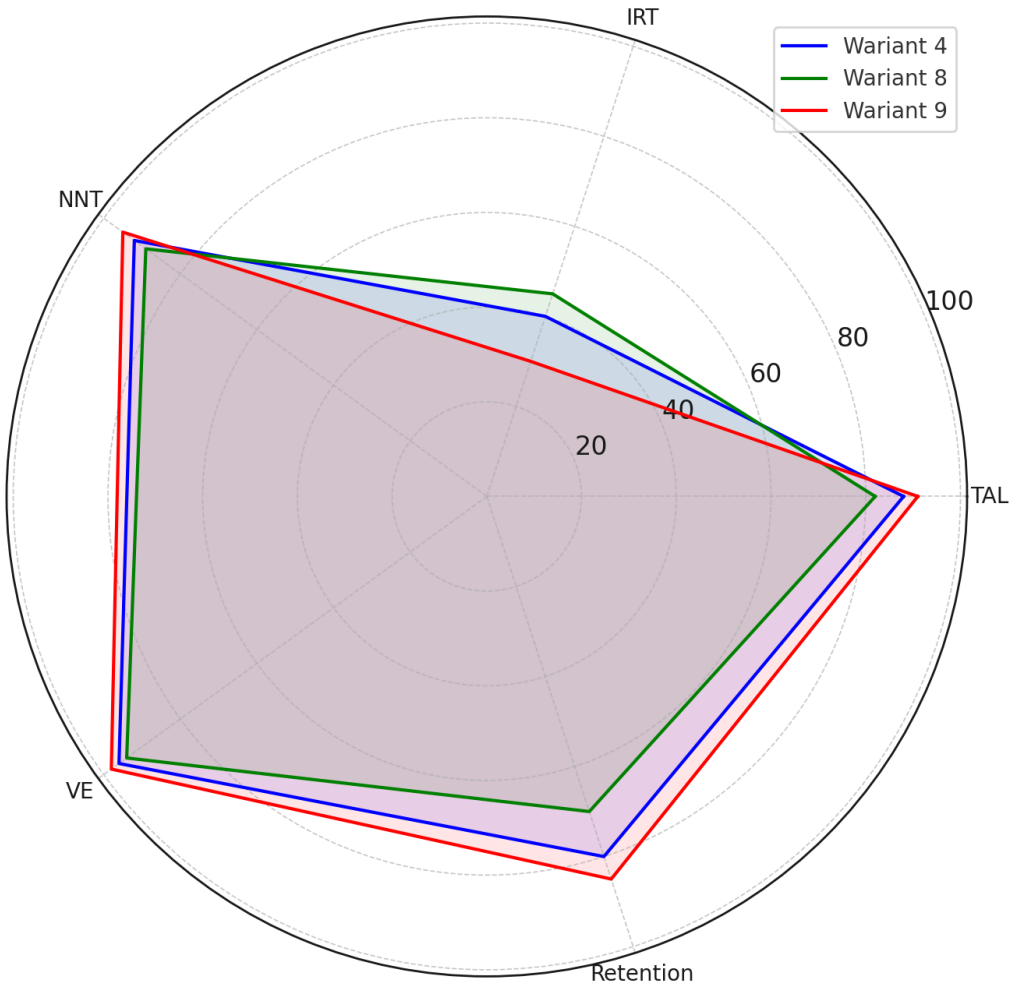
Procedury weryfikacji pracowników i dostawców (warianty 3, 6, 7, 8) przyniosły pozytywne rezultaty w redukcji ryzyka, lecz brak regularności audytów w niektórych działach wymaga poprawy organizacji tego procesu. Zaawansowane zabezpieczenia fizyczne i cyfrowe (warianty 4, 8, 9) wykazały wysoką skuteczność, jednak integracja systemów pozostaje wyzwaniem technologicznym, które należy adresować priorytetowo. Obserwacje zostały przedstawione na wykresie nr 29.



Wykres 29 Mapa cieplna skuteczności procedur weryfikacyjnych
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Mapa cieplna obrazuje zróżnicowanie w poziomie efektywności procesów weryfikacyjnych oraz regularności przeprowadzanych audytów w wariantach 3, 6, 7 i 8. Obszary oznaczone kolorem zielonym wskazują na wysoką skuteczność tych działań, natomiast jaśniejsze odcienie sygnalizują te aspekty, które wymagają dalszej optymalizacji i doskonalenia.

Kluczowe wskaźniki optymalizacyjne stanowią podstawę oceny skuteczności działań i definiowania docelowego poziomu efektywności. Wykres nr 30 przedstawia porównanie wskaźników dla wariantu 4, 8 oraz 9.



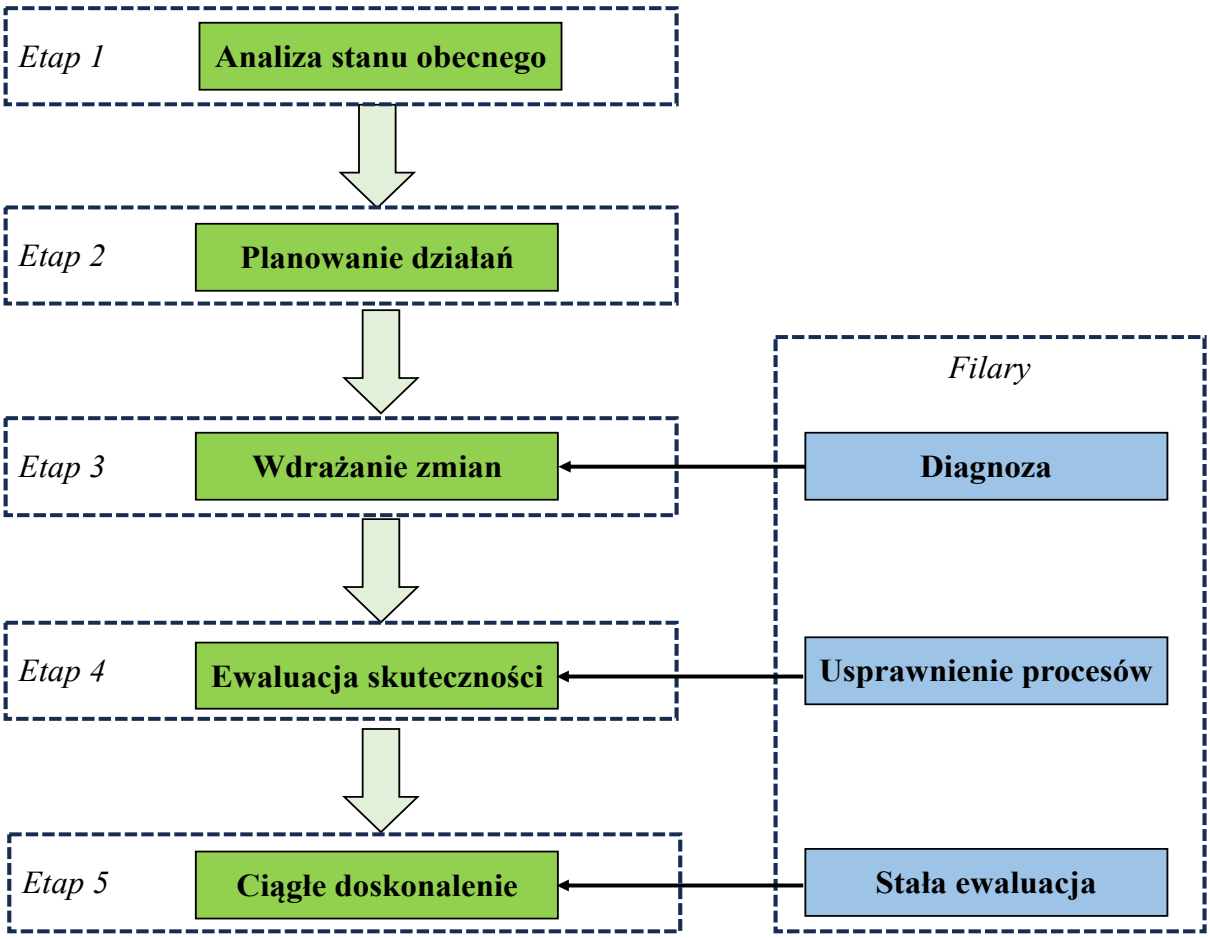
Wykres 30 Porównanie kluczowych wskaźników w wybranych wariantach
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Wykres radarowy przedstawia porównanie kluczowych wskaźników efektywności (KPI) dla wariantów 4, 8 i 9. Wariant 9 charakteryzuje się najwyższymi wynikami we wszystkich analizowanych wskaźnikach, co wskazuje na jego kompleksową skuteczność. Wariant 8 natomiast wykazuje niedociągnięcia, zwłaszcza w obszarze retencji wiedzy oraz poziomu świadomości zagrożeń (TAL), co sugeruje konieczność wdrożenia działań naprawczych w tych kluczowych obszarach.

W obszarze zwiększania świadomości zagrożeń celem jest osiągnięcie poziomu ≥90% w każdym dziale, co można osiągnąć poprzez personalizację kampanii i wprowadzenie regularnych powtórek wiedzy. Retencja wiedzy po szkoleniach powinna wynosić ≥85% po sześciu miesiącach, co wymaga wdrożenia cyklicznych przypomnień e-learningowych oraz elementów grywalizacji. Skuteczność weryfikacji pracowników i dostawców powinna osiągać ≥98%, a procesy weryfikacyjne można usprawnić poprzez automatyzację i cykliczne przeglądy. Neutralizacja zagrożeń powinna natomiast wynosić ≥95% w wykrywaniu incydentów, a średni

czas reakcji (IRT) ≤30 minut, co wymaga regularnych testów penetracyjnych i integracji systemów SIEM i PSIM.

Optymalizacja modelu zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych (ICT) wymaga wdrożenia wieloetapowego podejścia, które umożliwia dostosowanie systemu do dynamicznie zmieniającego się środowiska oraz skuteczną eliminację zidentyfikowanych luk. Główne działania optymalizacyjne obejmują pięć kluczowych etapów: analizę obecnego stanu, planowanie działań, wdrażanie zmian, ewaluację skuteczności oraz ciągłe doskonalenie. Uzupełnieniem tego procesu jest strategia składająca się z trzech podstawowych filarów: diagnozy, usprawnienia procesów i stałej ewaluacji. Kluczowe etapy optymalizacji w relacji do strategii zostały przedstawione na rysunku nr 30.



Rysunek 30 Kluczowe etapy optymalizacji w relacji do strategii
Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Optymalizacja modelu zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych (ICT) wymaga wdrożenia wieloetapowego podejścia, które umożliwia dostosowanie systemu do dynamicznie zmieniającego się środowiska oraz skuteczną eliminację zidentyfikowanych luk. Główne działania

optymalizacyjne obejmują pięć kluczowych etapów: analizę obecnego stanu, planowanie działań, wdrażanie zmian, ewaluację skuteczności oraz ciągłe doskonalenie. Uzupełnieniem tego procesu jest strategia składająca się z trzech podstawowych filarów: diagnozy, usprawnienia procesów i stałej ewaluacji.

Pierwszy etap – analiza obecnego stanu – koncentruje się na identyfikacji mocnych i słabych stron istniejącego modelu zarządzania bezpieczeństwem. W tym celu zbierane są dane z systemów monitorujących, takich jak SIEM i PSIM, wyniki audytów, testów penetracyjnych oraz ankiety pracownicze. Na podstawie tych danych przeprowadzana jest ocena wskaźników KPI, takich jak poziom świadomości zagrożeń (TAL), czas reakcji na incydenty (IRT) czy skuteczność weryfikacji (VE). Wyniki analizy pozwalają określić obszary priorytetowe, takie jak działy charakteryzujące się niskim poziomem świadomości zagrożeń lub przestarzałe systemy zabezpieczeń technicznych.

Drugi etap, planowanie działań optymalizacyjnych, zakłada opracowanie kompleksowego harmonogramu dostosowanego do specyficznych potrzeb organizacji. Cele optymalizacyjne są precyzyjnie definiowane dla każdego obszaru, co umożliwia efektywne alokowanie zasobów finansowych i technologicznych. Wdrażane są również narzędzia wspierające, takie jak platformy LMS do zarządzania szkoleniami, zautomatyzowane systemy weryfikacji pracowników i dostawców czy zintegrowane rozwiązania SIEM/PSIM. Kluczowym rezultatem tego etapu jest szczegółowy plan działań, obejmujący priorytety, zadania i odpowiedzialności.

Trzeci etap, wdrażanie działań optymalizacyjnych, obejmuje realizację zaplanowanych zmian, takich jak aktualizacja programów szkoleniowych, automatyzacja procesów weryfikacyjnych oraz modernizacja zabezpieczeń technicznych. Wdrożone zostają nowe procedury, które integrują szkolenia, weryfikacje i zabezpieczenia w jeden spójny system zarządzania bezpieczeństwem. Przeprowadzane są również symulacje incydentów i warsztaty praktyczne, które zwiększają zaangażowanie pracowników oraz umożliwiają identyfikację potencjalnych słabości systemu.

Czwarty etap, ewaluacja skuteczności, zakłada ocenę osiągniętych wyników na podstawie zebranych danych post-implementacyjnych oraz wskaźników KPI. Analiza trendów w poziomie świadomości zagrożeń, retencji wiedzy po szkoleniach czy liczby wykrytych i zneutralizowanych incydentów pozwala na identyfikację obszarów wymagających dalszych usprawnień. Regularne raporty przedstawiane zarządowi umożliwiają monitorowanie postępów oraz podejmowanie decyzji dotyczących przyszłych działań.

Piąty etap, ciągłe doskonalenie, obejmuje regularne audyty, aktualizację procesów oraz dostosowanie wskaźników KPI do zmieniających się warunków organizacyjnych

i technologicznych. Kluczowym elementem tego etapu jest monitorowanie nowych zagrożeń oraz rozwój technologii, co pozwala na bieżące modyfikowanie strategii bezpieczeństwa. Działania te zapewniają stałą skuteczność i adekwatność modelu do wymagań dynamicznego otoczenia.

Proces optymalizacji modelu zarządzania bezpieczeństwem w sektorze technologii informacyjno-komunikacyjnych (ICT) opiera się na danych uzyskanych z wdrożenia dziewięciu wariantów zarządzania oraz analizy kluczowych wskaźników efektywności (KPI). Optymalizacja obejmuje zarówno techniczne, jak i organizacyjne aspekty systemu, co pozwala na eliminację luk i zwiększenie efektywności działań w dynamicznym środowisku ICT. Biorąc pod uwagę powyższe, w tabeli nr 34 przedstawiono syntetyczny opis etapów optymalizacji modelu zarządzania bezpieczeństwem przedsiębiorstwa.

Tabela 34 Etapy optymalizacji modelu zarządzania bezpieczeństwem przedsiębiorstwa

Etap	Opis	Kluczowe działania	Rezultaty
1	Identyfikacja mocnych i słabych stron istniejącego modelu zarządzania bezpieczeństwem oraz zdiagnozowanie luk	– Zbieranie danych z systemów SIEM i PSIM, audytów oraz ankiet – Ocena wskaźników KPI, takich jak poziom świadomości zagrożeń (TAL) i czas reakcji na incydenty (IRT)	– Wytypowanie obszarów wymagających poprawy (np. niska świadomość zagrożeń w niektórych działach) – Opracowanie listy priorytetów i szczegółowy raport diagnostyczny
2	Opracowanie harmonogramu oraz zasobów wymaganych do wdrożenia działań optymalizacyjnych	– Ustalanie celów KPI dla poszczególnych obszarów – Przygotowanie narzędzi wspierających (np. platformy LMS, narzędzia automatyzacji weryfikacji)	– Kompleksowy plan działań uwzględniający priorytety i zasoby – Zdefiniowanie odpowiedzialności i harmonogramu
3	Realizacja zaplanowanych działań optymalizacyjnych w celu eliminacji zidentyfikowanych luk	– Modernizacja systemów bezpieczeństwa (np. integracja SIEM i PSIM) – Automatyzacja weryfikacji pracowników i dostawców.	– Aktualizacja procesów i procedur w organizacji – Zwiększenie poziomu bezpieczeństwa dzięki realizacji priorytetów
4	Ocena osiągniętych wyników na podstawie wskaźników efektywności (KPI) oraz analiza trendów	– Porównanie wyników z założonymi celami KPI	– Identyfikacja dalszych obszarów wymagających poprawy

Etap	Opis	Kluczowe działania	Rezultaty
		– Przygotowanie raportów z wynikami dla zarządu	– Określenie sukcesów i niedociągnięć we wdrożeniu
5	Regularna aktualizacja systemu, procedur i wskaźników KPI w odpowiedzi na zmieniające się warunki	– Organizowanie cyklicznych audytów i przeglądów systemów – Dostosowanie procedur do nowych zagrożeń i technologii	– Zwiększenie efektywności i adekwatności systemu zarządzania bezpieczeństwem – Ciągłe dostosowanie modelu do dynamicznego środowiska

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Ponadto, w tabeli nr 35 przedstawiono szczegółowe opracowanie kluczowych wskaźników efektywności (KPI) opracowanych dla optymalizacji modelu zarządzania bezpieczeństwem w przedsiębiorstwach sektora ICT. Każdy wskaźnik został omówiony w kontekście jego celu, znaczenia oraz sposobu interpretacji wyników.

Tabela 35 Etapy optymalizacji modelu zarządzania bezpieczeństwem przedsiębiorstwa

Wskaźnik (KPI)	Opis	Cel optymalizacyjny
TAL – Poziom świadomości zagrożeń	Mierzy odsetek pracowników świadomych zagrożeń w kontekście bezpieczeństwa organizacji. Dane pozyskiwane są z ankiet, testów wiedzy oraz zgłoszeń incydentów	Osiągnięcie poziomu świadomości **≥90%** w każdym dziale, z uwzględnieniem różnic między działami technicznymi i nietechnicznymi
Retencja wiedzy po szkoleniach	Wskaźnik ten określa, jaki procent wiedzy pracownicy zachowali po sześciu miesiącach od ukończenia szkoleń. Pozyskiwane dane bazują na testach powtórkowych	Retencja wiedzy na poziomie **≥85%** dzięki zastosowaniu cyklicznych przypomnień (e-learning) i grywalizacji w szkoleniach.
VE – Skuteczność weryfikacji	Mierzy procent pracowników i dostawców, którzy zostali zweryfikowani zgodnie z wymaganiami organizacji. Wskaźnik obejmuje audyty oraz automatyczne przeglądy.	Zapewnienie skuteczności weryfikacji na poziomie **≥98%**, co minimalizuje ryzyko związane z niewłaściwymi kontrahentami i pracownikami.
NNT – Neutralizacja zagrożeń	Wskaźnik określa odsetek wykrytych zagrożeń, które zostały skutecznie zneutralizowane przez systemy ochronne, takie jak SIEM czy PSIM	**≥95% neutralizacji zagrożeń** w czasie rzeczywistym, co wymaga skutecznej integracji systemów ochronnych oraz regularnych testów.
IRT – Czas reakcji na incydenty	Mierzy średni czas (w minutach) potrzebny na podjęcie działań od momentu wykrycia incydentu. Dane zbierane są z logów systemów SIEM/PSIM	Skrócenie czasu reakcji na incydenty do **≤30 minut**, co wymaga wprowadzenia procedur automatyzacji i szybkiej analizy zagrożeń.

Źródło: opracowanie własne na podstawie przeprowadzonych badań empirycznych.

Optymalizacja modelu zarządzania bezpieczeństwem w organizacjach sektora ICT wymaga wykorzystania wskaźników efektywności (KPI) jako narzędzi oceny skuteczności

wdrożonych działań. Jednym z kluczowych wskaźników jest **TAL – poziom świadomości zagrożeń**, który mierzy zdolność pracowników do rozpoznawania i unikania ryzykownych działań. Wskaźnik ten jest szczególnie istotny, gdyż wysoka świadomość umożliwia wczesne wykrywanie incydentów oraz ograniczenie ich negatywnych skutków. Osiągnięcie wartości ≥90% wskazuje, że większość pracowników posiada odpowiedni poziom wiedzy, natomiast niższe wartości sygnalizują konieczność zwiększenia nakładów na szkolenia.

Drugim istotnym wskaźnikiem jest **retencja wiedzy po szkoleniach**, który ocenia trwałość efektów programów edukacyjnych. Szkolenia stanowią kosztowny element strategii bezpieczeństwa, dlatego ich długoterminowa skuteczność ma kluczowe znaczenie. Wartość ≥85% po sześciu miesiącach od zakończenia szkolenia wskazuje na właściwe dostosowanie programów do potrzeb uczestników. W przypadku niskiej retencji wiedzy rekomendowane jest wdrożenie mechanizmów wspierających, takich jak e-learning czy interaktywne przypomnienia, aby efekty szkoleniowe były bardziej trwałe.

VE – skuteczność weryfikacji stanowi kluczowy wskaźnik oceniający jakość procesów sprawdzających dla pracowników oraz dostawców. Regularna i dokładna weryfikacja jest niezbędna, aby minimalizować ryzyko wynikające z potencjalnych zagrożeń wewnętrznych i zewnętrznych. Osiągnięcie wartości ≥98% świadczy o wysokim poziomie zaufania do osób i organizacji związanych z przedsiębiorstwem. Wartości poniżej tego progu mogą wskazywać na potrzebę zastosowania bardziej zaawansowanych narzędzi weryfikacyjnych oraz usystematyzowania procedur.

Wskaźnik **NNT – neutralizacja zagrożeń** określa zdolność organizacji do skutecznego eliminowania potencjalnych incydentów zanim wpłyną one negatywnie na jej funkcjonowanie. Jego wysoka wartość (≥95%) jest dowodem na efektywność systemów ochronnych, takich jak SIEM czy PSIM, oraz procedur reagowania. Niskie wartości tego wskaźnika mogą sygnalizować braki w infrastrukturze technicznej lub niedostateczne zasoby ludzkie. Regularne testy penetracyjne oraz optymalizacja procesów operacyjnych pozwalają zwiększyć skuteczność w neutralizowaniu zagrożeń.

IRT – czas reakcji na incydenty mierzy zdolność organizacji do szybkiego podejmowania działań w odpowiedzi na wykryte zagrożenia. Krótki czas reakcji (≤30 minut) minimalizuje straty oraz zmniejsza ryzyko eskalacji problemów. Wskaźnik ten odzwierciedla zarówno skuteczność procedur, jak i dostępność zasobów technicznych oraz ludzkich. Dłuższy czas reakcji sugeruje konieczność rewizji strategii, w tym lepszego wykorzystania technologii monitorujących oraz poprawy koordynacji zespołów odpowiedzialnych za bezpieczeństwo.

Wskaźniki efektywności (KPI) są niezbędnym narzędziem w procesie optymalizacji systemu zarządzania bezpieczeństwem. Każdy z omówionych wskaźników dostarcza danych

umożliwiających identyfikację obszarów wymagających usprawnienia oraz ocenę skuteczności wdrożonych działań. Regularna analiza KPI pozwala na podejmowanie decyzji opartych na danych, co prowadzi do zwiększenia efektywności i odporności organizacji na zagrożenia. Systematyczne monitorowanie wskaźników oraz wdrażanie działań doskonalących przyczyniają się do ciągłego rozwoju strategii bezpieczeństwa w dynamicznie zmieniającym się środowisku ICT.

Proces optymalizacji wiąże się jednak z pewnymi ryzykami. Wysokie koszty wdrożenia i utrzymania systemów można zminimalizować poprzez priorytetyzację działań w kluczowych obszarach. Niski poziom zaangażowania pracowników wymaga zastosowania działań motywacyjnych, takich jak nagrody za udział w szkoleniach i poprawę wyników KPI. Brak kompetencji technicznych w organizacji można rozwiązać poprzez odpowiednie szkolenia zespołów wdrożeniowych. Dzięki takim działaniom można skutecznie zarządzać ryzykami i zwiększać efektywność systemu bezpieczeństwa.

Podsumowując, optymalizacja modelu zarządzania bezpieczeństwem w sektorze ICT wymaga systemowego podejścia opartego na danych i technologii. Kluczowe działania obejmują personalizację kampanii edukacyjnych, automatyzację procesów weryfikacji, integrację systemów zabezpieczeń oraz regularne monitorowanie wyników KPI. Realizacja tych kroków pozwoli na zwiększenie efektywności działań oraz maksymalizację poziomu bezpieczeństwa w organizacji. Wdrażanie strategii optymalizacyjnej powinno być procesem ciągłym, dostosowywanym do dynamicznie zmieniającego się otoczenia.

PODSUMOWANIE

W dobie globalizacji i dynamicznego rozwoju technologii przedsiębiorstwa funkcjonujące w sektorze technologii informacyjno-komunikacyjnych oraz w innych wysoko innowacyjnych branżach stają w obliczu coraz bardziej złożonych zagrożeń. Jednym z kluczowych wyzwań współczesnego zarządzania bezpieczeństwem jest szpiegostwo korporacyjne, które stanowi istotne ryzyko dla stabilności i konkurencyjności organizacji. Zjawisko to, polegające na świadomym i nielegalnym pozyskiwaniu poufnych informacji dla uzyskania przewagi konkurencyjnej, zyskuje na znaczeniu w erze cyfrowej, gdzie informacje są jednym z najważniejszych zasobów strategicznych organizacji. Wpływ szpiegostwa korporacyjnego obejmuje straty finansowe, utratę przewagi rynkowej i problemy wizerunkowe organizacji, co podkreśla konieczność wdrożenia kompleksowych strategii zarządzania bezpieczeństwem.

Efektywna ochrona przed zagrożeniami, takimi jak szpiegostwo korporacyjne, wymaga zintegrowanego podejścia, które łączy zaawansowane technologie ochrony z rozwojem świadomości i kompetencji pracowników. Kluczowym aspektem skutecznej obrony jest edukacja, która umożliwia pracownikom identyfikację potencjalnych zagrożeń oraz właściwe reagowanie. Problem ten szczególnie dotyka sektorów o wysokiej dynamice innowacji, takich jak ICT, gdzie przedsiębiorstwa, często dysponujące unikalnym know-how, są atrakcyjnym celem dla konkurentów i grup przestępczych. Zarządzanie bezpieczeństwem staje się w tym kontekście wyzwaniem nie tylko dla działów technologicznych i bezpieczeństwa, ale również dla organów zarządczych, które muszą uwzględniać wielowymiarowość zagrożeń w procesie podejmowania decyzji strategicznych.

Podsumowując, współczesne przedsiębiorstwa muszą przyjąć proaktywną postawę wobec ochrony wrażliwych informacji, integrując nowoczesne technologie z międzynarodowymi standardami bezpieczeństwa oraz systematycznym doskonaleniem kompetencji pracowników. Takie podejście nie tylko minimalizuje ryzyko strat wynikających z szpiegostwa korporacyjnego, ale również wzmacnia odporność organizacji na dynamiczne zmiany w środowisku biznesowym, stanowiąc fundament jej stabilnego i konkurencyjnego funkcjonowania.

Rozdział pierwszy pracy doktorskiej, stanowi kluczowy fundament teoretyczny, analizując złożoność pojęcia bezpieczeństwa w kontekście współczesnych organizacji. Autor podejmuje szczegółową charakterystykę bezpieczeństwa jako stanu niezagrożenia oraz procesu adaptacyjnego, podkreślając dualistyczną naturę tego terminu. Przeanalizowano ewolucję jego znaczenia w obszarze organizacyjnym, szczególnie w odniesieniu do postępu technologicznego

i społeczno-ekonomicznego. Bezpieczeństwo przedstawiono jako integralny element zarządzania strategicznego, zapewniający stabilność operacyjną, ochronę zasobów i osiąganie celów organizacyjnych. Rozdział wyróżnia kluczowe wymiary bezpieczeństwa – finansowe, technologiczne, informacyjne, fizyczne i relacyjne – uwzględniając ich wzajemne zależności w holistycznym podejściu do zarządzania. Omówiono również różnorodne modele, takie jak podejścia zasobowe, procesowe, zadaniowe i systemowe, akcentując znaczenie elastyczności i adaptacji w obliczu dynamicznych zmian w otoczeniu zewnętrznym. Przedstawione w rozdziale wyzwania, w tym ochrona informacji i przeciwdziałanie cyberzagrożeniom, wskazują na konieczność integracji nowoczesnych technologii ochronnych, rozwoju świadomości pracowników oraz przestrzegania standardów międzynarodowych. Autor podkreśla, że skuteczne zarządzanie bezpieczeństwem wymaga interdyscyplinarnego, dynamicznego podejścia, łączącego aspekty technologiczne, proceduralne i ludzkie w celu sprostania współczesnym wyzwaniom.

Drugi rozdział omawia kluczowe zagadnienia zarządzania bezpieczeństwem informacyjnym. Stanowi to podstawę teoretyczną i praktyczną dla opracowania polityk ochrony danych. Autor szczegółowo omawia interdyscyplinarny charakter bezpieczeństwa informacyjnego, wskazując na różnice między tym pojęciem a bezpieczeństwem informacji, szczególnie w kontekście ochrony poufności, integralności i dostępności danych. Rozdział identyfikuje główne przesłanki wdrażania systemów zarządzania bezpieczeństwem informacji (SZBI), takie jak regulacje prawne, w tym RODO, oraz zagrożenia cybernetyczne, które mogą destabilizować działalność przedsiębiorstw. Przeanalizowano również standardy międzynarodowe, takie jak ISO/IEC 27001, TISM, TRA i COBIT, podkreślając ich znaczenie w kontekście specyfiki organizacyjnej. Szczególną uwagę poświęcono strategiom ochrony informacji, w tym politykom bezpieczeństwa, zarządzaniu ryzykiem oraz wyzwaniom wynikającym z różnorodności technologii i podejść ludzkich. Autor dokonuje także klasyfikacji zagrożeń informacyjnych, wskazując na konieczność ich monitorowania i dynamicznego zarządzania. Podkreślono kluczową rolę dobrze zdefiniowanej polityki bezpieczeństwa, która powinna uwzględniać zarówno aspekty techniczne, jak i edukacyjne, wspierając rozwój świadomości pracowników. Rozdział stanowi kompleksowe ujęcie teorii i praktyki zarządzania bezpieczeństwem informacyjnym, wskazując, że skuteczna implementacja wymaga zintegrowanego podejścia, uwzględniającego technologie, procesy oraz zasoby ludzkie, i powinna być nieodzownym elementem strategii organizacyjnej.

Trzeci rozdział rozprawy doktorskiej, poświęcony został analizie istoty szpiegostwa korporacyjnego w kontekście zagrożeń, z którymi mierzą się organizacje sektora ICT. Autor precyzyjnie definiuje szpiegostwo korporacyjne, odróżniając je od podobnych pojęć, takich jak

szpiegostwo gospodarcze czy przemysłowe, podkreślając jego szeroki zakres działań zmierzających do nielegalnego pozyskania strategicznych informacji w celu uzyskania przewagi konkurencyjnej. Szczegółowo omówiono stosowane metody, takie jak phishing, spyware, socjotechnika czy wywiad jawnoźródłowy (OSINT), oraz wskazano na wykorzystywanie zaawansowanych technologii i luk w systemach zabezpieczeń. Zidentyfikowano szczególne ryzyka sektora ICT, w tym kradzież danych klientów, know-how oraz innowacyjnych technologii, co wynika z intensywnej konkurencji i dynamicznego rozwoju technologii w tej branży. Rozdział podkreśla znaczenie dostosowania strategii zarządzania bezpieczeństwem do specyficznych wyzwań wynikających ze szpiegostwa korporacyjnego, akcentując potrzebę inwestycji w nowoczesne technologie ochrony, podnoszenia kompetencji pracowników oraz budowania organizacyjnej kultury bezpieczeństwa.

Rozdziały piąty i szósty niniejszej dysertacji przedstawiają szczegółowe wyniki badań empirycznych oraz płynące z nich wnioski, które stały się podstawą opracowania modelu zarządzania bezpieczeństwem dedykowanego przedsiębiorstwom działającym w sektorze technologii informacyjno-komunikacyjnych (ICT). Głównym celem przeprowadzonych badań było określenie kluczowych determinant skutecznego zarządzania bezpieczeństwem, z uwzględnieniem zróżnicowanego postrzegania zagrożeń przez pracowników oraz oceny funkcjonalności opracowanego modelu. Wyniki badań jednoznacznie potwierdziły trafność proponowanego podejścia, które integruje różnorodne perspektywy postrzegania zagrożeń wewnątrz organizacji.

Opracowany model, który został przetestowany za pomocą symulacji, oferuje praktyczne narzędzia umożliwiające dostosowanie działań prewencyjnych i ochronnych do szczególnych wymagań zarówno organizacji, jak i jej pracowników. Wyniki badań wskazują, że skuteczność zarządzania bezpieczeństwem w sektorze ICT opiera się na synergii trzech kluczowych obszarów: zaawansowanych technologii ochronnych, efektywnych procedur zarządczych oraz świadomości i zaangażowania pracowników, wspieranych przez aktywne działania liderów organizacyjnych. Model ten pozwala na elastyczną adaptację strategii ochrony do dynamicznie zmieniającego się środowiska technologicznego, wspierając tym samym trwałość i efektywność systemów zarządzania bezpieczeństwem w przedsiębiorstwach tego sektora.

Zgodnie z metodyką pisania rozpraw doktorskich, aby osiągnąć założone cele pracy, opisano proces badawczy, który umożliwił weryfikację postawionych hipotez oraz rozwiązanie określonych problemów badawczych. Sformułowany główny problem badawczy dotyczył pytania, jakie wyzwania dla zarządzania bezpieczeństwem w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych wynikają ze zróżnicowanego postrzegania przez

pracowników zagrożeń ze strony szpiegostwa korporacyjnego. Rozszerzając tę problematykę, postawiono problemy szczegółowe, które w formie pytań dotyczyły jaką rolę i znaczenie odgrywa bezpieczeństwo w zarządzaniu przedsiębiorstwem sektora technologii informacyjno-komunikacyjnych, jakie przesłanki i wyzwania wpływają na implementację zarządzania bezpieczeństwem informacyjnym w organizacji, w jaki sposób zagrożenia wynikające ze szpiegostwa korporacyjnego wpływają na zarządzanie bezpieczeństwem przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych, w jaki sposób można ocenić poziom świadomości pracowników na temat zagrożeń wynikających ze szpiegostwa korporacyjnego oraz skuteczność zarządzania bezpieczeństwem oraz jaka jest zależność pomiędzy poziomem świadomości pracowników a skutecznością zarządzania bezpieczeństwem w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych.

Postawione szczegółowe problemy badawcze miały na celu kompleksowe rozwinięcie głównego celu badawczego. W rezultacie doprowadziły one do opracowania jednej hipotezy głównej, zakładającej, że zarządzanie bezpieczeństwem przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych powinno uwzględniać różnice w postrzeganiu przez pracowników zagrożeń wynikających ze szpiegostwa korporacyjnego. Jednocześnie postawiono cztery hipotezy szczegółowe, koncentrujące się na tym, iż racjonalne zarządzanie bezpieczeństwem, w tym wdrażanie odpowiednich procesów decyzyjnych oraz strategii identyfikacji i minimalizacji ryzyka, warunkuje ciągłość działania organizacji oraz zabezpieczenie jej kluczowych zasobów. Ponadto, stosowanie odpowiednich standardów i norm w zarządzaniu bezpieczeństwem informacji, pozwala na skuteczne rozpoznawanie zagrożeń, kształtując poziom ochrony danych oraz tajemnicy przedsiębiorstwa. Również, że szpiegostwo korporacyjne stawia przed zarządzaniem bezpieczeństwem przedsiębiorstwa konieczność przeciwdziałania środkom i metodom dostępu do danych oraz pozyskiwania informacji w celu zdobycia przewagi konkurencyjnej. Finalnie, że skuteczne zarządzanie bezpieczeństwem przedsiębiorstw sektora technologii informacyjno-komunikacyjnych wymaga uwzględnienia sposobu, w jaki pracownicy postrzegają szpiegostwo korporacyjne.

Metodyka badań, opisana w tym rozdziale, stanowiła solidny fundament dla przeprowadzenia analizy empirycznej i zweryfikowania przyjętych założeń, zapewniając jednocześnie logiczne i systematyczne podejście do badanej problematyki.

Dzięki przeprowadzeniu wszechstronnych analiz teoretycznych i praktycznych oraz realizacji badań empirycznych, udało się w pełni zrealizować główny cel rozprawy, jakim było opracowanie modelu zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych, który uwzględnia zróżnicowane postrzeganie zagrożeń wynikających ze szpiegostwa korporacyjnego przez pracowników, w celu zwiększenia ochrony

danych i tajemnicy przedsiębiorstwa. Model ten uwzględnia różnice w percepcji zagrożeń związanych ze szpiegostwem korporacyjnym przez różne grupy pracowników. Powstał w wyniku szczegółowych analiz teoretycznych, badań empirycznych oraz symulacji wdrożeniowych, co zapewniło jego solidne podstawy metodologiczne i praktyczne.

Stworzony model zarządzania bezpieczeństwem integruje trzy kluczowe aspekty: techniczny, proceduralny i ludzki. Uwzględnia istotne elementy takie jak identyfikacja zagrożeń, jasny podział ról i odpowiedzialności, rozwój świadomości pracowników, wykorzystanie nowoczesnych technologii ochronnych oraz bieżące monitorowanie skuteczności działań. Jego konstrukcja uwzględnia specyfikę sektora ICT, charakteryzującego się dynamicznymi zmianami technologicznymi i wymagającego elastyczności oraz zdolności adaptacyjnych.

Badania empiryczne wykazały znaczące różnice w poziomie świadomości i percepcji zagrożeń wśród pracowników, co zostało uwzględnione w modelu. Proponuje on personalizowane szkolenia oraz zindywidualizowane działania prewencyjne, co zwiększa skuteczność zarządzania bezpieczeństwem w organizacji. Symulacje wdrożeniowe dowiodły, że model wspiera wzrost ochrony kluczowych zasobów przedsiębiorstwa, takich jak dane i tajemnice organizacyjne. Zastosowane mechanizmy ciągłego doskonalenia, obejmujące monitorowanie wskaźników efektywności, takich jak czas reakcji na incydenty czy poziom świadomości pracowników, dodatkowo wzmacniają długoterminową skuteczność zarządzania bezpieczeństwem.

Przeprowadzone testy praktyczne potwierdziły nie tylko teoretyczną zasadność modelu, ale również jego funkcjonalność w rzeczywistych warunkach. Jego wdrożenie przyczynia się do ograniczenia ryzyka związanego ze szpiegostwem korporacyjnym, oferując organizacjom skuteczne narzędzie ochrony. Podsumowując, autor dysertacji zrealizował postawiony cel badawczy, tworząc innowacyjny i kompleksowy model zarządzania bezpieczeństwem, który odpowiada specyfice sektora ICT. Praca dostarcza istotnych narzędzi wspierających ochronę danych i tajemnic przedsiębiorstwa, co ma kluczowe znaczenie w kontekście globalnych zagrożeń informacyjnych.

W toku rozważań teoretycznych oraz badań empirycznych hipoteza główna została pozytywnie zweryfikowana. Jej formułowanie oparto na połączeniu metody dedukcyjnej, wynikającej z analizy teorii oraz indukcyjnej, opartej na obserwacjach empirycznych, co zapewniło spójność metodologiczną. Hipoteza została skonstruowana w sposób przejrzysty, spełniając kluczowe wymogi badawcze, w tym precyzyjne określenie relacji między zmiennymi, ich charakteru (dodatniego lub ujemnego), a także warunków, w jakich relacje te występują. Jednocześnie zadbano, aby była ona weryfikowalna za pomocą dostępnych narzędzi

badawczych i pozbawiona elementów wartościujących[378], co zwiększa jej wiarygodność i zastosowanie w praktyce badawczej. W wyniku przeprowadzenia wielowymiarowych analiz teoretycznych, badań empirycznych oraz symulacji wdrożeniowych potwierdzono zasadność hipotezy głównej, sformułowanej jako zarządzanie bezpieczeństwem przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych powinno uwzględniać różnice w postrzeganiu przez pracowników zagrożeń wynikających ze szpiegostwa korporacyjnego.

Przedstawione badania i rozważania dowiodły, że efektywne zarządzanie bezpieczeństwem w sektorze ICT w dużej mierze zależy od uwzględnienia zróżnicowanego postrzegania zagrożeń przez pracowników różnych szczebli organizacyjnych. Analiza literatury przedmiotu wskazała, że percepcja zagrożeń wśród pracowników jest determinowana przez czynniki takie jak doświadczenie zawodowe, dostęp do szkoleń, zakres obowiązków czy poziom zaawansowania technologicznego w pracy. Wyniki teoretyczne dowiodły, że stosowanie jednolitego podejścia w zarządzaniu bezpieczeństwem może skutkować lukami w systemach ochrony, co podkreśla konieczność adaptacyjnych strategii uwzględniających różnice w poziomie świadomości zagrożeń wśród personelu.

Część empiryczna badań ujawniła wyraźne różnice w postrzeganiu ryzyka związanego ze szpiegostwem korporacyjnym. Wyniki ankiet wskazały, że pracownicy techniczni wykazują większą świadomość zagrożeń cybernetycznych, podczas gdy kadra administracyjna częściej bagatelizuje tego rodzaju ryzyka. Z kolei wyższa kadra zarządzająca lepiej rozumie strategiczne znaczenie ochrony danych, ale posiada mniejsze kompetencje w obszarze technicznych mechanizmów zabezpieczeń. Wywiady eksperckie potwierdziły, że uwzględnienie tych różnic w procesach zarządzania bezpieczeństwem umożliwia lepsze dopasowanie działań prewencyjnych i reaktywnych, takich jak personalizowane szkolenia i szczegółowe procedury postępowania w sytuacjach kryzysowych. Symulacje wdrożeniowe opracowanego modelu zarządzania bezpieczeństwem wykazały poprawę w kluczowych wskaźnikach skuteczności w organizacjach stosujących podejście uwzględniające różnorodność percepcji zagrożeń. W szczególności zauważono szybsze reakcje na incydenty, lepsze przestrzeganie polityk bezpieczeństwa przez pracowników oraz wyższą efektywność systemów zarządzania ryzykiem.

Podsumowując, pozytywna weryfikacja hipotezy głównej była możliwa dzięki wszechstronnemu uzasadnieniu teoretycznemu, przeprowadzeniu rzetelnych badań empirycznych oraz weryfikacji praktycznej opracowanego modelu. Wyniki jednoznacznie wskazują, że zarządzanie bezpieczeństwem w sektorze ICT powinno uwzględniać różnice

[378] C. Frankfort-Nachmias, D. Nachmias, *Metody badawcze w naukach społecznych*, Wydawnictwo Zysk i S-ka, Poznań 2001, s. 35.

w postrzeganiu zagrożeń przez pracowników, co umożliwia optymalizację strategii ochronnych, zwiększenie odporności organizacji na ryzyka związane ze szpiegostwem korporacyjnym oraz poprawę skuteczności działań prewencyjnych. Wnioski te mają istotne znaczenie dla rozwoju nauk o zarządzaniu i jakości, oferując jednocześnie cenne wskazówki dla praktyki zarządzania w dynamicznym środowisku sektora technologicznego.

Na podstawie przeprowadzonych analiz można stwierdzić, że zarówno główny cel, jak i cele szczegółowe wyznaczone w niniejszej pracy doktorskiej zostały w pełni zrealizowane. W trakcie realizacji celów dokonano weryfikacji zarówno hipotezy głównej, jak i hipotez szczegółowych, a także udzielono odpowiedzi na kluczowe pytania badawcze, związane z zidentyfikowanymi problemami badawczymi. Ponadto, dzięki zastosowanej oraz skutecznie przeprowadzonej procedurze badawczej, wszystkie hipotezy zostały zweryfikowane pozytywnie, co potwierdziło ich zasadność w sposób jednoznaczny i wolny od wątpliwości.

Przyjęta procedura badawcza oraz struktura pracy umożliwiły przedstawienie teoretycznych koncepcji dotyczących omawianych zagadnień, które zostały następnie poddane weryfikacji w ramach przeprowadzonych badań empirycznych. Dzięki realizacji założonych analiz udało się skutecznie potwierdzić postawione hipotezy i osiągnąć wyznaczone cele, co pozwoliło na sformułowanie następujących wniosków końcowych:

1. **Zintegrowane podejście do zarządzania bezpieczeństwem jako klucz do efektywności** – Efektywne zarządzanie bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych (ICT) wymaga połączenia aspektów technologicznych, proceduralnych i ludzkich. Wyniki przeprowadzonych badań potwierdzają, że organizacje stosujące kompleksowe podejście do bezpieczeństwa, które uwzględnia różnice w percepcji zagrożeń przez pracowników, uzyskują lepsze rezultaty w redukcji ryzyka. Tego rodzaju strategia umożliwia bardziej precyzyjne dopasowanie narzędzi ochronnych do specyficznych potrzeb organizacji.
2. **Personalizacja strategii ochrony w odpowiedzi na zróżnicowaną percepcję zagrożeń –** Badania empiryczne ujawniły, że różnice w świadomości zagrożeń wśród pracowników są istotnym czynnikiem wpływającym na skuteczność systemów zarządzania bezpieczeństwem. Odpowiednie dostosowanie strategii ochrony, obejmujące szkolenia, procedury reagowania oraz przydział ról w systemie zabezpieczeń, okazuje się kluczowe w optymalnym funkcjonowaniu systemów ochronnych w sektorze ICT.
3. **Edukacja i budowanie świadomości jako fundament zarządzania bezpieczeństwem** – Jednym z fundamentalnych elementów zarządzania

bezpieczeństwem jest edukacja pracowników w zakresie identyfikacji i przeciwdziałania zagrożeniom. Wyniki badań wskazują, że regularne szkolenia, kampanie informacyjne i symulacje zdarzeń kryzysowych znacząco podnoszą zdolność organizacji do efektywnej ochrony. Organizacje inwestujące w rozwój kompetencji pracowników w tym obszarze wykazują większą odporność na incydenty bezpieczeństwa.

4. **Zaawansowane technologie jako element wsparcia zarządzania bezpieczeństwem** – Opracowany model zarządzania bezpieczeństwem podkreśla znaczenie wykorzystania nowoczesnych technologii, takich jak systemy monitorujące, szyfrowanie danych czy zaawansowane narzędzia analityczne. Wyniki badań dowodzą, że wdrożenie takich technologii w połączeniu z adekwatnymi procedurami zwiększa skuteczność ochrony kluczowych zasobów, takich jak dane organizacyjne czy tajemnice przedsiębiorstwa.
5. **Adaptacyjność jako konieczność w dynamicznym środowisku sektora ICT** – Środowisko sektora ICT, charakteryzujące się szybkim tempem zmian, wymaga strategii zarządzania bezpieczeństwem opartych na elastyczności i zdolności do adaptacji. Wyniki symulacji wdrożeniowych pokazują, że systemy, które są regularnie oceniane i doskonalone w oparciu o wyniki monitoringu, osiągają wyższą skuteczność w minimalizowaniu ryzyka.
6. **Przyjęta metodyka badawcza jako model dla przyszłych badań** – Zastosowana w pracy procedura badawcza, obejmująca analizy literaturowe, badania empiryczne (ankiety i wywiady eksperckie) oraz symulacje wdrożeniowe, okazała się skutecznym narzędziem w identyfikacji kluczowych czynników wpływających na zarządzanie bezpieczeństwem w sektorze ICT. Metodyka ta może znaleźć zastosowanie również w badaniach innych sektorów o podwyższonym poziomie ryzyka operacyjnego.
7. **Praktyczne znaczenie opracowanego modelu zarządzania bezpieczeństwem** – Zaprezentowany model zarządzania bezpieczeństwem dla przedsiębiorstw sektora ICT został pozytywnie zweryfikowany jako narzędzie zwiększające skuteczność działań ochronnych. Model ten zapewnia strukturalne ramy wdrożenia kompleksowych strategii zarządzania, uwzględniając specyficzne potrzeby organizacji oraz charakter zagrożeń. Jego implementacja w praktyce wzmacnia ochronę zasobów przedsiębiorstwa i poprawia jego pozycję konkurencyjną na rynku.

Wnioski sformułowane w niniejszej dysertacji jednoznacznie wskazują na pełną realizację założonego celu badawczego. Przyjęte podejście metodologiczne, obejmujące zarówno wieloaspektową analizę teoretyczną, jak i empiryczną weryfikację hipotez, w istotny sposób wzbogaca dyscyplinę nauk o zarządzaniu i jakości. Opracowany model zarządzania bezpieczeństwem w sektorze technologii informacyjno-komunikacyjnych (ICT) dostarcza nie tylko solidnych podstaw teoretycznych, ale również praktycznych narzędzi, które umożliwiają skuteczną ochronę zasobów informacyjnych przedsiębiorstw działających w dynamicznym i wymagającym środowisku technologicznym.

Wyniki badań dowodzą, że integracja technicznych, proceduralnych i ludzkich aspektów zarządzania bezpieczeństwem jest kluczowa dla efektywnego funkcjonowania organizacji w sektorze ICT. Pozytywna weryfikacja hipotez oraz praktyczne zastosowanie opracowanego modelu stanowią istotny wkład do rozwoju wiedzy w tym obszarze, oferując rozwiązania, które można elastycznie dostosować do specyficznych potrzeb organizacyjnych. Co więcej, przedstawione wnioski otwierają nowe perspektywy badawcze, wskazując na możliwość adaptacji wypracowanego podejścia do innych sektorów gospodarki, szczególnie tych, które również charakteryzują się wysoką dynamiką zmian oraz dużą zależnością od innowacji technologicznych.

Opracowany model zarządzania bezpieczeństwem może służyć jako fundament dla dalszych badań w zakresie skuteczności ochrony danych, zwiększania świadomości pracowników w kontekście zagrożeń informacyjnych oraz optymalizacji procedur zarządzania ryzykiem. Tym samym wyniki pracy nie tylko wzbogacają literaturę naukową, ale także stanowią inspirację dla praktyków, wskazując na kierunki rozwoju strategii zarządzania bezpieczeństwem w obliczu globalnych wyzwań związanych z cyfryzacją i szpiegostwem korporacyjnym.

BIBLIOGRAFIA

1. Abd Jalil J., Hassan H., *Protecting trade secret from theft and corporate espionage: some legal and administrative measures*, International Journal of Business and Society, Vol. 21 S1, 2020.
2. Agresti A., *Statistical Methods for the Social Sciences (5th ed.)*. Pearson, Boston 2018.
3. Altintas K. M., *Comparative Analysis of Strategic Relationship between Industrial versus Corporate Espionage within the Framework of Implementation Methods*, Global Security and Intelligence Studies Vol. 6, No. 1 2021.
4. Anugerah A. R., Muttaqin P. S., Trinarningsih W., *Social network analysis in business and management research: A bibliometric analysis of the research trend and performance from 2001 to 2020*, Heliyon 8 (2022), https://doi.org/10.1016/j.heliyon.2022.e09270.
5. Apanowicz J., *Metodologia nauk*, Wydawnictwo TNOiK „Dom Organizatora", Toruń 2003.
6. Ausat A. M. A., Permana B., Harahap M. A. K., *Do Information Technology and Human Resources Create Business Performance: A Review*, Journal of Professional Business Review 2023 8 (8), https://doi.org/10.26668/businessreview/2023.v8i8.2206.
7. Barczyk A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy Bellona, Warszawa 2003.
8. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2015.
9. Bega M., *The New Arms Race Between China and the US: A Comparative Analysis of Ai-Powered Military and Economic Pursuits*, EUROPOLITY, vol. 17, no. 2, 2023, DOI: 10.25019/europolity.2023.17.2.3.
10. Bell D. E., LaPadula L. J., *Secure computer system: Unified exposition and Multics Interpretation*, Mitre Corporation, Bedford 1976.
11. Bellaby R. W., *The Ethics of Economic Espionage*, Ethics & International Affairs, 37 (2023).
12. Benzaghta M. A., Elwalda A., Mousa M. M., Erkan I., Rahman M., *SWOT analysis applications: An integrative literature review*, Journal of Global Business Insights Issue 1 (2021) Vol. 6, https://www.doi.org/10.5038/2640-6489.6.1.1148.
13. *Bezpieczeństwo informacji – wprowadzenie*, Narodowy standard cyberbezpieczeństwa NSC 800-12, Ministerstwo Cyfryzacji.

14. Bharadiya J. P., *A Comparative Study of Business Intelligence and Artificial Intelligence with Big Data Analytics*, American Journal of Artificial Intelligence 2023 7(1), doi: 10.11648/j.ajai.20230701.14.
15. Bitkowska A., *Uwarunkowania realizacji projektów wdrożenia zarządzania procesowego*, Studia i Prace Kolegium Zarządzania i Finansów, Zeszyt Naukowy 186/2022, https://doi.org/10.33119/SIP.2022.186.2.
16. Bitkowska A., Szymborski M., *Cyfryzacja przedsiębiorstw z perspektywy procesowo-projektowej*, W: *Wykorzystanie technik informacyjnych w zarządzaniu* (red.) Leszek Kiełtyka, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2023.
17. Blim M., *Teoria ochrony informacji (część 1)*, „Zabezpieczenia" nr 3/2007.
18. Bobkowski K., *Zarządzanie bezpieczeństwem informacji w ujęciu wybranych aktów normatywnych w zakresie Systemu Zarządzania Bezpieczeństwem Informacji*, Zarządzanie i Finanse Journal of Management and Finance Vol. 16, No. 3/2/2018.
19. Brown T. A., *Confirmatory Factor Analysis for Applied Research (2nd ed.)*, Guilford Press, New York 2015.
20. Brzozowska A., Bubel D., Pabian A., *Implementation of technical and information systems in environmental management*, Procedia - Social and Behavioral Sciences 213 (2015), https://doi.org/10.1016/j.sbspro.2015.11.516.
21. Brzozowska A., Bubel D., Nekrasenko L., *Organisation Management in the Digital Economy: Globalization Challenges*, CRC Press, Boca Raton 2022.
22. Brzozowska A., *Information Management in a Dynamic Business Environment – A Case Study of Fractal Organisations*, Acta Universitatis Lodziensis. Folia Oeconomica 2 (367) 2024, DOI: https://doi.org/10.18778/0208-6018.367.01.
23. Button M., *Editorial: economic and industrial espionage*, Security Journal (2020) 33:1–5, https://doi.org/10.1057/s41284-019-00195-5.
24. Byrne B. M., *Structural Equation Modeling with AMOS: Basic Concepts, Applications*, and Programming (3rd ed.), Routledge, New York 2016.
25. Chan M., *Corporate Espionage and Workplace Trust/Distrust*, Journal of Business Ethics Vol. 42, No. 1 (Jan., 2003).
26. Chodorowska P., Brańko M., Tomaszewska E., *Real-Time Marketing jako narzędzie budowania wizerunku przedsiębiorstwa w mediach społecznościowych*, Akademia Zarządzania, vol. 8 (2) 2024, DOI: 10.24427/az-2024-0022.
27. Cialdini R. B., *Wywieranie wpływu na ludzi. Teoria i praktyka*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2012.
28. Ciborowski L., *Walka informacyjna*, Wydawnictwo Adam Marszałek, Toruń 2001.

29. Ciecińska B., Łunarski J., Perłowski R., D. Stadnicka, *Systemy zarządzania bezpieczeństwem w przedsiębiorstwie*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2006.
30. Ciekanowski Z., Majkowska J., Załoga W., *Wpływ otoczenia na funkcjonowanie organizacji*, Nowoczesne Systemy Zarządzania Zeszyt 13 (2018), nr 4 (kwiecień-czerwiec).
31. Culot G., Nassimbeni G., Podrecca M., Sartor M., *The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda*, The TQM Journal Volume 33 Issue 7 (2021).
32. Cunningham-Dickie M., *Are we ready for the next WannaCry?*, Computer Fraud & SecurityVol. 2023, No. 9, https://doi.org/10.12968/S1361-3723(23)70041-9.
33. Czekaj J., *Podstawy zarządzania informacją*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2012.
34. Czupryński A., *Bezpieczeństwo w ujęciu teoretycznym*, W: *Bezpieczeństwo. Teoria-Badania-Praktyka.* (red.) A. Czupryński, B. Wiśniewski, J. Zboina, Wydawnictwo CNBOP-PIB, Józefów 2015.
35. Ćwiklicki M., *Metodyka przeglądu zakresu literatury*, W: *Współczesne zarządzanie – koncepcje i wyzwania* (red.) A. Sopińska, A. Modliński, Wydawnictwo SGH, Warszawa 2020.
36. Dalko V., Michael B., Wang M., *Spoofing: effective market power building through perception alignment*, Studies in Economics and Finance Vol. 37 No. 3 (2020), https://doi.org/10.1108/SEF-09-2019-0346.
37. Dawidczyk A., *Podstawy badań bezpieczeństwa*, W: *Bezpieczeństwo. Teoria-Badania-Praktyka* (red.) A. Czupryński, B. Wiśniewski, J. Zboina, Wydawnictwo CNBOP-PIB, Józefów 2015.
38. Deb D., Jain A. K., *Look locally infer globally: A generalizable face anti-spoofing approach*, IEEE Transactions on Information Forensics and Security, 16 (2020).
39. Decker M. J., *Enterprise Security Capability: Common Models*, W: *Encyclopedia of Information Assurance* (red.) R. Herold, M. K. Rogers, CRC Press, Londyn 2010.
40. Deming W. E., *Out of the crisis*, Massachusetts Institute of Technology, Cambridge 1986.
41. Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwo WNT, Warszawa 2002.
42. Dmowska A., *Słownik współczesnego języka polskiego*, Warszawa 1996.

43. Dobrowolski G., Filipkowski W., Kisiel-Dorohnicki M., Rakoczy W., *Wsparcie informatyczne dla analizy otwartych źródeł informacji w Internecie w walce z terroryzmem. Zarys problemu*, W: *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu* (red.) L. K. Paprzycki, Z. Rau, Wydawnictwo Wolters Kluwer, Warszawa 2009.
44. Duraj A. N., *Rezerwy a strategie finansowe publicznych spółek akcyjnych*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2008.
45. Ergan M., Mather T., *The Executive Guide to Information Security*, Addison-Wesley, Indianapolis 2005.
46. Fałdowski M., *Współczesny wymiar bezpieczeństwa*, „Zeszyty Naukowe SGSP" 2018, nr 66(2).
47. Farzaneh M., Wilden R., Afshari L., Mehralian G., *Dynamic capabilities and innovation ambidexterity: The roles of intellectual capital and innovation orientation*, Journal of Business Research 148 (2022), https://doi.org/10.1016/j.jbusres.2022.04.030.
48. Fischer B., *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Wydawnictwo Zakamycze, Kraków 2000.
49. Fitzpatrick W. M., DiLullo S. A., Burke D. R., *Trade Secret Piracy and Protection: Corporate Espionage. Corporate Security and the Law*, Advances in Competitiveness Research, Vol. 12, No. 1 2004.
50. Fort R. M., *Economic Espionage*, W: *U. S. Intelligence at the Crossroads: Agendas for Reforms* (red.) R. Godson, E. May, G. Schmitt, Wydawnictwo Brassey's, Waszyngton 1995.
51. Frankfort-Nachmias C., Nachmias D., *Metody badawcze w naukach społecznych*, Wydawnictwo Zysk i S-ka, Poznań 2001, s. 35.
52. Garner B. A., *Black's Law Dictionary*, Thomson Reuters, Toronto 2019.
53. Gembalska-Kwiecień A., Żurakowski Z., *Zarządzanie bezpieczeństwem a problem partycypacji pracowników w przedsiębiorstwie*, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie", nr 159, 2015, DOI: 10.29119/1641-3466.2022.159.
54. Genuer R., Poggi J-M., *Random Forrest with R*, Springer International Publishing, Londyn 2020.
55. Ghaznavi-Zadeh R., *Enterprise Security Architecture - A Top-down Approach*, „ISACA JOURNAL", 2017 nr 4.
56. Gierszewska G., *Wspomaganie zarządzania wiedzą we współczesnych organizacjach*, W: *Gospodarka cyfrowa 2016. Zarządzanie, innowacje, społeczeństwo i technologie*

(red.) A. Gąsiorkiewicz, K. Sitarski, O. Sobolewska, M. Wiśniewski, Wydział Zarządzania Politechniki Warszawskiej, Warszawa 2017.

57. Gryz J., *Zarys podstaw teorii bezpieczeństwa*, Akademia Obrony Narodowej, Warszawa 2010.
58. Hanausek T., *Zarys taktyki kryminalistycznej*, Dom Wydawniczy ABC, Warszawa 1994.
59. Herman P., *Ochrona komunikacji biznesowej przez szpiegostwem*, W: *Ochrona przedsiębiorstwa przed szpiegostwem gospodarczym. Prawne i praktyczne aspekty zapewnienia bezpieczeństwa aktywów przedsiębiorcy* (red.) P. Herman, P. Łabuz, T. Safjański, Wydawnictwo Difin, Warszawa 2021.
60. Herman P., *Ochrona zasobów informatycznych przed szpiegostwem gospodarczym*, W: *Ochrona przedsiębiorstwa przed szpiegostwem gospodarczym. Prawne i praktyczne aspekty zapewnienia bezpieczeństwa aktywów przedsiębiorcy* (red.) P. Herman, P. Łabuz, T. Safjański, Wydawnictwo Difin, Warszawa 2021.
61. Herman P., Safjański T., *Zbieranie informacji biznesowych na poziomie operacyjnym – wywiad gospodarczy*, W: *Wywiad i analityka w biznesie. Prawne i praktyczne aspekty analizy wywiadowczej* (red.) P. Herman, P. Łabuz, T. Safjański, Difin, Warszawa 2023.
62. Horan S., *Corporate and Industrial Espionage and Their Effect on American Competitiveness - A statement before the House Subcommittee on International Economic Policy and Trade*, IO6 Congress. Serial No: 106-180, Waszyngton 2000.
63. Horosiewicz K., *Przedsięwzięcia werbunkowe*, „Przegląd Policyjny" 2012, nr 4 (108).
64. Horosiewicz K., *Wybrane elementy taktyki werbowania i współpracy z osobowymi źródłami informacji*, Wydawnictwo WSPol, Szczytno 2019.
65. Iershova N., Garkusha V., *Functioning of the system of ensuring the economic security of the industrial enterprise: conceptual provisions*, „Economics & Education", 2021 nr 06(02).
66. Ijzermans M., Van den Berge W., *Resilience after Corporate or Industrial Espionage*, The BCI Netherlands & Belgium Conference, Utrecht 2019.
67. Inayat U., Farzan M., Mahmood S., Zia M. F., Hussain S., Pallonetto F., *Insider threat mitigation: Systematic literature review*, Ain Shams Engineering Journal 2024, https://doi.org/10.1016/j.asej.2024.103068.
68. ISO / IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*, ISO, Geneva 2018.

69. ISO / IEC 27031:2011, *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*, ISO, Geneva 2011.
70. ISO / IEC 27032:2012, *Information technology – Security techniques – Guidelines for cybersecurity*, ISO, Geneva 2012.
71. ISO / IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*, ISO, Geneva 2015.
72. ISO / IEC 27034-1:2011, *Information technology – Security techniques – Application security – Part 1: Overview and concepts*, ISO, Geneva 2011.
73. ISO / IEC 27035-1:2016, *Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management*, ISO, Geneva 2016.
74. ISO / IEC 27036-1:2014, *Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts*, ISO, Geneva 2014.
75. ISO / IEC 27037:2012, Information technology – *Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*, ISO, Geneva 2012.
76. ISO / IEC 27038:2014, *Information technology – Security techniques – Specification for digital redaction*, ISO, Geneva 2014.
77. ISO / IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*, ISO, Geneva 2015.
78. ISO / IEC 27040:2015, *Information technology – Security techniques – Storage security*, ISO, Geneva 2015.
79. ISO / IEC 27041:2015, *Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method*, ISO, Geneva 2015.
80. ISO / IEC 27042:2015, *Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*, ISO, Geneva 2015.
81. ISO / IEC 27043:2015, *Information technology – Security techniques – Incident investigation principles and processes*, ISO, Geneva 2015.
82. ISO / IEC 27050-1:2016, *Information technology – Security techniques – Electronic discovery – Part 1: Overview and concepts*, ISO, Geneva 2016.
83. ISO / IEC 29101:2013, *Information technology – Security techniques – Privacy architecture framework*, ISO, Geneva 2013.

84. Jameson D. A., *The rhetoric of industrial espionage: the case of Starwood v. Hilton*, Business Communication Quarterly, 74(3) 2011, doi:10.1177/1080569911413811.
85. Jarczewska-Walendziak K., *Wykorzystanie otwartych źródeł informacji przez służby śledcze*, Toruńskie Studia Bibliologiczne 2017 nr 1 (18), doi: http://dx.doi.org/10.12775/TSB.2017.008.
86. Janus D., *Holizm w controllingowym zarządzaniu organizacjami*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu", 2022, t. 66, nr 2, DOI: 10.15611/pn.2022.2.05.
87. Jones A., *Industrial espionage in a hi-tech world*, Computer Fraud & Security, Volume 2008, Issue 1 2008, doi:10.1016/S1361-3723(08)70010-1.
88. Kawa A., Fuks K., Januszewski P., *Symulacja komputerowa jako metoda badań w naukach o zarządzaniu*, Studia Oeconomica Posnaniensia 2016, Vol. 1, No. 1, doi: 10.18559/SOEP.2016.1.8.
89. Khan A., Malik K. M., Ryan J., Saravanan M., *Battling voice spoofing: a review, comparative analysis, and generalizability evaluation of state-of-the-art voice spoofing counter measures*, Artificial Intelligence Review Vol. 56 (2023), https://doi.org/10.1007/s10462-023-10539-8.
90. Kiedrowicz-Wywiał A., *Pharming i jego penalizacja*, „Prokuratura i Prawo" 2011, nr 6.
91. Kiełtyka L., *Zarządzanie informacją w organizacji – podejście systemowe*, W: *Zarządzanie zasobami niematerialnymi w organizacji. Człowiek, Informacja, Wiedza, Narzędzia IT* (red.) L. Kiełtyka, W. Jędrzejczyk, Wydawnictwo TNOIK, Toruń 2022.
92. Kline R. B., *Principles and Practice of Structural Equation Modeling (4th ed.)*, Guilford Press, New York 2015.
93. Koen C., London B., *To Catch a Thief: Protecting Proprietary Information Including Trade Secrets from Corporate Espionage*, The Health Care Manager, Oct/Dec 2019; 38 (4), doi: 10.1097/HCM.0000000000000283.
94. Konieczny M., *Manipulacja, perswazja i socjotechnika jako formy wywierania wpływu*, Studia Prawnicze. Rozprawy i Materiały 2023, nr 2 (33), DOI: 10.48269/2451-0807-sp-2023-2-006.
95. Konopatsch C., *Fighting industrial and economic espionage through criminal law: lessons to be learned from Austria and Switzerland*, Security Journal Volume 33 (2020), https://doi.org/10.1057/s41284-019-00200-x.

96. Kosiński J., *Cyberprzestępczość*, W: *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne* (red.) W. Jasiński, Szczytno 2013.
97. Koziej S., *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, Bezpieczeństwo Narodowe II-2011 (18), Biuro Bezpieczeństwa Narodowego, Warszawa 2011.
98. Kozłowski K., *Ewolucja szpiegostwa biznesowego: Od konkurencji przemysłowej do cyberprzestrzen*i, Management and Quality – Zarządzanie i Jakość, Vol. 6 No 1 (2024).
99. Kozłowski K., *System Bezpieczeństwa Wewnętrznego RP. Wybrane aspekty zarządzania bezpieczeństwem w XXI w.*, Management and Quality – Zarządzanie i Jakość, Vol. 4 No 3 (2022).
100. Kozłowski K., *Technological Advancements and Their Impact on Organisational Information Security*, Applied Business and Economics Journal, Vol. 2 No 1 (2024), doi: 10.61089/abej.2024.2.87.
101. Księżopolski K. M., *Bezpieczeństwo ekonomiczne*, Dom Wydawniczy ELIPSA, Warszawa 2011.
102. Kulej-Dudek E., Pypłacz P., *Rola zasobów niematerialnych w kształtowaniu wartości przedsiębiorstw*, W: *Zarządzanie zasobami niematerialnymi w organizacji. Człowiek, Informacja, Wiedza, Narzędzia IT* (red.) L. Kiełtyka, W. Jędrzejczyk, Wydawnictwo TNOIK, Toruń 2022.
103. Kuta M., *Polityka bezpieczeństwa informacji w przedsiębiorstwie – aspekty praktyczne*, W: *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa* (red.) R. Borowiecki, M. Kwieciński, Wydawnictwo Zakamycze, Kraków 2003.
104. Kwak D. H., Kizzier D. M., Jung E., *Spyware Knowledge in Anti-Spyware Program Adoption: Effects on Risk, Trust, and Intention to Use*, 2011 44th Hawaii International Conference on System Sciences, Kauai, HI, USA, 2011, doi: 10.1109/HICSS.2011.382.
105. Latosińska A., *Wywiad gospodarczy a bezpieczeństwo ekonomiczne państwa*, W: *Wywiad i kontrwywiad gospodarczy Materiały z konferencji naukowych* (red.) H. Szafran, J. W. Wójcik, Wydawnictwo Wszechnicy Polskiej, Warszawa 2019.
106. Li Z., Oprea A., *Operational Security Log Analytics for Enterprise Breach Detection*, 2016 IEEE Cybersecurity Development (SecDev), Boston, MA, USA, 2016, doi: 10.1109/SecDev.2016.015.
107. Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa 2008.

108. Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydawnictwo PWN, Warszawa 2017.
109. Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej*, Wydawnictwo Difin, Warszawa 2011.
110. Lis T., Ptak A., *ICT a Efektywność Zarządzania Informacją w Przedsiębiorstwie*, W: *Technologie informacyjno-komunikacyjne w zarządzaniu, logistyce i turystyce. Wybrane zagadnienia* (red.) L. Kiełtyka, K. Smoląg, Wydawnictwo TNOiK "Dom Organizatora" w Toruniu, Toruń 2022.
111. Lisiński M., Szarucki M., *Metody badawcze w naukach o zarządzaniu i jakości*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2020.
112. Lula P., Oczkowska R., Wiśniewska S., Wójcik K., *An attempt to estimate the competency gap in the IT sector*, „International Entrepreneurship Review", 2019, vol. 5, nr 3, DOI: 10.15678/IER.2019.0503.07.
113. Łuczak J. (red.), *Zarządzanie bezpieczeństwem informacji*, Wydawnictwo „Oficyna Współczesna", Poznań 2004.
114. Łuczak J., Tyburski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Wydawnictwo Uniwersytetu Ekonomicznego, Poznań 2010.
115. Łusiakowski K., *Model trzech linii w systemie zarządzania ryzykiem przedsiębiorstwa*, Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie, Nr 55 (2024), DOI: 10.17512/znpcz.2024.3.09.
116. Majer P., *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*, „Przegląd bezpieczeństwa wewnętrznego" 2012, nr 7(4).
117. Malinowski K., *Inwigilacja elektroniczna i bezpośrednia. Część 2*, Wydawnictwo Spyshop Expert Sp. z o. o., Poznań 2017.
118. Maslow A. H., *Motivation and Personality*, Longman, Nowy Jork 1987.
119. Maśloch P., *Globalizacja a zarządzanie bezpieczeństwem współczesnych organizacji*, Wydawnictwo ASzWoj, Warszawa 2018.
120. Matacz M., Vodičková W., *Zjawisko phisingu w Polsce*, De Securitate Et Defensione. O Bezpieczeństwie I Obronności, 9 (1) 2023, https://doi.org/10.34739/dsd.2023.01.09.
121. Maynard S. B., Ahmad A., *Information Security Management in High Quality IS Journals: A Review and Research Agenda*, Cryptography and Security 2022 (arXiv:2208.13087), https://doi.org/10.48550/arXiv.2208.13087.
122. Mąkosa G., *Zarządzanie ryzykiem jako determinanta cyberbezpieczeństwa*, Nowoczesne Systemy Zarządzania Instytut Organizacji i Zarządzania Zeszyt 14 (2019) nr 3 (lipiec-wrzesień).

123.Menard S., *Logistic Regression. From Introductory to Advanced Concepts and Applications*, SAGE Publications, Nowy York 2010.

124.*Metody i formy pracy operacyjnej stosowane przez oficerów Głównego Zarządu Rozpoznania Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, WSI, Warszawa 2004.

125.Mitnick K. D., Simon W. L., *Sztuka podstępu*, Wydawnictwo Helion, Gliwice 2016.

126.Mizrak F., *Effective Change Management Strategies: Exploring Dynamic Models for Organizational Transformation*, W: *Perspectives on Artificial Intelligence in Times of Turbulence: Theoretical Background to Applications* (red.) N. Geada, G. L. Jamil, IGI Global, Nowy Jork 2023, DOI: 10.4018/978-1-6684-9814-9.ch009.

127.Mozgawa M., *Phishing w ujęciu prawnokarnym*, W: *Współczesne oblicza prawa karnego, prawa wykroczeń, kryminologii i polityki kryminalnej. Księga jubileuszowa dedykowana Profesor Violetcie Konarskiej-Wrzosek* (red.) J. C. Bojarski, N. Daśko, J. Lachowski, T. Oczkowski, A. Ziółkowska, Wydawnictwo: Wolters Kluwer Polska, Warszawa 2023.

128.Mroziewicz K., *Czas pluskiew*, Wydawnictwo: Wołoszański, Warszawa 2007.

129.Mughal A. A., *Building and Securing the Modern Security Operations Center (SOC)*, International Journal of Business Intelligence and Big Data Analytics, 5(1) 2022.

130.Mungoli N., Scalable, *Distributed AI Frameworks: Leveraging Cloud Computing for Enhanced Deep Learning Performance and Efficiency*, Computer Science 2023, https://doi.org/10.48550/arXiv.2304.13738.

131.Musiał F., *Teoria pracy operacyjnej Służby Bezpieczeństwa w świetle wydawnictw resortowych Ministerstwa Spraw Wewnętrznych PRL (1970-1989)*, Wydanie III, Kraków-Warszawa 2018.

132.Naser M., Bazar H., Abdel-Jaber H., *Mobile Spyware Identification and Categorization: A Systematic Review*, Informatica 47 (2023), https://doi.org/10.31449/inf.v47i8.4881.

133.Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Difin, Warszawa 2011.

134.Nycz M., Michno B., Mlicki R., *Badanie efektywności ataków socjotechnicznych w jednostkach samorządu terytorialnego*, W: *Innowacyjna Gmina. Informatyka w jednostkach samorządu terytorialnego* (red.) M. Hajder. Wydawnictwo Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie, Rzeszów 2014.

135.OECD, *Embracing the Technology Frontier*, OECD Digital Economy Outlook 2024 (Volume 1), DOI: https://doi.org/10.1787/a1689dc5-en.

136.Onwubiko C., Lenaghan A. P., *Managing Security Threats and Vulnerabilities for Small to Medium Enterprises*, 2007 IEEE Intelligence and Security Informatics, New Brunswick, NJ, USA, 2007, doi: 10.1109/ISI.2007.379479.

137.Pachghare V. K., *Cryptography and information security. Third edition*, Wydawnictwo PHI Learning Pvt. Ltd., Delhi 2019.

138.Piasecki B., *Kontrwywiad – atak i obrona*, Wydawnictwo LTW, Łomianki 2021.

139.Piotrowska K., *Etapy procesu innowacyjnego jako obszary ryzyka w audycie wewnętrznym*, Finanse, Rynki Finansowe, Ubezpieczenia nr 6/2016 (84), cz. 1, DOI: 10.18276/frfu.2016.84/1-30.

140.Polaczek T., *Audyt bezpieczeństwa informacji w praktyce*, Wydawnictwo Helion, Gliwice 2006.

141.Połowin A., *Cyberzagrożenia w internecie –analiza przypadków*, Cybersecurity and Law Issue 2/2024 vol. 12, DOI: https://doi.org/10.35467/cal/188562.

142.Porteous S. D., *Economic/Commercial Interests and the World's Intelligence Services: A Canadian Perspective*, International Journal of Intelligence and Counterintelligence Vol. 8, No. 3, 1995.

143.Poselski projekt ustawy *o czynnościach operacyjno-rozpoznawczych* z dn. 7 lutego 2008 r. (Druk nr 353).

144.Potejko P., *Bezpieczeństwo informacyjne*, W: *Bezpieczeństwo państwa: wybrane problemy* (red.) K. A. Wojtaszczyk, A. Materska-Sosnowska, Oficyna Wydawnicza Aspra, Warszawa 2009.

145.Rabik W., *Information security as a global challenge for the 21st century*, Studia nad Bezpieczeństwem Nr 7 (2022), DOI: 10.34858/SNB.7.2022.003.

146.Raczkowski K., *Współczesny model tetrarchii zarządzania a bezpieczeństwo ekonomiczne obrotu gospodarczego*, W: *Bezpieczeństwo ekonomiczne obrotu gospodarczego. Ekonomia. Prawo. Zarządzanie* (red.) K. Raczkowski, Wolters Kluwer, Warszawa 2014.

147.Radoš K., Brkic M., Begušic D., *Recent Advances on Jamming and Spoofing Detection in GNSS*, Sensors 2024, 24, 4210, https://doi.org/10.3390/s24134210.

148.*Raport o stanie bezpieczeństwa w cyberprzestrzeni*, Zespół CSIRT GOV, Warszawa 2023.

149.Rothke B., *Corporate Espionage and What Can Be Done to Prevent It*, Information Systems Security. (2001) 10:5, doi: 10.1201/1086/43315.10.5.20011101/31716.3.

150.Rokach L., *Maimon O., Data Mining with Decision Trees. Theory and Applications (2nd ed)*, World Scientific, Singapur 2014.

151. Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. *w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania* (Dz.U. 2009 nr 226 poz. 1828).
152. Rozporządzenie Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*.
153. Rychły-Lipińska A., Kamiński W., *Bezpieczeństwo informacji w erze pracy zdalnej a rola modelu ISO 27001:2017*, Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie Nr 53 (2024), DOI: 10.17512/znpcz.2024.1.09.
154. Rybicki J., *Holizm w controllingowym zarządzaniu organizacjami*, „Przegląd Organizacji", Nr 1(984), 2022, DOI: 10.33141/po.2022.01.02.
155. Shaikh F. A., Siponen M., *Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity*, Computers & Security Volume 124, January 2023, https://doi.org/10.1016/j.cose.2022.102974.
156. Sienkiewicz P., *Społeczeństwo informacyjne jako społeczeństwo ryzyka*, W: *Społeczeństwo informacyjne. Aspekty funkcjonalne i dysfunkcjonalne* (red.) W. Haber, M. Niezgoda, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006.
157. Sienkiewicz, P., *Badania naukowe bezpieczeństwa systemów*, W: *Wyzwania bezpieczeństwa cywilnego XXI wieku – Inżyniera działań w obszarach nauki, dydaktyki i praktyki* (red.) B. Kosowski, A. Włodarski, Fundacja Edukacja i Technika Ratownictwa, Warszawa 2007.
158. *Słownik terminów z zakresu bezpieczeństwa*, (red.) J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, Wydawnictwo Adam Marszałek, Toruń 2020.
159. Søile K. S., *Economic and industrial espionage at the start of the 21 st century – Status quaestionis*, Journal of Intelligence Studies in Business Vol. 6, No. 3 (2016).
160. Sromczyński B., Waszkiewicz P., *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo: 2014 nr 5.
161. Stachowiak Z., Kurek S., Kurek S., *Bezpieczeństwo ekonomiczne Rzeczypospolitej Polskiej*, Akademia Obrony Narodowej, Warszawa 2004.

162. Stanik J., Hoffman R., Napiórkowski J., *Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji*, Ekonomiczne Problemy Usług nr 123 (2016), DOI:10.18276/epu.2016.123-30.
163. Stanik J., Kiedrowicz M., *Model systemu zarządzania bezpieczeństwem organizacji jako podstawa kształtowania polityki bezpieczeństwa informacyjnego*, Ekonomiczne Problemy Usług nr 2/2018 (131), t. 1, DOI: 10.18276/EPU.2018.131/1.
164. Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Wyd. ISP, Warszawa 1996.
165. Sułkowski Ł., R. Lenart-Gasiniec R., *Epistemologia, metodologia i metody badań w naukach o zarządzaniu i jakości*, Społeczna Akademia Nauk, Łódź 2021.
166. Sutherland I., *Industrial espionage from residual data: risks and countermeasures*, School of Computer and Information Science, Perth 2008, doi:10.4225/75/57b2771540cc2.
167. Swamy S. N., Jadhav D., Kulkarni N., *Security threats in the application layer in IOT applications*, 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, doi: 10.1109/I-SMAC.2017.8058395.
168. Szczepaniuk E., *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa*, rozprawa doktorska, AON, Warszawa 2015.
169. Świeboda H., *Zagrożenia bezpieczeństwa współczesnych organizacji*, Ekonomiczne Problemy Usług 2012 nr 88.
170. Tarka P., *Własności 5- i 7-stopniowej skali Likerta w kontekście normalizacji zmiennych metodą Kaufmana i Rousseeuwa*, W: *Taksonomia 25. Klasyfikacja i analiza danych – teoria i zastosowania* (red.) K. Jajuga, M. Walesiak, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu nr 385 (2015).
171. Tomczak A., Dostatni E., Górski F., *Narzędzie informatyczne wspomagające zarządzanie danymi klientów*, Zarządzanie Przedsiębiorstwem 2023 Vol. 26 No. 1, DOI: 10.25961/ent.manag.26.02.04.
172. Tuz M., *Wpływ cyberzagrożeń na funkcjonowanie organizacji*, Przegląd Policyjny 2023/151(3).
173. Ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych* (Dz. U. 2018 poz. 1000, t. j.).
174. Ustawa z dnia 16 lipca 2004 r. – *Prawo telekomunikacyjne* (Dz. U. 2022, poz. 1648, t. j.).
175. Ustawa z dnia 18 lipca 2002 r. *o świadczeniu usług drogą elektroniczną* (Dz.U.2020.0.344, t.j.).

176. Ustawa z dnia 24 września 2010 r. *o ewidencji ludności* (Dz. U. 2010 Nr 217 poz. 1427, t. j.).
177. Ustawa z dnia 28 lipca 2023 r. *o zwalczaniu nadużyć w komunikacji elektronicznej* (Dz.U. 2023 poz. 1703)
178. Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz.U. 1997 Nr 133 poz. 883, t. j., akt utracił moc).
179. Vashisth A., Kumar A., *Corporate espionage: The insider threat*, Business Information Review, 30(2) 2013, https://doi.org/10.1177/0266382113491816.
180. Wagner R. E., *Bailouts and the potential for distortion of federal criminal law: Industrial espionage and beyond*, Tulane Law Review, 86(5) 2012.
181. Werner J., Szczepaniuk E., *Bezpieczeństwo informacyjne organizacji*, Zeszyty Naukowe AON nr 4 (105) 2016.
182. Wimmer B., *Business espionage. Risk, Threats and Countermeasures*, Elsevier, Oxford 2015.
183. Wiśniewski P., *Systemy zarządzania bezpieczeństwem informacji w przedsiębiorstwie*, Acta Universitatis Nicolai Copernici. Zarządzanie, 45(2), https://doi.org/10.12775/AUNC_ZARZ.2018.026.
184. Wojnar J., *Zróżnicowanie wykorzystania technologii informacyjno-komunikacyjnych w krajach Unii Europejskiej*, Wiadomości Statystyczne. The Polish Statistician, 2020, vol. 65(8), DOI: 10.5604/01.3001.0014.3526.
185. Woody A., *Enterprise security: A data-centric approach to securing the enterprise*, Packt Publishing, Birmingham 2013.
186. Worona J., *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Rozprawa doktorska, Uniwersytet w Białymstoku, Białystok 2017.
187. Woźniak J., *Kryterium bezpieczeństwa organizacji*, W: *Projektowanie i doskonalenie organizacji* (red.) J. Woźniak, Wojskowa Akademia Techniczna, Warszawa 2015.
188. Woźniak J., *Percepcja i kształtowanie bezpieczeństwa organizacji w warunkach gospodarki cyfrowej*, W: *Bezpieczeństwo organizacji w warunkach gospodarki cyfrowej* (red.) W. Gonciarski, J. Woźniak, Difin, Warszawa 2021.
189. Woźniak J., *Zarządzanie ryzykiem w sektorach kreatywnych*, Wydawnictwo CeDeWu, Warszawa 2019.
190. Wróbel P., *Implementing full-time remote work in the IT sector: Consequences and solutions*, „Scientific Papers of Silesian University of Technology. Organization and Management Series", 2023, nr 178, DOI: 10.29119/1641-3466.2023.178.43.

191. Xu H., Zhou Y., Gao C., Kang Y., Lyu M. R., *SpyAware: Investigating the privacy leakage signatures in app execution traces*, 2015 IEEE 26th International Symposium on Software Reliability Engineering (ISSRE), Gaithersbury, MD, USA, 2015, doi: 10.1109/ISSRE.2015.7381828.
192. Zaskórski P., Woźniak J., Szwarc K., Tomaszewski Ł, *Zarządzanie projektami w ujęciu systemowym*, Wojskowa Akademia Techniczna, Warszawa 2015.
193. Zawiła-Niedźwiedzki J., *Zarządzanie ryzykiem operacyjnym w zapewnieniu ciągłości działania organizacji*, Wydawnictwo edu-Libri, Kraków-Warszawa 2013.
194. Zhu E., Ju Y., Chen Z., Liu F., Fang X., *An Artificial Neural Network phishing detection model based on Decision Tree and Optimal Features*, Applied Soft Computing Journal 95 (2020).
195. Zuboff S., *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, Public Affairs, Nowy Jork 2019.
196. Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, Roczniki Kolegium Analiz Ekonomicznych nr 29/2013.
197. Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2006.
198. Żebrowski A., Mielus M., *Zagrożenia dla bezpieczeństwa informacji i wiedzy w organizacji*, Bezpieczeństwo. Teoria i Praktyka 2009 nr 3-4.
199. Żukrowska K., *Ekonomia jako sfera bezpieczeństwa państwa*, W: *Interdyscyplinarność nauk o bezpieczeństwie* (red.) K. Raczkowski, K. Żukrowska, M. Żuber, Difin, Warszawa 2013.
200. Żywiołek J., *Zarządzanie zasobami informacji i wiedzy jako determinanta bezpieczeństwa przedsiębiorstwa*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2020.

NETOGRAFIA

1. Bochyńska N., *To koniec smishingu i spoofingu? Zobacz, co się zmieni*, Cyberdefence24.pl, https://cyberdefence24.pl/polityka-i-prawo/wchodzi-w-zycie-wazna-ustawa-o-smishingu-i-spoofingu-zobacz-co-sie-zmieni [dostęp 15.04.2024 r.]
2. *Co to jest bezpieczeństwo informacji (InfoSec)?*, Microsoft Corporation, https://www.microsoft.com/pl-pl/security/business/security-101/what-is-information-security-infosec [dostęp 15.02.2024 r.].
3. *COBIT An ISACA Framework*, ISACA, https://www.isaca.org/resources/cobit [dostęp 22.02.2024 r.].
4. *Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report*, Verizon, https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report [dostęp 04.04.2024 r.].
5. *Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?*, Ministerstwo Cyfryzacji, https://www.gov.pl/web/cyfryzacja/czym-jest-spoofing--jak-go-rozpoznac-i-nie-dac-sie-nabrac [dostęp 15.04.2024 r.].
6. *Director of Central Intelligence Directive 2/12*, Community Open Source Program, https://irp.fas.org/offdocs/dcid212.htm [dostęp 28.02.2024 r.]
7. Dobrołowicz M., Żak K., *Wyciek danych medycznych. Spółka ALAB wydała komunikat*, RMF FM, 2023, https://www.rmf24.pl/fakty/polska/news-wyciek-danych-medycznych-spolka-alab-wydala-komunikat,nId,7175272#crp_state=1 [dostęp 15.01.2024 r.].
8. *Economic Espionage Act of 1996*, PUBLIC LAW 104–294—OCT. 11, 1996, https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf [dostęp 24.02.2024 r.].
9. European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2024*, wrzesień 2024, https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf [dostęp 01.10.2024 r.].
10. ESET, DAGMA, *Cyberportret polskiego biznesu*, 2024, https://www.gov.pl/web/baza-wiedzy/cyberportret-polskiego-biznesu---raport-przygotowany-przez-eset-i-dagma-bezpieczenstwo-it? [dostęp 08.10.2024 r.].
11. Farage E., *UN releases report on Ukraine telecoms damage by Russia*, Reusters 2023, https://www.reuters.com/world/europe/un-releases-report-ukraine-telecoms-damage-by-russia-2023-01-06/ [dostęp 15.01.2024 r.].

12. Fowler K., Urbanowicz K., Burns W., *Cybersecurity threats and incidents differ by region*, Deloitte Center for Integrated Research, https://www2.deloitte.com/us/en/insights/topics/cyber-risk/global-cybersecurity-threat-trends.html [dostęp 15.01.2024 r.].
13. Gazda K., *Które informacje stanowią dane osobowe w świetle RODO?*, Poradnik Przedsiębiorcy, https://poradnikprzedsiebiorcy.pl/-ktore-informacje-stanowia-dane-osobowe-w-swietle-rodo [dostęp 20.02.2024 r.].
14. Ghaemi S., *Powering the Distant Future: 5G and Machine Learning at the Edge*, Unite.ai, https://www.unite.ai/powering-the-distant-future-5g-and-machine-learning-at-the-edge/ [dostęp 13.11.2024 r.].
15. Gnych G., *Znaczenie zarządzania bezpieczeństwem informacji*, EIIT, https://eitt.pl/baza-wiedzy/znaczenie-zarzadzania-bezpieczenstwem-informacji/ [dostęp 15.04.2024 r.].
16. Guembe B., Azeta A., Misra S., Chukwudi Osamor V., Fernandez-Sanz L., Pospelova V., *The Emerging Threat of Ai-driven Cyber Attacks: A Review*, Applied Artificial Intelligence, 36:1 (2022), https://www.tandfonline.com/doi/epdf/10.1080/08839514.2022.2037254?needAccess=true [dostęp 15.04.2024 r.].
17. *Harmonized Threat and Risk Assessment (TRA) Methodology*, Communications Security Establishment, Ottawa 2007, https://www.cyber.gc.ca/sites/default/files/cyber/publications/tra-emr-1-e.pdf [dostęp 22.02.2024 r.].
18. Huaman N., Skarczinski B., Stransky C., Wermke D., Acar Y., Dreißigacker A., Fahl S., *A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises*, 30th USENIX Security Symposium 2021, https://www.usenix.org/system/files/sec21-huaman.pdf [dostęp 22.02.2024 r.].
19. ISO / IEC 27001:2022, *Information security, cybersecurity and privacy protection. Information security management systems Requirements*, ISO, https://www.iso.org/standard/27001 [dostęp 21.02.2024 r.].
20. Kaloudi N., Li J., *The AI-Based Cyber Threat Landscape: A Survey*, https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2642553/%28withoutACM%29AIsurvey+copy.pdf?sequence=1 [dostęp 15.04.2024 r.].

21. Kasprzak A., *System zarządzania bezpieczeństwem informacji*, LexDigital, https://lexdigital.pl/system-zarzadzania-bezpieczenstwem-informacji [dostęp 10.09.2024 r.].
22. Keary T., *How mass layoffs can create new risks for corporate security*, Venture Beat 2023, https://venturebeat.com/security/how-mass-layoffs-can-create-new-risks-for-corporate-security/ [dostęp 15.01.2024 r.].
23. Komisja Nadzoru Finansowego, *Cyberoszustwa inwestycyjne. Termin – socjotechnika*, https://www.knf.gov.pl/dla_konsumenta/kampanie_informacyjne/cyberoszustwa_inwestycyjne/slownik [dostęp 01.03.2024 r.].
24. Kwieciński M., *Zarządzanie bezpieczeństwem działalności przedsiębiorstwa – zarys problematyki*, PWSZ Krosno, http://archiwum.pwsz.krosno.pl/gfx/pwszkrosno/pl/defaultopisy/1155/4/1/9_miroslaw_kwiecinski_zarzadzanie_bezpieczenstwem_dzialalnosci_przedsiebiorstwa__zarys_problematyki.pdf [dostęp 16.12.2023 r.].
25. Loba N., *O "Pegazie", czyli fakty zamiast mitu*, Infosecurity24.pl, https://infosecurity24.pl/sluzby-specjalne/o-pegazie-czyli-fakty-zamiast-mitu-opinia [dostęp 15.04.2024 r.].
26. Maj M., *Koniec ze scamami przez telefon? Rusza wykaz DNO a w życie wchodzi ustawa antyspoofingowa*, Niebezpieczenik.pl, https://niebezpiecznik.pl/post/rusza-dno-czyli-ustawa-anty-spoofingowa/ [dostęp 15.04.2024 r.].
27. Moes T., *Spyware Examples (2024): The 5 Worst Attacks of All Time*, SoftwareLab.org, https://softwarelab.org/blog/spyware-examples/ [dostęp 15.04.2024 r.].
28. Mrowiec D., *Polityka bezpieczeństwa – Czym jest i co decyduje o jej skuteczności?*, Bezpieczeństwo biznesu, https://bezpieczenstwobiznesu.com.pl/index.php/2018/09/09/polityka-bezpieczenstwa-cz-1-czym-jest-i-co-decyduje-o-jej-skutecznosci/ [dostęp: 20.02.2024 r.].
29. Mrożek M., *Zarządzanie bezpieczeństwem organizacji o strukturze heterarchicznej*, https://sg-cdn.uek.krakow.pl/file/root/stanowisko-ds.-obronnych/sdo-zarzadzanie-bezpieczenstwem-organizacji-o-strukturze-heterarchicznej-artykul.pdf [dostęp: 15.12.2023 r.].
30. National Counterintelligence and Security Center (NCSC), *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, Waszyngton 2000, https://fas.org/irp/ops/ci/docs/fecie_fy00.pdf [dostęp 26.02.2024 r.].

31. Pierce D., *From Eliza to ChatGPT: why people spent 60 years building chatbots*, TheVerge.com, https://www.theverge.com/24054603/chatbot-chatgpt-eliza-history-ai-assistants-video [dostęp 15.04.2024 r.].
32. Płecka M., *Bezpieczeństwo ekonomiczne małych i średnich przedsiębiorstw*, https://revue.vsdanubius.sk/sites/default/files/Plecka%20-%20BEZPIECZE%C5%83STWO%20EKONOMICZNE%20MA%C5%81YCH%20I%20%C5%9AREDNIC%20PRZEDSI%C4%98BIORSTW.pdf [dostęp: 15.12.2023 r.].
33. *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego Internetu*, NASK-PIB/CERT Polska, https://cert.pl/uploads/docs/Raport_CP_2022.pdf [dostęp 15.04.2024 r.].
34. *Seven Tips for Implementing COBIT*, ISACA, https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/infographics/seven-tips-cobit-infographic_1223.pdf [dostęp 22.02.2024 r.].
35. Stoecklin M. P., Jang J., Kirat D., *DeepLocker: How AI Can Power a Stealthy New Breed of Malware*, SecurityIntelligence, https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/ [dostęp 15.04.2024 r.].
36. Sprycha I., Kurek M., Wysocka-Golec J., *Nowy wymiar compliance*, KPMG, https://kpmg.com/pl/pl/home/insights/2024/03/nowy-wymiar-compliance.html? [dostęp 03.10.2024 r.].
37. Surdyk K., Nogacki R., *Szpiegostwo przemysłowe w Polsce i na świecie*, PWG Skarbiec, https://www.wywiad-gospodarczy.pl/szpiegostwo-przemyslowe-polska-swiat.html [dostęp 26.02.2024 r.].
38. Tomczyk J., *Technologiczni giganci inwestują w Edge Computing*, MITSloan, https://mitsmr.pl/b/technologiczni-giganci-inwestuja-w-edge-computing/PelOIcy3P [dostęp 13.11.2024 r.].
39. Uniwersalny słownik języka polskiego, *Bezpieczeństwo – hasło*, http://sjp.pwn.pl/sjp/bezpieczenstwo;2443939.html [dostęp: 19.07.2022].
40. *What is Phishing?*, CISCO, https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html [dostęp 15.04.2024 r.].
41. *What Is Spoofing?*, CISCO, https://www.cisco.com/c/en/us/products/security/email-security/what-is-spoofing.html?dtid=osscdc000283 [dostęp 15.04.2024 r.].
42. Woźniak K., Tatka M., *Bezpieczeństwo informacji – hasło*, Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Bezpiecze%C5%84stwo_informacji [dostęp 15.12.2023 r.].

43. Wójcik E., *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej*, https://wspia.eu/media/00jnsacq/44-w%C3%B3jcik.pdf [dostęp 28.02.2024 r.].
44. Zacharska N., *Jak budować zaufanie klientów poprzez transparentność w zakresie ochrony danych osobowych?*, iSecure, https://www.isecure.pl/blog/jak-budowac-zaufanie-klientow-poprzez-transparentnosc-w-zakresie-ochrony-danych-osobowych/? [dostęp 18.11.2024 r.].
45. *Zarządzanie Bezpieczeństwem Informacji*, Polski Komitet Normalizacyjny, https://www.pkn.pl/informacje/2018/01/zarzadzanie-bezpieczenstwem-informacji [dostęp 15.02.2024 r.].

SPIS RYSUNKÓW, TABEL, WYKRESÓW

A. RYSUNKI

B. TABELE

C. WYKRESY

ZAŁĄCZNIKI

Załącznik nr 1

Jakie czynniki wpływają na bezpieczeństwo przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych?

Ekspert 1.
Jednolitość i wewnętrzna funkcjonalność całej infrastruktury bezpieczeństwa, która jest zaprojektowana przez architektów. Ponadto, odpowiedni dobór środków przeciwdziałających zidentyfikowanym zagrożeniom. Skrupulatna i pełna analiza zagrożeń z jakimi przedsiębiorstwo może się stykać powinna być ukierunkowana na zmieniające się otoczenie i technologie. Dodatkowo, istotną rolę odgrywa również odpowiednia polityka kadrowa, ponieważ w większości przypadków za zagrożeniem dla bezpieczeństwa przedsiębiorstwa stoi nieświadomy pracownik. Kluczową rolę odgrywa zatem security awareness oraz monitorowanie lojalności pracowników. Podsumowując, kwestie osobowe, techniczne, zabezpieczeń peryferyjnych oraz bieżąco aktualizowanych planów ochrony obiektów przedsiębiorstwa.

Ekspert 2.
W kontekście przedsiębiorstw sektora technologii informacyjno-komunikacyjnych można wyróżnić dwie główne grupy czynników wpływających na zapewnienie bezpieczeństwa/cyberbezpieczeństwa: wewnętrzne i zewnętrzne. Czynniki zewnętrzne obejmują przede wszystkim akty prawne, które regulują funkcjonowanie tych przedsiębiorstw w Polsce. Ponadto, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych podlegają wpływowi czynników zewnętrznych związanych z łańcuchem dostaw, współpracą z partnerami biznesowymi oraz firmami dostarczającymi usługi lub technologie. Warto zauważyć, że działania podejmowane przez klientów końcowych również mają istotny wpływ na bezpieczeństwo przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych. W związku z tym, istotne jest, aby przedsiębiorstwa te były w stanie skutecznie chronić swoje aktywa oraz zapewnić poufność, integralność i dostępność informacji tylko dla autoryzowanych klientów. W przypadku czynników wewnętrznych, przedsiębiorcy sektora technologii informacyjno-komunikacyjnych są zobowiązani do przestrzegania różnorodnych regulacji prawnych oraz przepisów, które nakładają na nich określone obowiązki. Wdrożenie odpowiednich procesów technicznych, technologii i usług zgodnych z przepisami oraz przyznanymi koncesjami jest kluczowe. Przykładowo, przestrzeganie prawa telekomunikacyjnego w Polsce lub rozporządzenia RODO jest konieczne. Kluczowe czynniki dotyczące wewnętrznego bezpieczeństwa przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych obejmują: dostawy energii (brak zasilania może negatywnie wpływać na funkcjonowanie przedsiębiorstwa), właściwe zabezpieczenie i rozlokowanie kolokacji oraz organizacja i nadzór nad dostępem fizycznym i logicznym do zasobów przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych (w tym zapewnienie ochrony dostępu do danych

klientów). Przykładowo, jeśli klienci mają możliwość dostosowania ustawień swoich usług, konieczna jest odpowiednia autoryzacja i autentykacja każdego klienta, aby zapewnić, że zmiany są dokonywane przez właściwego klienta, a nie przez kogoś innego. Kontrola i monitorowanie działań pracowników przedsiębiorstwa na danych powierzonych przez klientów są również istotne i kluczowe w kontekście świadczonych klientom usług.

Ekspert 3.

Bezpieczeństwo przedsiębiorstw sektora technologii informacyjno-komunikacyjnych jest kształtowane przez szereg czynników zewnętrznych i wewnętrznych, które w znacznym stopniu wpływają na sposób, w jaki organizacje te zarządzają ryzykiem i utrzymują ciągłość działania. Wśród zagrożeń zewnętrznych na szczególną uwagę zasługują coraz częstsze zaawansowane ataki cybernetyczne, takie jak DDoS, phishing, ransomware czy APT, które stanowią poważne wyzwanie dla bezpieczeństwa informacji. Organizacje muszą również dostosować się do różnych regulacji prawnych, takich jak GDPR, co wymusza na nich stosowanie odpowiednich strategii bezpieczeństwa i zarządzania ryzykiem. Dodatkowo, współpraca z partnerami i dostawcami również wymaga odpowiedniego nadzoru, aby unikać wprowadzania dodatkowego ryzyka przez strony trzecie. Wewnętrznie, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych stają przed wyzwaniem właściwego zarządzania tożsamością i dostępem, co jest kluczowe dla zapobiegania nadużyciom i nieautoryzowanemu dostępowi do krytycznych systemów. Przestarzała infrastruktura i brak inwestycji w nowoczesne technologie zabezpieczające mogą zwiększać podatność na ataki. Ponadto, niespójne polityki bezpieczeństwa i procedury reagowania na incydenty, a także niewłaściwe zarządzanie ryzykiem, mogą osłabiać obronność organizacji. Istotną rolę odgrywa także świadomość i szkolenie pracowników; niedostatecznie przeszkoleni pracownicy mogą nieumyślnie stać się słabym ogniwem w łańcuchu ochrony. Czynniki technologiczne i operacyjne, takie jak integracja systemów i rozwój technologii, takich jak IoT czy 5G, wprowadzają nowe wyzwania związane z zarządzaniem bezpieczeństwem w coraz bardziej złożonym środowisku IT. Na płaszczyźnie społecznej i ekonomicznej, rosnące oczekiwania klientów dotyczące prywatności i bezpieczeństwa danych wymagają od firm ciągłego doskonalenia strategii bezpieczeństwa. Dodatkowo, ograniczenia budżetowe mogą hamować zdolność przedsiębiorstw do inwestowania w najnowsze technologie i najlepsze praktyki.

Ekspert 4.

Bezpieczeństwo przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych jest determinowane przez szereg czynników wewnętrznych i zewnętrznych. Na zewnątrz organizacji, kluczowe zagrożenia obejmują cyberataki takie jak malware, ransomware, phishing czy ataki DDoS, które stanowią realne niebezpieczeństwo dla infrastruktury i danych organizacji. Równie ważne są zmiany w regulacjach prawnych, takich jak GDPR, które wymagają dostosowania strategii bezpieczeństwa, a szybkie tempo rozwoju technologicznego, na przykład wdrażanie sieci 5G, nakłada konieczność ciągłej aktualizacji środków ochronnych. Dodatkowo, istnieje ryzyko szpiegostwa przemysłowego i działań konkurencji, które mogą próbować uzyskać dostęp do wrażliwych informacji. W obrębie samego przedsiębiorstwa, kluczowym elementem jest kultura bezpieczeństwa, która zależy od świadomości pracowników i ich zaangażowania w przestrzeganie zasad bezpieczeństwa. Zarządzanie dostępem, zarówno do zasobów fizycznych, jak i cyfrowych, jest fundamentalne w zapobieganiu

nieautoryzowanemu dostępowi. Ważne są także fizyczne środki bezpieczeństwa, które chronią infrastrukturę i personel przed takimi zagrożeniami jak kradzież czy wandalizm, oraz skuteczność procedur reagowania na incydenty bezpieczeństwa i ciągłości operacyjnej. Na poziomie ludzkim, regularne szkolenia z zakresu bezpieczeństwa są niezbędne do minimalizowania ryzyka błędów, a kompleksowe zarządzanie ryzykiem pozwala na implementację odpowiednich środków zaradczych i prewencyjnych. Wewnętrzne zagrożenia, takie jak działania nieetyczne czy niezadowoleni pracownicy, również wymagają uwagi. W kontekście technologii i infrastruktury, kluczowe jest budowanie i utrzymywanie odpornych na awarie, ataki i katastrofy naturalne systemów informacyjno-komunikacyjnych. Regularne aktualizacje oprogramowania i systemów są konieczne, aby zapewnić ochronę przed znanymi zagrożeniami. Przyjęcie holistycznego podejścia do zarządzania tymi wszystkimi aspektami jest niezbędne. Wymaga to współpracy pomiędzy różnymi działami organizacji oraz stałego monitorowania i dostosowywania strategii bezpieczeństwa do dynamicznie zmieniającego się środowiska zagrożeń.

Ekspert 5.

Bezpieczeństwo przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych jest uwarunkowane przez szereg czynników, które można grupować w różne kategorie, każda z nich odgrywa istotną rolę w kształtowaniu ogólnego bezpieczeństwa. Postęp technologiczny, choć wprowadza innowacje takie jak 5G, Internet Rzeczy czy technologie chmurowe, jednocześnie niesie za sobą nowe zagrożenia, jak podatności oprogramowania, które mogą być wykorzystywane przez cyberprzestępców. Czynnik ludzki także ma kluczowe znaczenie, gdyż błędy pracowników, brak świadomości bezpieczeństwa czy zagrożenia wewnętrzne mogą prowadzić do naruszeń. Struktura organizacyjna i kultura korporacyjna przedsiębiorstwa są fundamentalne dla skuteczności działań bezpieczeństwa, gdzie kluczowe jest posiadanie klarownych procedur i polityk, efektywnych systemów zarządzania ryzykiem i regularnych audytów. Zewnętrzne czynniki, takie jak zmieniające się regulacje prawne czy geopolityczne napięcia, również wpływają na bezpieczeństwo, zwłaszcza w kontekście międzynarodowym, gdzie organizacje sektora technologii informacyjno-komunikacyjnych mogą stać się celami cyberataków. Ograniczenia budżetowe mogą z kolei ograniczać możliwości inwestycyjne w nowoczesne technologie i szkolenia, co negatywnie wpływa na poziom bezpieczeństwa. Na koniec, przepisy dotyczące ochrony danych osobowych, takie jak GDPR, oraz inne krajowe i międzynarodowe regulacje, wymagają od firm stosowania odpowiednich środków ochronnych i zgodności z prawem, co jest niezbędne do ochrony informacji. Efektywne zarządzanie tymi czynnikami jest kluczowe dla utrzymania wysokiego poziomu bezpieczeństwa w każdym przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych.

Ekspert 6.

Bezpieczeństwo przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych zależy od zintegrowanego podejścia obejmującego różnorodne czynniki. Kluczowe jest utworzenie jednolitej i funkcjonalnej infrastruktury bezpieczeństwa, zaprojektowanej przez specjalistów, która obejmuje nie tylko elementy fizyczne, ale także odpowiednie oprogramowanie i sprzęt, regularnie aktualizowane w odpowiedzi na nowe zagrożenia. Równie istotna jest skrupulatna i ciągła analiza potencjalnych zagrożeń, które mogą pojawiać się w dynamicznie zmieniającej się branży sektora technologii informacyjno-komunikacyjnych. Element ludzki również

odgrywa znaczącą rolę – szkolenia z zakresu świadomości bezpieczeństwa, starannie przeprowadzane procesy rekrutacyjne i monitorowanie lojalności pracowników mogą zmniejszyć ryzyko incydentów. Ponadto, niezbędne jest dostosowanie środków ochrony do specyfiki i skali identyfikowanych zagrożeń, co może obejmować zastosowanie zaawansowanych technologii kryptograficznych i bezpiecznych protokołów komunikacyjnych. Ważna jest także ochrona fizyczna obiektów infrastruktury, takich jak centra danych czy stacje bazowe, za pomocą systemów alarmowych, monitoringu wizyjnego i fizycznych barier. Całość tworzy skuteczny system obronny, który chroni przed różnorodnymi zagrożeniami.

Ekspert 7.

Bezpieczeństwo przedsiębiorstw sektora technologii informacyjno-komunikacyjnych jest kształtowane przez szereg czynników, które można podzielić na zewnętrzne i wewnętrzne. Czynniki zewnętrzne to przede wszystkim akty prawne regulujące działalność tych firm w Polsce, wpływy wynikające z łańcuchów dostaw, współpraca z partnerami biznesowymi oraz wpływ firm dostarczających technologie. Również działania klientów końcowych mają znaczący wpływ na poziom bezpieczeństwa przedsiębiorstwa, podkreślając potrzebę skutecznej ochrony aktywów i zapewnienia poufności, integralności oraz dostępności informacji tylko dla autoryzowanych użytkowników. W zakresie czynników wewnętrznych, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych muszą przestrzegać licznych regulacji prawnych i przepisów nakładających na nie określone obowiązki. Kluczowe jest wdrożenie odpowiednich procesów technicznych i technologii zgodnie z przepisami oraz posiadanych koncesji. Przykładem jest przestrzeganie prawa telekomunikacyjnego w Polsce oraz rozporządzeń takich jak RODO. Wewnętrzne aspekty bezpieczeństwa obejmują m.in. dostawy energii, które są krytyczne dla funkcjonowania przedsiębiorstwa, odpowiednie zabezpieczenie i rozmieszczenie kolokacji oraz zarządzanie dostępem fizycznym i logicznym do zasobów organizacji, co obejmuje zapewnienie bezpieczeństwa danych klientów. Ważne jest, by klient miał możliwość dostosowania ustawień swoich usług, z odpowiednią autoryzacją i autentykacją, aby unikać nieautoryzowanych zmian. Kontrolowanie i monitorowanie działań pracowników w zakresie danych powierzonych przez klientów jest również kluczowe dla zapewnienia bezpiecznych i skutecznych usług.

Ekspert 8.

Bezpieczeństwo przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych z perspektywy informatycznej jest kompleksowym wyzwaniem, które obejmuje wiele różnorodnych aspektów. Istotne czynniki to przede wszystkim zagrożenia zewnętrzne takie jak cyberataki, w tym ataki typu denial-of-service (DoS), które mogą zakłócić działanie usług, phishing, czy też zaawansowane trwałe zagrożenia (APT). Wymaga to zastosowania zaawansowanych systemów wykrywania i reagowania na incydenty (SIEM), regularnych audytów bezpieczeństwa oraz ciągłego monitorowania sieci. Istotne jest również wewnętrzne zarządzanie bezpieczeństwem, w tym polityki dotyczące silnego uwierzytelniania i szyfrowania danych, które zapewniają ochronę przesyłanych informacji oraz danych przechowywanych na serwerach. Należy także uwzględnić ryzyko wewnętrzne, związane z działaniami pracowników, które może prowadzić do nieumyślnego ujawnienia danych lub błędów w konfiguracji systemów.

Ekspert 9.

Zarządzanie bezpieczeństwem osobowym w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych wymaga integracji różnorodnych strategii zapewniających ochronę pracowników i zasobów przedsiębiorstwa. Kluczowymi czynnikami są tutaj polityki w zakresie kontroli dostępu, które muszą być rygorystycznie egzekwowane, aby ograniczyć dostęp do wrażliwych obszarów wyłącznie do autoryzowanego personelu. Szkolenia z zakresu bezpieczeństwa są niezbędne do podnoszenia świadomości personelu na temat potencjalnych zagrożeń oraz odpowiednich reakcji na incydenty bezpieczeństwa. Ponadto, kluczowe znaczenie ma procedura reagowania na incydenty, która powinna być regularnie przeglądana i aktualizowana, aby dostosować ją do ewoluującego krajobrazu zagrożeń. Ważne jest także prowadzenie regularnych audytów i testów penetracyjnych, które pomagają identyfikować i eliminować potencjalne słabości w systemach bezpieczeństwa.

Ekspert 10.

Bezpieczeństwo fizyczne przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych jest niezwykle ważne, ponieważ bez odpowiednich środków zabezpieczających, wszystkie inne formy ochrony mogą okazać się niewystarczające. Czynniki wpływające na to bezpieczeństwo obejmują kontrolę dostępu do obiektów, co można osiągnąć poprzez systemy kart dostępowych, biometryczne systemy identyfikacji, jak również przez zabezpieczenia mechaniczne takie jak zamki, bariery czy ogrodzenia. Ważne jest również zastosowanie systemów monitoringu wizyjnego, które umożliwiają ciągłą obserwację i nagrywanie aktywności w kluczowych punktach przedsiębiorstwa. Systemy alarmowe, zarówno antywłamaniowe, jak i przeciwpożarowe, muszą być regularnie testowane i konserwowane, aby zapewnić ich niezawodność w krytycznych momentach. Ponadto, należy wziąć pod uwagę planowanie awaryjne i zarządzanie kryzysowe, które są kluczowe w przypadku wystąpienia sytuacji nadzwyczajnych, takich jak katastrofy naturalne czy inne zagrożenia dla infrastruktury fizycznej.

Ekspert 11.

Czynniki wpływające na bezpieczeństwo przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych obejmują implementację nowych technologii, takich jak 5G, IoT (Internet of Things) oraz sztuczna inteligencja (AI), które wprowadzają nowe wektory ataku, wymagające odpowiednich zabezpieczeń. Kluczowe jest również regularne aktualizowanie systemów operacyjnych, aplikacji oraz firmware urządzeń, aby zabezpieczyć się przed nowymi zagrożeniami. Migracja danych i usług do chmury wiąże się z koniecznością stosowania zaawansowanych środków zabezpieczających, takich jak szyfrowanie i kontrola dostępu. Ponadto, wykorzystanie technologii takich jak SDN (Software-Defined Networking) i NFV (Network Functions Virtualization) wymaga nowych podejść do bezpieczeństwa sieciowego, które mogą skutecznie zarządzać wirtualnymi zasobami.

Ekspert 12.

Czynniki wpływające na bezpieczeństwo przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych obejmują ludzkie aspekty i odpowiednie szkolenia. Nieświadomi lub niezadowoleni pracownicy mogą stanowić poważne zagrożenie, dlatego regularne szkolenia z zakresu bezpieczeństwa i budowanie świadomości są kluczowe. Ważne jest również

stosowanie zasady najmniejszych uprawnień (least privilege) i regularne przeglądy uprawnień pracowników, co pomaga ograniczyć ryzyko nieautoryzowanego dostępu do krytycznych danych. Zaawansowane systemy monitorowania i analizy zachowań w sieci mogą wykrywać nietypowe działania i potencjalne naruszenia bezpieczeństwa. Ataki socjotechniczne, takie jak phishing i spear-phishing, są często używane przez hakerów do uzyskania dostępu do systemów, dlatego edukacja pracowników w zakresie rozpoznawania takich zagrożeń jest niezbędna.

Jaki wpływ na bezpieczeństwo przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych mają regulacje ustawowe i przepisy wewnętrzne?

Ekspert 1.
Regulacje ustawowe i przepisy wewnętrzne narzucają pewien schemat postępowania i normy funkcjonowania przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych. Obecnie funkcjonujące przepisy regulujące kwestie cyberbezpieczeństwa wymagają od przedsiębiorstw działających w branży, m. in. wymóg posiadania Security Operations Centre (centrum zapewniającego analizę i obsługę incydentów w cyberprzestrzeni przedsiębiorstwa). Większą role jednak odgrywają regulacje wewnętrzne tworzone na szczeblu zarządzania strategicznego przedsiębiorstwa. Jest to swoisty rodzaj kodeksu dobrych praktyk, który dostosowany jest do warunków, w których funkcjonuje przedsiębiorstwo. Kluczowym jest również zwrócenie uwagi na kwestie wynikające z unijnej dyrektywy NIS 2 (dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii). Wskazana dyrektywa w dużo większym stopniu określać będzie regulacje dotyczące kwestii zabezpieczeń w przedsiębiorstwach *teleinformatycznych oraz reagowania na incydenty w cyberprzestrzeni. W tej ostatniej kwestii szczególny nacisk położony został na kwestie usystematyzowania i ujednolicenia procedur.*

Ekspert 2.
Przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych, ze szczególnym uwzględnieniem przepisów prawa telekomunikacyjnego, w tym wymogu dotyczącego neutralności sieci, są zobligowane do wprowadzenia odpowiednich wewnętrznych regulacji (compliance), dzięki którym stosowane zasady i procedury w firmie są znane i powszechnie stosowane przez pracowników. Mają one chociażby gwarantować, że żadne usługi oferowane klientom indywidualnym lub biznesowym (B2B) nie dyskryminują określonych klientów, chyba że taka dyskryminacja jest prawnie uregulowana, na przykład przez ustawę antyhazardową. W niektórych przypadkach, choć przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych ma obowiązek zapewnienia neutralności sieci, może być zmuszone do blokowania dostępu do sieci ze względu na inne przepisy lub ograniczać dostęp klientów swojej sieci do określonych zasobów, zarówno krajowych, jak i zagranicznych. Compliance musi zarówno regulować wewnętrzne funkcjonowanie przedsiębiorstwa, jak i być zgodne z przepisami zewnętrznymi, aby uniknąć sprzeczności między tym, co firma chce osiągnąć biznesowo, a co jest regulowane. Regulacje ustawowe zazwyczaj nie stanowią dużego wyzwania, o ile są spójne i przewidywalne. Na przykład, jeśli istnieje prawo regulujące aukcję na konkretne pasmo częstotliwości, przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych, które wygrywa taką aukcję i nabywa licencję na 10, 15 lub nawet 20 lat, jest

zobowiązane do zapewnienia pokrycia sieci na odpowiednim obszarze lub świadczenia usług dla np. 85% ludności w określonym czasie od rozstrzygnięcia aukcji. W takich przypadkach przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych planują inwestycje i nawiązują długoterminowe relacje z dostawcami. Jednak pojawienie się nowego prawa w trakcie realizacji tych inwestycji, które nagle wymaga wyłączenia określonych dostawców, technologii lub urządzeń w trybie pilnym, stwarza dwa zasadnicze problemy. Po pierwsze, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych ponoszą straty, które mają ogólny wpływ na ich kondycję finansową i zdolność funkcjonowania. Po drugie, jeśli takie wyłączenia mają charakter globalny dla polskiego rynku, to wszystkie przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych muszą nagle w bardzo krótkim czasie zdobyć alternatywne urządzenia oraz uzyskać usługi od innych dostawców obecnych na rynku. Pytanie brzmi, czy inni dostawcy są w stanie sprostać zdecydowanie większym zamówieniom ze strony wszystkich przedsiębiorstw sektora technologii informacyjno-komunikacyjnych, jednocześnie zachowując odpowiedni poziom usług. W związku z tym regulacje prawne i ustawowe, które są wprowadzane, muszą uwzględniać realne możliwości i nie doprowadzać do sytuacji, w której przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych muszą zrezygnować z rozwoju usług i inwestycji ze względu na straty finansowe oraz konieczność dostosowania się w trybie pilnym do nowych regulacji.

Ekspert 3.

Regulacje ustawowe i przepisy wewnętrzne odgrywają kluczową rolę w kształtowaniu bezpieczeństwa przedsiębiorstw sektora technologii informacyjno-komunikacyjnych, wpływając na nie zarówno bezpośrednio, jak i pośrednio, obejmując szereg aspektów zabezpieczania infrastruktury krytycznej i danych. Regulacje prawne takie jak GDPR w Unii Europejskiej, RODO w Polsce, czy CCPA w Kalifornii wymagają od firm sektora technologii informacyjno-komunikacyjnych wdrożenia ścisłych procedur ochrony danych osobowych klientów. Ustawa o krajowym systemie cyberbezpieczeństwa i inne podobne regulacje na poziomie krajowym i międzynarodowym nakładają na te organizacje obowiązek ochrony infrastruktury krytycznej, co bezpośrednio wpływa na ich polityki bezpieczeństwa. Przepisy wewnętrzne są tworzone, by dostosować działania przedsiębiorstwa do wymogów prawnych oraz specyfiki działalności i ryzyk związanych z branżą sektora technologii informacyjno-komunikacyjnych, określając m.in. procedury dostępu do systemów, zarządzania incydentami bezpieczeństwa czy szkolenia pracowników w zakresie świadomości cyberbezpieczeństwa. Regulacje te zmuszają organizacje do systematycznego identyfikowania, oceny i zarządzania ryzykiem cybernetycznym oraz do tworzenia i utrzymywania planów ciągłości działania i odzyskiwania po awarii, co zapewnia przygotowanie na różne scenariusze i minimalizuje potencjalne szkody wynikające z incydentów bezpieczeństwa. Ponadto, dzięki wymogom regulacyjnym przedsiębiorstwa są zachęcane do stosowania najlepszych praktyk i międzynarodowych standardów w dziedzinie bezpieczeństwa informacji, takich jak ISO/IEC 27001, co przyczynia się do podnoszenia ogólnego poziomu bezpieczeństwa w branży. Przestrzeganie regulacji i wdrożenie solidnych przepisów wewnętrznych wzmacniają wizerunek organizacji jako zaufanego dostawcy, co jest kluczowe dla utrzymania i rozwoju relacji biznesowych oraz dla konkurencyjności na rynku. Organizacje muszą nieustannie monitorować i dostosowywać się do zmieniających się przepisów, co wymaga elastyczności i innowacyjności w podejściu do zarządzania bezpieczeństwem. To z kolei może stymulować

rozwój nowych technologii i metod ochrony. Podsumowując, regulacje ustawowe i przepisy wewnętrzne są fundamentalne dla zapewnienia bezpieczeństwa przedsiębiorstw sektora technologii informacyjno-komunikacyjnych, kreując ramy działania, które wspierają zarządzanie ryzykiem, ochronę danych i ciągłość operacyjną, wymagając jednak od organizacji ciągłego monitorowania zmian prawnych, dostosowywania procedur oraz inwestowania w rozwój kompetencji i technologii bezpieczeństwa.

Ekspert 4.

Regulacje ustawowe oraz przepisy wewnętrzne odgrywają kluczową rolę w zapewnianiu bezpieczeństwa przedsiębiorstw sektora technologii informacyjno-komunikacyjnych, oddziałując na nie zarówno bezpośrednio, jak i pośrednio. Moje doświadczenie zdobyte w sektorze technologii informacyjno-komunikacyjnych pozwala mi zauważyć, że regulacje prawne takie jak ogólne rozporządzenie o ochronie danych (GDPR) w Europie oraz inne lokalne przepisy dotyczące ochrony danych i bezpieczeństwa sieci ustanawiają minimalne standardy, które przedsiębiorstwa muszą spełniać. Dzięki nim możliwe jest zapewnienie ochrony danych osobowych klientów i utrzymanie zaufania do usług informacyjno-komunikacyjnych. Regulacje te motywują również przedsiębiorstwa do stosowania najlepszych dostępnych praktyk i technologii, a także wspierają współpracę między przedsiębiorstwami a rządami oraz innymi sektorami w celu wspólnego rozwiązywania problemów bezpieczeństwa. Z kolei przepisy wewnętrzne pozwalają przedsiębiorstwu na dostosowanie ogólnych wymogów prawnych do własnych potrzeb i specyfiki działalności, co zwiększa skuteczność implementowanych rozwiązań bezpieczeństwa. One również przyczyniają się do rozwoju kultury bezpieczeństwa wśród pracowników oraz umożliwiają szczegółowe zarządzanie ryzykiem związanym z bezpieczeństwem informacji. Dobrze opracowane procedury wewnętrzne dotyczące reagowania na incydenty i plany ciągłości działania są kluczowe dla minimalizacji skutków ewentualnych ataków i szybkiego przywracania normalnego funkcjonowania. Podsumowując, zarówno regulacje ustawowe, jak i przepisy wewnętrzne stanowią fundament zapewnienia wysokiego poziomu bezpieczeństwa w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych. Ich odpowiednie zastosowanie i ciągłe dostosowywanie do zmieniających się warunków i zagrożeń są kluczowe dla ochrony zarówno infrastruktury, jak i danych klientów.

Ekspert 5.

Regulacje ustawowe i przepisy wewnętrzne stanowią fundamentalną podstawę dla utrzymania i zapewnienia bezpieczeństwa w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych. Stanowią one zestaw zasad i wymogów, które przedsiębiorstwo musi spełniać, aby zabezpieczyć swoją infrastrukturę, dane i usługi przed różnymi formami zagrożeń. Regulacje te mogą obejmować kwestie związane z ochroną danych osobowych, zarządzaniem ryzykiem, ciągłością działania, bezpieczeństwem infrastruktury krytycznej oraz obowiązkami w zakresie raportowania incydentów bezpieczeństwa. Z jednej strony, regulacje ustawowe, takie jak RODO (Ogólne Rozporządzenie o Ochronie Danych) w Unii Europejskiej czy inne lokalne i międzynarodowe przepisy dotyczące cyberbezpieczeństwa, nakładają na przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych szereg obowiązków prawnych. Te obowiązki mogą dotyczyć zarówno sposobu przetwarzania i zabezpieczania danych osobowych klientów, jak i wymogów dotyczących zgłaszania naruszeń bezpieczeństwa

danych do odpowiednich organów nadzorczych. Z drugiej strony, przepisy wewnętrzne, opracowane i wdrożone przez same przedsiębiorstwa, dostosowują ogólne wymogi prawne do specyfiki działalności danego przedsiębiorstwa, uwzględniając jego rozmiar, charakter przetwarzanych danych i realne zagrożenia dla bezpieczeństwa. Przepisy te mogą obejmować polityki bezpieczeństwa informacji, procedury reagowania na incydenty, zasady zarządzania dostępem i identyfikacji użytkowników, a także regularne audyty i testy bezpieczeństwa. Współdziałanie regulacji ustawowych i przepisów wewnętrznych kreuje kompleksowy system zarządzania bezpieczeństwem, który jest kluczowy dla skutecznej ochrony przedsiębiorstw sektora technologii informacyjno-komunikacyjnych przed rosnącym spektrum zagrożeń cyfrowych. Ponadto, odpowiednie stosowanie się do tych regulacji buduje zaufanie klientów i partnerów biznesowych, co jest nieocenioną wartością w sektorze technologii informacyjno-komunikacyjnych, gdzie zaufanie i wiarygodność są kluczowe dla utrzymania konkurencyjności na rynku.

Ekspert 6.

Regulacje ustawowe oraz przepisy wewnętrzne są niezwykle istotne w zapewnieniu bezpieczeństwa przedsiębiorstw sektora technologii informacyjno-komunikacyjnych, oddziałując na nie na wielu poziomach. Wprowadzone przez Unię Europejską dyrektywy, takie jak NIS 2, zobowiązują te organizacje do wdrażania zaawansowanych technologicznych i organizacyjnych rozwiązań, w tym na przykład do tworzenia specjalistycznych jednostek jak Security Operations Centre (SOC), które monitorują bezpieczeństwo sieci i reagują na incydenty. Działania te mają na celu standaryzację i ujednolicenie procedur w celu podniesienia poziomu cyberbezpieczeństwa w całej Unii. Z kolei przepisy wewnętrzne, formułowane jako kodeks dobrych praktyk, są dostosowane do unikalnych potrzeb i zagrożeń danej organizacji, często przewyższając wymogi ustawowe. Te wewnętrzne regulacje mogą obejmować zasady postępowania z danymi klientów czy polityki dostępu do systemów. Organizacje sektora technologii informacyjno-komunikacyjnych podlegają również międzynarodowym standardom branżowym, takim jak normy ISO, które mogą być integralną częścią ich wewnętrznych regulacji. Ponadto, regulacje te stymulują organizacje do stosowania najnowszych technologii i najlepszych praktyk, co nie tylko minimalizuje ryzyko incydentów, ale również sprzyja innowacjom, które mogą ustanawiać nowe standardy w branży. Wszystko to razem wpływa znacząco na poziom bezpieczeństwa w kontekście rosnących zagrożeń cybernetycznych.

Ekspert 7.

Przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych muszą przestrzegać przepisów prawa telekomunikacyjnego, w tym wymogów dotyczących neutralności sieci, co obliguje je do implementacji odpowiednich wewnętrznych regulacji zapewniających, że zasady i procedury są powszechnie znane i stosowane przez pracowników. Te regulacje mają na celu zapewnienie, że usługi oferowane klientom indywidualnym oraz biznesowym nie będą dyskryminować określonych grup odbiorców, chyba że takie działania są bezpośrednio usankcjonowane prawem, na przykład przez ustawę antyhazardową. Czasami, w związku z innymi przepisami prawnymi, przedsiębiorstwo może być zmuszone do ograniczenia dostępu do swojej sieci, co wpływa na dostępność określonych zasobów zarówno krajowych, jak i zagranicznych. Stosowanie wewnętrznych regulacji jest niezbędne nie tylko dla zarządzania

wewnętrznym funkcjonowaniem organizacji, ale także musi być zgodne z zewnętrznymi przepisami prawnymi, co zapobiega konfliktom między celami biznesowymi a regulacjami prawnymi. Ustawa regulująca, na przykład, aukcję pasm częstotliwości zobowiązuje wygrywające przedsiębiorstwo do zapewnienia pokrycia sieci na określonym obszarze lub świadczenia usług dla określonego procenta populacji w wyznaczonym czasie, co wymaga od firm długoterminowego planowania i inwestycji. Jednakże, wprowadzenie nowego prawa, które nagle zmienia zasady gry, wymuszając wycofanie określonych dostawców czy technologii, może powodować znaczące straty finansowe dla przedsiębiorstw sektora technologii informacyjno-komunikacyjnych i wpłynąć na ich zdolność do funkcjonowania. Gdy takie zmiany mają charakter globalny, wymagają od wszystkich firm sektora technologii informacyjno-komunikacyjnych szybkiego dostosowania się i pozyskania alternatywnych rozwiązań, co stawia pod znakiem zapytania możliwości dostawców do zaspokojenia nagłego wzrostu popytu przy zachowaniu odpowiedniej jakości usług. Dlatego nowo wprowadzane regulacje prawne i ustawowe muszą uwzględniać realne możliwości firm i nie powinny prowadzić do sytuacji, gdzie przedsiębiorstwa są zmuszone rezygnować z dalszego rozwoju i inwestycji z powodu finansowych strat i konieczności szybkiej adaptacji do zmienionych regulacji.

Ekspert 8.

Regulacje ustawowe i przepisy wewnętrzne mają kluczowe znaczenie dla bezpieczeństwa informatycznego przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych. Zewnętrzne regulacje, takie jak Ogólne Rozporządzenie o Ochronie Danych (GDPR) w Unii Europejskiej, wymagają od firm stosowania odpowiednich środków technicznych i organizacyjnych do ochrony danych osobowych, co bezpośrednio wpływa na metody przechowywania i przetwarzania danych przez przedsiębiorstwa. Z kolei lokalne regulacje dotyczące cyberbezpieczeństwa mogą nakładać obowiązek regularnych audytów bezpieczeństwa, raportowania incydentów bezpieczeństwa oraz implementacji zaawansowanych technologii zabezpieczających. Przepisy wewnętrzne, takie jak polityki dostępu i zarządzania hasłami, zapewniają dodatkową warstwę ochrony poprzez kontrolę, kto i w jaki sposób może korzystać z zasobów przedsiębiorstwa, co jest kluczowe w prewencji wycieków danych i innych zagrożeń.

Ekspert 9.

Regulacje prawne oraz przepisy wewnętrzne odgrywają istotną rolę w zapewnieniu bezpieczeństwa osobowego w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych. Ustawodawstwo związane z ochroną pracy, takie jak przepisy dotyczące zdrowia i bezpieczeństwa w miejscu pracy, wymusza na firmach tworzenie bezpiecznych środowisk pracy, co obejmuje zarówno fizyczne, jak i psychologiczne aspekty bezpieczeństwa pracowników. Wewnętrzne kodeksy postępowania oraz polityki etyczne kształtują kulturę korporacyjną, promując odpowiedzialne zachowania i zapobiegając nadużyciom oraz innym działaniom mogącym zagrażać bezpieczeństwu przedsiębiorstwa. Przestrzeganie tych przepisów jest kluczowe nie tylko dla zapewnienia zgodności z prawem, ale także dla utrzymania zaufania klientów i partnerów biznesowych.

Ekspert 10.

W kontekście bezpieczeństwa fizycznego, regulacje ustawowe i przepisy wewnętrzne mają zasadnicze znaczenie dla ochrony infrastruktury przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych. Regulacje takie jak przepisy przeciwpożarowe, normy bezpieczeństwa budowlanego czy przepisy dotyczące zarządzania kryzysowego wymuszają na firmach implementację odpowiednich systemów bezpieczeństwa oraz regularne przeglądy techniczne obiektów. Dzięki temu możliwe jest minimalizowanie ryzyka katastrof, jak również szybkie reagowanie na awarie czy inne nieprzewidziane zdarzenia. Wewnętrzne przepisy dotyczące kontroli dostępu czy monitoringu wizyjnego umożliwiają skuteczną ochronę przed nieautoryzowanym dostępem, zarówno przez osoby trzecie, jak i przez niefrasobliwych pracowników, co jest niezbędne dla zachowania integralności krytycznej infrastruktury informacyjno-komunikacyjnej.

Ekspert 11.

Regulacje ustawowe i przepisy wewnętrzne odgrywają kluczową rolę w zapewnieniu bezpieczeństwa przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych. Regulacje prawne, takie jak dyrektywa NIS 2 w Unii Europejskiej, nakładają na przedsiębiorstwa obowiązek implementacji zaawansowanych rozwiązań technologicznych i organizacyjnych, które mają na celu ochronę przed cyberzagrożeniami. Przepisy te wymagają również regularnych audytów bezpieczeństwa i zgodności z normami, co zmusza organizacji do stałego podnoszenia standardów zabezpieczeń. Wewnętrzne przepisy i polityki bezpieczeństwa, które są dostosowane do specyficznych warunków działania organizacji, uzupełniają regulacje prawne, umożliwiając lepsze zarządzanie ryzykiem i reakcję na incydenty bezpieczeństwa. Wprowadzenie jednolitych procedur, które są zgodne z przepisami ustawowymi, jest kluczowe dla stworzenia spójnego i efektywnego systemu ochrony.

Ekspert 12.

Regulacje ustawowe i przepisy wewnętrzne mają istotny wpływ na bezpieczeństwo przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych poprzez ustanowienie ram prawnych i proceduralnych, które pomagają chronić przed zagrożeniami wewnętrznymi i zewnętrznymi. Przepisy prawne, takie jak regulacje dotyczące ochrony danych osobowych (RODO), narzucają obowiązek wdrażania odpowiednich środków ochrony danych i zgłaszania naruszeń bezpieczeństwa, co zwiększa odpowiedzialność firm za ochronę informacji. Wewnętrzne przepisy, takie jak polityki dostępu i procedury zarządzania incydentami, zapewniają strukturalne podejście do zarządzania bezpieczeństwem. Takie przepisy pomagają również w budowaniu kultury bezpieczeństwa wśród pracowników, poprzez szkolenia i monitorowanie zgodności z politykami organizacji. Przepisy te są niezbędne do ustanowienia jasno określonych ról i odpowiedzialności, co ułatwia szybkie i skuteczne reagowanie na incydenty bezpieczeństwa.

Jakie zagrożenia dla bezpieczeństwa przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych odnotowuje się najczęściej?

Ekspert 1.

Najczęściej odnotowywane zagrożenia związane są z obecną sytuacją polityczną w regionie. Głównymi aktorami na tym polu są Rosja oraz Chiny, które prowadzą operacje APT (Advanced Persistent Threats – głównym celem tych ataków jest własność intelektualna przechowywana na komputerach organizacji i opierają się o atak na nieświadomego użytkownika sieci posiadającego dostęp z pozycji stacji roboczej do interesujących atakującego danych lub plików), infiltrują i upubliczniają dane przedsiębiorstw, penetrują sieci wewnętrzne w celu wykrywania i wykorzystania podatności oraz szpiegostwo. W przypadku przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych, szpiegostwo realizowane jest głównie w wymiarze cyberprzestrzeni. Zatem z tego punktu widzenia, klienci przedsiębiorstwa znajdują się w zainteresowaniu służb rosyjskich i chińskich i odnotowuje się ataki różnego rodzaju wymierzone w zasoby przedsiębiorstwa. Głównym rodzajem odnotowywanych ataków są mało i średnio zaawansowane ataki typu DDoS, próby realizowania kampanii phishingowych, ataki typu XSS, Remote Shell oraz ataki kombinowane mające na celu sprawdzenie zabezpieczeń. Odnotowywane są również przypadki szpiegostwa przemysłowego, które jest trudne do wykrycia, jednak przedsiębiorstwo stara się monitorować taki przypadki i minimalizować straty. Dodatkowo, pod uwagę brane są również zagrożenia związane z działaniem sił natury. Analizowane są głównie pod kątem możliwości wystąpienia, wpływu na funkcjonowanie przedsiębiorstwa oraz minimalizowania skutków ich wystąpienia

Ekspert 2.

Jednym z powszechnych zagrożeń, z jakimi spotykają się przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych na co dzień, są ataki typu DOS (Denial of Service) lub D-DOS (Distributed Denial of Service), które występują w różnych skalach. Ataki te mają na celu zaszkodzić infrastrukturze, usługom lub punktom wymiany informacji, takim jak punkty międzyoperatorskie. Ataki te różnią się parametrami, zarówno pod względem czasu trwania, jak i wolumenu generowanego ruchu. Niektóre z tych ataków są bardzo intensywne. Innym wyzwaniem, z jakim przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych muszą się zmagać, są problemy związane z inwestycjami, zwłaszcza w przypadku budowy nowych stacji bazowych w Polsce. Proces uzyskania zgód w celu postawienia nowych stacji bazowych jest zwykle długotrwały i skomplikowany. Nawet po uzyskaniu zgód, istnieje lista organizacji, które mogą protestować przeciwko inwestycji. W rezultacie, budowa jednej stacji bazowej może potrwać nawet 3 lata, mimo że mogłaby zostać zrealizowana w ciągu 2 miesięcy. Ponadto, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych muszą radzić sobie z sezonowymi zjawiskami pogodowymi, takimi jak silne wiatry lub obfite opady śniegu. W przypadku przerw w dostawach energii na obszarze objętym tymi zjawiskami, usługi nie mogą być świadczone, gdyż po wyczerpaniu awaryjnych źródeł zasilania, takich jak baterie lub generatory, kończą się możliwości techniczne i usługi nie są świadczone. Oprócz ataków typu DOS, istnieje wiele innych rodzajów cyberataków, których celem jest przejęcie kontroli nad zasobami lub uzyskanie dostępu do systemów i danych poprzez skompromitowane uprawnienia lub stosując socjotechniki. Takie ataki stanowią poważne zagrożenie, zwłaszcza w przypadku ransomware, gdy odzyskanie normalnego funkcjonowania usług i systemów jest zazwyczaj skomplikowane i długotrwałe. Należy również uwzględnić zagrożenia wewnętrzne związane z pracownikami. Istnieje ryzyko, że niezadowolony pracownik może próbować pozyskać jak najwięcej informacji wewnętrznych, aby wykorzystać je poza firmą (np. w nowej pracy). Im szerszy dostęp do danych i systemów ma pracownik, tym większe potencjalne szkody może

wyrządzić w przypadku działania z premedytacją i niezgodnie z przyjętymi zasadami. Istnieją również przypadki, w których pracownik, nieświadomie lub w wyniku błędnej procedury, może spowodować przerwy w działaniu systemu lub w usługach, które są oparte na tym systemie.

Ekspert 3.

Przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych, ze względu na swoją specyfikę działalności i kluczowe znaczenie dla społeczeństwa oraz gospodarki, są narażone na różnorodne zagrożenia, które mogą znacząco wpłynąć na ich operacje. Ataki DDoS, które polegają na zasypywaniu systemów informacyjno-kacyjnych ogromną ilością niepożądanych zapytań, mają na celu przeciążenie i uniemożliwienie normalnego funkcjonowania, stanowią poważne wyzwanie dla tych firm, czyniąc je atrakcyjnym celem dla cyberprzestępców. Ponadto, phishing i inne ataki socjotechniczne, które polegają na podszywaniu się pod zaufane instytucje w celu wyłudzenia poufnych informacji, są powszechne wśród użytkowników usług informacyjno-komunikacyjnych, a pracownicy tych firm mogą stać się celem ataków mających na celu uzyskanie dostępu do wewnętrznych systemów. Ataki na łańcuch dostaw, które wykorzystują słabości w zabezpieczeniach jednego z ogniw łańcucha, również stanowią zagrożenie dla infrastruktury telekomunikacyjnej. Złośliwe oprogramowanie, takie jak spyware, ransomware, wirusy i trojany, stanowi ciągłe zagrożenie dla systemów i danych firm sektora technologii informacyjno-komunikacyjnych, prowadząc do potencjalnej utraty danych, zakłóceń w świadczeniu usług oraz szkód finansowych. Naruszenia danych, które mogą prowadzić do poważnych konsekwencji prawnych, finansowych i reputacyjnych, są szczególnie niebezpieczne, ponieważ przedsiębiorstwa te przechowują ogromne ilości danych osobowych i poufnych informacji biznesowych. Ataki na infrastrukturę krytyczną, które mają na celu destabilizację lub szpiegostwo państwowe, podkreślają znaczenie sieci telekomunikacyjnych dla państwa i gospodarki. Niezadowoleni pracownicy lub ci, którzy nieświadomie naruszają polityki bezpieczeństwa, mogą również stanowić wewnętrzne zagrożenie dla bezpieczeństwa informacji. Dodatkowo, niezałatane luki w zabezpieczeniach sprzętu i oprogramowania mogą być wykorzystane przez cyberprzestępców do przeprowadzenia ataków. Zarządzanie ryzykiem i skuteczne strategie ochrony są kluczowe dla zapewnienia ciągłości działania, ochrony danych klientów oraz infrastruktury krytycznej, co jest niezbędne dla przedsiębiorstw sektora technologii informacyjno-komunikacyjnych w obliczu tych wyzwań.

Ekspert 4.

Na podstawie mojego doświadczenia w policji oraz w branży sektora technologii informacyjno-komunikacyjnych, zidentyfikowałem różne zagrożenia, które mają wpływ na bezpieczeństwo przedsiębiorstw sektora technologii informacyjno-komunikacyjnych, zarówno w aspekcie cybernetycznym, jak i fizycznym. Do zagrożeń cybernetycznych zaliczają się między innymi ataki DDoS, które przeciążają systemy i uniemożliwiają dostęp do usług, próby wyłudzenia poufnych informacji poprzez phishing oraz inne ataki socjotechniczne, a także malware i ransomware, które mogą infekować systemy, kraść dane lub szyfrować je w celu uzyskania okupu. Istotne są także ataki na łańcuch dostaw, gdzie wykorzystywane są słabości w zabezpieczeniach dostawców do uzyskania dostępu do systemów organizacji. W obszarze zagrożeń fizycznych wymienia się włamania, kradzieże czy sabotaż infrastruktury, które mogą zakłócić działanie usług. Zagrożenia wewnętrzne obejmują działania niezadowolonych pracowników, którzy mają dostęp do systemów i mogą być motywowani chęcią zemsty lub

korzyści osobistej, a także błędy ludzkie, takie jak nieprawidłowe konfiguracje systemów, które mogą prowadzić do luk w bezpieczeństwie. Przestarzała infrastruktura i oprogramowanie często zawierają niezałatane luki bezpieczeństwa, co ułatwia przeprowadzenie ataków. Naruszenia danych i wycieki informacji mogą prowadzić do naruszeń prywatności oraz konsekwencji prawnych i finansowych. Szpiegostwo przemysłowe jest kolejnym zagrożeniem, gdzie konkurencyjne organizacje lub państwa mogą próbować uzyskać dostęp do tajemnic handlowych. Aby skutecznie zarządzać tymi zagrożeniami, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych muszą stosować wielowarstwowe strategie bezpieczeństwa, które łączą zaawansowane technologie, procedury operacyjne i szkolenia dla pracowników. Kluczowe jest także utrzymanie bliskiej współpracy z organami ścigania i innymi instytucjami zajmującymi się cyberbezpieczeństwem.

Ekspert 5.

Bezpieczeństwo przedsiębiorstw sektora technologii informacyjno-komunikacyjnych jest narażone na różnorodne zagrożenia, które mogą poważnie zakłócić ich działalność. Cyberataki, takie jak phishing, malware, ransomware oraz ataki DDoS, stanowią poważne zagrożenie, mogąc uszkadzać systemy, zakłócać działanie sieci czy prowadzić do kradzieży wrażliwych danych. Równie istotne są wewnętrzne zagrożenia wynikające z błędów pracowników, niewłaściwego zarządzania dostępem czy świadomych działań szkodzących bezpieczeństwu przedsiębiorstwa, podejmowanych przez obecnych lub byłych pracowników. Zagrożenia mogą również pochodzić od konkurencyjnych firm lub rządów, które dążą do uzyskania dostępu do tajemnic handlowych czy innych poufnych informacji. Podatności w oprogramowaniu i sprzęcie, spowodowane nieaktualnymi systemami czy błędami w oprogramowaniu, również mogą być wykorzystywane przez cyberprzestępców. Fizyczne zagrożenia, takie jak kradzież lub zniszczenie sprzętu, mogą prowadzić do utraty danych i zakłóceń w funkcjonowaniu usług. Dodatkowo, metody manipulacji psychologicznej, jak inżynieria społeczna, phishing, czy vishing (voice phishing), są stosowane do uzyskiwania poufnych informacji. Zabezpieczenie przed tymi zagrożeniami wymaga zastosowania zarówno technicznych środków ochrony, jak i edukacji pracowników, by zwiększyć ich świadomość na temat potencjalnych niebezpieczeństw.

Ekspert 6.

Przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych są wystawione na wiele różnorodnych zagrożeń, które mogą przybierać różne formy. Na przykład zaawansowane ataki trwałe, znane jako APT, często prowadzone przez państwowe agencje wywiadowcze z krajów takich jak Rosja i Chiny, stanowią jedno z najpoważniejszych zagrożeń. Mają one na celu długotrwałe i dyskretne penetracje sieci w celu kradzieży wartościowych danych, takich jak własność intelektualna, wykorzystując przy tym metody takie jak phishing czy manipulowanie nieświadomymi użytkownikami wewnątrz organizacji. Innym przykładem są ataki DDoS, które polegają na zalewaniu serwerów dużą ilością ruchu sieciowego, powodując ich przeciążenie i uniemożliwiając dostęp do usług. Dodatkowo, organizacje te są również narażone na kampanie phishingowe, które wykorzystują fałszywe komunikaty do wyłudzania danych logowania lub innych poufnych informacji, często z wykorzystaniem technik socjotechnicznych. Ataki typu Cross-Site Scripting (XSS) i Remote Shell umożliwiają atakującym wprowadzenie szkodliwego kodu do systemów lub zdalne kontrolowanie urządzeń ofiar, co stanowi techniczne

zagrożenie dla bezpieczeństwa. Szpiegostwo przemysłowe, często motywowane konkurencyjnymi lub geopolitycznymi celami, jest kolejnym poważnym wyzwaniem dla tych przedsiębiorstw. W końcu, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych muszą również uwzględniać ryzyko związane z siłami natury, jak huragany, powodzie czy trzęsienia ziemi, które mogą bezpośrednio wpływać na ich infrastrukturę fizyczną. Całościowe zarządzanie bezpieczeństwem w tych firmach wymaga ciągłej analizy i adaptacji do różnorodnych zagrożeń, zarówno tych wynikających z działalności ludzkiej, jak i zdarzeń naturalnych, co jest kluczowe dla utrzymania ich stabilności i bezpieczeństwa.

Ekspert 7.

Przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych codziennie mierzą się z różnorodnymi wyzwaniami, w tym z atakami typu Denial of Service (DOS) i Distributed Denial of Service (DDOS), które mają na celu zakłócenie działania infrastruktury, usług lub punktów wymiany informacji, takich jak punkty międzyoperatorskie. Te ataki mogą znacznie różnić się skalą, czasem trwania oraz ilością generowanego ruchu, a niektóre z nich są szczególnie intensywne. Innym istotnym problemem dla tych przedsiębiorstw są trudności inwestycyjne, szczególnie widoczne podczas budowy nowych stacji bazowych, które w Polsce mogą napotkać na skomplikowany i czasochłonny proces zatwierdzania. Mimo uzyskania niezbędnych zgód, opóźnienia mogą wynikać z protestów różnych organizacji, co może przedłużyć realizację projektu nawet do trzech lat, chociaż technicznie możliwe byłoby zakończenie prac w ciągu dwóch miesięcy. Przedsiębiorstwa te muszą także radzić sobie z wpływem zjawisk pogodowych, takich jak silne wiatry czy obfite opady śniegu, które mogą prowadzić do przerw w dostawach energii. W takich przypadkach, gdy wyczerpią się awaryjne źródła zasilania, jak baterie czy generatory, możliwości techniczne do świadczenia usług są ograniczone. Poza atakami DOS i DDOS, przedsiębiorstwa te stają również w obliczu innych zagrożeń cybernetycznych, takich jak ataki ransomware, które mogą skomplikować lub uniemożliwić odzyskanie normalnego funkcjonowania systemów i usług. Istnieje także ryzyko związane z wewnętrznymi zagrożeniami od pracowników, którzy będąc niezadowoleni lub działając z premedytacją, mogą próbować wykorzystać wewnętrzne informacje poza firmą, na przykład przy zmianie pracy. Błędy pracowników, wynikające z niewiedzy lub błędnych procedur, również mogą prowadzić do przerw w działaniu systemów lub usług, co podkreśla konieczność skutecznego zarządzania dostępem do danych i systemów w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych.

Ekspert 8.

W przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych najczęściej odnotowuje się zagrożenia związane z cyberatakami. Do najbardziej powszechnych należą ataki typu DDoS (Distributed Denial of Service), które mają na celu zakłócenie działania usług przez przeciążenie systemów. Innym częstym zagrożeniem są ataki phishingowe, które celują w wyłudzenie poufnych informacji, takich jak dane logowania użytkowników. Ważnym zagrożeniem są również ataki wykorzystujące złośliwe oprogramowanie (malware), w tym ransomware, które może zaszyfrować dane przedsiębiorstwa i żądać okupu za ich odblokowanie. Oprócz tych, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych muszą zmagać się z zagrożeniami wewnętrznymi, takimi jak nieumyślne błędy

pracowników lub niewłaściwe zarządzanie konfiguracją systemów, co może prowadzić do luk w zabezpieczeniach.

Ekspert 9.
Z punktu widzenia bezpieczeństwa osobowego, jednym z głównych zagrożeń dla przedsiębiorstw sektora technologii informacyjno-komunikacyjnych jest nieautoryzowany dostęp do obiektów i informacji. Zagrożenia te mogą wynikać zarówno z działań zewnętrznych, jak i wewnętrznych. Wśród zagrożeń wewnętrznych kluczowe są błędy ludzkie, takie jak nieprzestrzeganie procedur bezpieczeństwa, co może prowadzić do wycieku informacji. Innym poważnym zagrożeniem jest kradzież danych przez pracowników, którzy mają dostęp do wrażliwych informacji. Zagrożenia zewnętrzne obejmują próby infiltracji przez osoby trzecie, które mogą próbować uzyskać dostęp do infrastruktury przedsiębiorstwa poprzez podszywanie się pod pracowników lub dostawców.

Ekspert 10.
Zagrożenia dla bezpieczeństwa fizycznego przedsiębiorstw sektora technologii informacyjno-komunikacyjnych często obejmują włamania do obiektów, wandalizm, jak również zagrożenia naturalne, takie jak pożary czy powodzie, które mogą uszkodzić krytyczną infrastrukturę. Włamania są szczególnie niebezpieczne, ponieważ mogą prowadzić do kradzieży sprzętu oraz dostępu do ważnych danych. Wandalizm, choć mniej szkodliwy dla danych, może powodować przerwy w świadczeniu usług i wymagać kosztownych napraw. Katastrofy naturalne, choć rzadkie, stanowią poważne zagrożenie dla infrastruktury fizycznej, zwłaszcza w regionach narażonych na ekstremalne zjawiska pogodowe. Dlatego kluczowe jest stosowanie odpowiednich środków zapobiegawczych, takich jak systemy alarmowe, monitoring i odpowiednie zabezpieczenia przeciwpowodziowe i przeciwpożarowe.

Ekspert 11.
Najczęściej odnotowywane zagrożenia dla bezpieczeństwa przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych związane są z zaawansowanymi stałymi zagrożeniami (APT), które są często inicjowane przez państwowe agencje wywiadowcze, takie jak te z Rosji i Chin. APT mają na celu długotrwałą i dyskretną penetrację sieci w celu kradzieży wartościowych danych. Ponadto, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych często stają w obliczu ataków typu DDoS (Distributed Denial of Service), które mogą powodować znaczne zakłócenia w usługach. Infiltracja przez zaawansowane malware, ataki na infrastrukturę sieciową oraz kradzież danych klientów również należą do częstych zagrożeń. Technologie takie jak IoT (Internet of Things) wprowadzają nowe wektory ataku, które mogą być wykorzystane do przeprowadzania zaawansowanych ataków na infrastrukturę informacyjno-komunikacyjną.

Ekspert 12.
Najczęściej odnotowywane zagrożenia dla bezpieczeństwa przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych obejmują zarówno zagrożenia wewnętrzne, jak i zewnętrzne. Do najczęstszych zagrożeń należą ataki socjotechniczne, takie jak phishing i spear-phishing, które mają na celu wyłudzenie danych logowania od pracowników. Częste są również ataki typu DDoS, które mają na celu zakłócenie usług. Wewnętrzne zagrożenia, takie

jak nieświadome działania pracowników, którzy mogą przypadkowo ujawnić poufne informacje, są równie istotne. Ataki z wykorzystaniem luk w oprogramowaniu, kradzież danych przez niezadowolonych pracowników oraz próby infiltracji przez zewnętrznych hakerów, którzy starają się uzyskać dostęp do krytycznych systemów, stanowią poważne ryzyko. Warto również zauważyć, że nieautoryzowane użycie platform do wymiany plików przez pracowników może prowadzić do przypadkowego wycieku informacji.

d)

W jaki sposób przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych powinno ocenić ryzyko związane z bezpieczeństwem informacji?

Ekspert 1.

Ocena zagrożeń powinna obejmować swoistą klasyfikację tych które mogą wystąpić najczęściej oraz te rzadko spotykane wraz z adekwatnymi procedurami reagowania. Głównymi obszarami, na których skupia się przedsiębiorstwo to ocena zabezpieczenia cybernetycznego oraz wycieku informacji. Odnotowywane są przypadki wykorzystywania przez pracowników przedsiębiorstwa ogólnodostępnych platform i serwisów do wymiany plików i informacji na potrzeby przesyłania firmowych dokumentów. Znamiennym jest przykład ostatniego wycieku tajnych informacji wywiadowczych zbieranych przez CIA na temat wojny w Ukrainie. Dokumenty zostały ujawnione na platformie Discord przez żołnierza Gwardii Narodowej USA. Zatem znamiennym jest odpowiednie szkolenie pracowników pracujących z danymi wrażliwymi oraz ścisłe monitorowanie dostępu do tych danych, obiegu oraz powielania. Również z punktu wizerunkowego, nie jest pożądanym zjawiskiem upublicznianie informacji opatrzonych firmowym logo w sposób niekontrolowany w sieci Internet.

Ekspert 2.

Jeśli chodzi o zapewnienie bezpieczeństwa informacji, kluczowym krokiem jest przeprowadzenie klasyfikacji posiadanych danych. Klasyfikacja ta polega na podziale informacji na różne kategorie, takie jak np. publicznie dostępne, do użytku wewnętrznego, chronione i ściśle tajne. Następnie konieczne jest zidentyfikowanie, które z tych informacji podlegają określonym przepisom prawnym. Na przykład wiele danych i informacji przetwarzanych przez te przedsiębiorstwa podlega zarówno prawu telekomunikacyjnemu, jak i RODO. W takim przypadku konieczne jest dostosowanie środków zabezpieczających do przepisów. Jeśli chodzi o informacje niejawne, istotnym aspektem jest certyfikacja systemów, które są zaimplementowane przez przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych przez właściwe organy państwa. Należy także uwzględnić odpowiednie poświadczenia bezpieczeństwa dla pracowników. Ocena ryzyka informacyjnego powinna uwzględniać potencjalne zagrożenia związane z danymi. Należy wziąć pod uwagę możliwość utraty, ujawnienia, zmiany lub braku dostępu do danych. Przy analizie ryzyka konieczne jest uwzględnienie potencjalnych wektorów ataku lub zagrożeń związanych z niedostępnością danych. Warto zastanowić się również nad lokalizacją informacji. Niektóre dane muszą być dostępne z zewnątrz, na przykład dla klientów, którzy chcą mieć dostęp do faktur lub zmieniać ustawienia usług. Inne systemy, takie jak systemy typu billing lub CRM, są przeznaczone wyłącznie dla użytku wewnętrznego i powinny być chronione przed dostępem osób trzecich z zewnątrz. Informacje powinny zostać podzielone na odpowiednie klasy, z uwzględnieniem ich

lokalizacji w systemach. Następnie należy przypisać odpowiednie role dostępu dla pracowników i klientów, aby zapobiec dostępowi do informacji, do których nie powinni mieć dostępu. Monitorowanie działań użytkowników i wykrywanie odstępstw od typowych dostępów jest kluczowe. Jeśli wystąpią jakiekolwiek nieprawidłowości, takie jak próby dostępu zewnętrznego bez użycia odpowiednich VPN-ów, powinny być generowane alerty. Ocena ryzyka musi uwzględniać również transfer danych na zewnątrz i wewnętrzny. Wprowadzenie odpowiednich zabezpieczeń, takich jak śledzenie działań, blokady DLP, kontrole dostępu, migawki danych i backupy, jest kluczowe dla ochrony danych. Backupy powinny być przechowywane zarówno wewnątrz organizacji, aby umożliwić szybkie przywracanie, jak i na zewnątrz, aby zapobiec całkowitej utracie danych w przypadku utraty kolokacji. Podsumowując, klasyfikacja informacji, mapowanie dostępu, analiza ryzyka, wprowadzanie środków zabezpieczających i monitorowanie działań stanowią integralną pętlę zwrotną procesu zapewniania bezpieczeństwa informacji. Konieczne jest także uwzględnienie przepisów prawnych i ewentualnych zmian w tych przepisach, aby dostosować strategie zabezpieczeń do zmieniającego się otoczenia prawnotechnicznego.

Ekspert 3.

Ocena ryzyka związana z bezpieczeństwem informacji to kluczowy proces w zarządzaniu cyberbezpieczeństwem przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych, umożliwiający identyfikację, analizę i priorytetowanie potencjalnych zagrożeń dla zasobów informacyjnych oraz opracowanie strategii ich minimalizacji. Proces ten powinien być integralną częścią ogólnej strategii bezpieczeństwa informacji w organizacji. W pierwszej kolejności należy zidentyfikować wszystkie kluczowe aktywa informacyjne organizacji, takie jak dane, systemy, sieci, oprogramowanie, sprzęt oraz zależne od nich procesy biznesowe i usługi. Następnie, dla każdego zidentyfikowanego aktywa, określić potencjalne zagrożenia, takie jak ataki cybernetyczne, awarie sprzętu czy błędy ludzkie, a także istniejące podatności, które mogą być przez te zagrożenia wykorzystane. Kolejnym krokiem jest ocena prawdopodobieństwa wystąpienia każdego zagrożenia oraz potencjalnego wpływu na organizację, w tym konsekwencje finansowe, wpływ na reputację, operacje biznesowe oraz zgodność z obowiązującymi przepisami prawa. Używając oceny prawdopodobieństwa i wpływu, określić poziom ryzyka dla każdego scenariusza zagrożenia, co można zrobić za pomocą metodyki oceny ryzyka, takiej jak macierz ryzyka, która ułatwia wizualizację i priorytetowanie ryzyka. Następnie, dla ryzyk o najwyższym priorytecie, opracować strategie zarządzania tymi ryzykami, które mogą obejmować unikanie ryzyka, jego akceptację, przeniesienie (na przykład poprzez ubezpieczenie) lub łagodzenie (poprzez wdrożenie odpowiednich kontroli bezpieczeństwa). Ważne jest, aby wybrane środki bezpieczeństwa były proporcjonalne do poziomu ryzyka. Po wyborze odpowiednich środków, należy je wdrożyć, aby zmniejszyć prawdopodobieństwo wystąpienia identyfikowanych zagrożeń lub ich wpływ na organizację. Proces oceny ryzyka powinien być cykliczny. Ważne jest, aby regularnie monitorować środowisko pod kątem nowych zagrożeń i podatności oraz przeprowadzać przeglądy oceny ryzyka, aby dostosować strategie zarządzania ryzykiem do zmieniającego się otoczenia. Ocena ryzyka wymaga zaangażowania wielu działów w organizacji, w tym IT, bezpieczeństwa informacji, prawnego, finansowego i operacyjnego, a także wsparcia ze strony kierownictwa.

Ekspert 4.

Ocena ryzyka związanego z bezpieczeństwem informacji to kluczowy element zarządzania bezpieczeństwem w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych. Z mojego doświadczenia wynika, że proces ten powinien zaczynać się od identyfikacji aktywów informacyjnych wymagających ochrony, takich jak dane osobowe klientów, informacje finansowe, tajemnice handlowe, infrastruktura krytyczna oraz inne zasoby cyfrowe i fizyczne. Następnie aktywa te należy sklasyfikować według ich wrażliwości i wartości dla przedsiębiorstwa, co pozwoli skoncentrować wysiłki ochronne na najważniejszych zasobach. Kolejnym etapem jest identyfikacja potencjalnych zagrożeń dla każdego z aktywów oraz istniejących podatności, które mogą zostać wykorzystane przez te zagrożenia. Zagrożenia te mogą pochodzić zarówno z zewnątrz, jak i z wewnątrz organizacji. Ocena ryzyka obejmuje analizę prawdopodobieństwa wystąpienia zagrożenia i potencjalnych skutków dla organizacji, gdzie ryzyko może być klasyfikowane jako wysokie, średnie lub niskie. Na podstawie tej oceny, przedsiębiorstwo powinno opracować plan działań mający na celu zmniejszenie ryzyka do akceptowalnego poziomu. Może to obejmować wzmocnienie zabezpieczeń technicznych, wprowadzenie nowych polityk i procedur, szkolenia dla pracowników oraz plany reagowania na incydenty. Kluczowe jest również regularne monitorowanie środowiska bezpieczeństwa informacji i przeprowadzanie okresowych przeglądów oceny ryzyka, aby dostosować się do nowych zagrożeń, zmian w technologii i środowisku biznesowym. Ważne jest także, aby wyniki oceny ryzyka oraz plany zarządzania ryzykiem były komunikowane wszystkim zainteresowanym stronom, w tym zarządowi, pracownikom i, w stosownych przypadkach, partnerom zewnętrznym. Szkolenie pracowników w zakresie rozpoznawania zagrożeń i właściwego reagowania jest niezbędne do zwiększenia ogólnej odporności organizacji. Efektywne zarządzanie ryzykiem w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych wymaga podejścia opartego na danych, które pozwala na głębokie zrozumienie i odpowiednie adresowanie zagrożeń związanych z bezpieczeństwem informacji.

Ekspert 5.

Przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych, aby skutecznie zarządzać bezpieczeństwem informacji, musi zastosować kompleksowe podejście do oceny ryzyka, które obejmuje zrozumienie przetwarzanych, przechowywanych i przesyłanych danych. Kluczowe jest ustalenie, które z tych danych są krytyczne dla działalności przedsiębiorstwa i wymagają szczególnej ochrony. Po zidentyfikowaniu aktywów konieczne jest ich klasyfikowanie według poziomu poufności i znaczenia, co pomoże w późniejszym określeniu odpowiednich środków bezpieczeństwa. Firma powinna również zidentyfikować potencjalne zagrożenia dla każdego z klasyfikowanych aktywów, zarówno wewnętrzne, jak i zewnętrzne, takie jak błędy pracowników, nadużycia, cyberataki czy katastrofy naturalne. Następnie należy ocenić podatność systemów i procesów na te zagrożenia, identyfikując istniejące środki bezpieczeństwa i potencjalne luki. Ważne jest również ocenienie potencjalnego wpływu każdego zagrożenia na działalność przedsiębiorstwa, co można przeprowadzić za pomocą analizy wpływu na działalność (BIA). Na tej podstawie przeprowadza się ocenę ryzyka, łącząc prawdopodobieństwo wystąpienia zagrożeń z ich potencjalnym wpływem, co pozwala na priorytetyzację ryzyk. W oparciu o ocenę ryzyka, przedsiębiorstwo powinno opracować plan działań zaradczych, określający, jakie środki bezpieczeństwa należy wzmocnić lub wprowadzić, aby zminimalizować ryzyko do akceptowalnego poziomu. Ponieważ bezpieczeństwo informacji to proces ciągły, firma powinna regularnie monitorować środowisko bezpieczeństwa,

aktualizować ocenę ryzyka i dostosowywać środki bezpieczeństwa w odpowiedzi na nowe zagrożenia i zmieniające się warunki. Takie podejście umożliwia skuteczną ocenę i zarządzanie ryzykiem związanym z bezpieczeństwem informacji, co jest kluczowe dla ochrony zasobów organizacji oraz utrzymania zaufania klientów i partnerów biznesowych.

Ekspert 6.

Ocena ryzyka związana z bezpieczeństwem informacji w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych powinna być kompleksowym procesem, który uwzględnia różnorodność potencjalnych zagrożeń i związanych z nimi skutków. Pierwszym etapem jest identyfikacja wszystkich potencjalnych zagrożeń dla bezpieczeństwa informacji, które mogą dotyczyć przedsiębiorstwa, w tym cyberzagrożeń jak ataki hakerskie, malware, phishing, a także zagrożeń fizycznych jak kradzież sprzętu czy katastrofy naturalne, oraz zagrożeń wewnętrznych takich jak nieautoryzowane użycie danych przez pracowników. Po rozpoznaniu zagrożeń następuje analiza ryzyka, w której ocenia się prawdopodobieństwo wystąpienia każdego z nich oraz potencjalne skutki dla organizacji. W tym kontekście ryzyka klasyfikowane są jako wysokie, średnie lub niskie, co ułatwia priorytetyzację działań zapobiegawczych i reakcyjnych. Kolejnym krokiem jest ocena obecnych środków zabezpieczających przed zagrożeniami, zarówno technologicznych jak firewall'e, antywirusy, szyfrowanie danych, jak i organizacyjnych takich jak polityki bezpieczeństwa czy procedury awaryjne, aby ustalić, czy są one wystarczające, czy wymagają wzmocnienia. Specjalna uwaga powinna być poświęcona ryzyku wycieku informacji, w tym przypadkowemu lub nieautoryzowanemu udostępnianiu danych przez pracowników, a niekontrolowane użycie platform do wymiany plików przez pracowników stanowi znaczące ryzyko. W związku z tym konieczne jest implementowanie i monitorowanie polityk dostępu oraz zarządzanie prawami dostępu do danych. Niezbędne są regularne szkolenia dotyczące bezpieczeństwa informacji dla pracowników, które powinny obejmować zagrożenia związane z cyberbezpieczeństwem, odpowiednie praktyki dotyczące ochrony informacji oraz konsekwencje naruszeń polityk organizacji. Dodatkowo, ciągłe monitorowanie systemów informatycznych oraz regularne przeglądy procedur i polityk bezpieczeństwa informacji pomagają w wykrywaniu i reagowaniu na nowe zagrożenia, co powinno również obejmować audyty bezpieczeństwa przeprowadzane przez zewnętrzne organizacje, które mogą zapewnić obiektywną ocenę zabezpieczeń. Przedsiębiorstwo powinno również mieć gotowy i przetestowany plan reagowania na incydenty bezpieczeństwa, który określa procedury postępowania w przypadku różnych typów naruszeń bezpieczeństwa. Skuteczna ocena ryzyka wymaga systematycznego podejścia, które obejmuje identyfikację, analizę, ochronę, edukację i ciągłe doskonalenie środków zabezpieczających, co pozwala minimalizować potencjalne zagrożenia dla bezpieczeństwa informacji.

Ekspert 7.

Kluczowym aspektem zapewnienia bezpieczeństwa informacji w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych jest odpowiednia klasyfikacja danych, która umożliwia ich podział na różne kategorie, takie jak informacje publicznie dostępne, do użytku wewnętrznego, chronione oraz ściśle tajne. Takie rozróżnienie jest niezbędne, aby zidentyfikować, które dane wymagają szczególnej ochrony zgodnie z obowiązującymi przepisami prawnymi, takimi jak prawo telekomunikacyjne czy przepisy RODO. Ważne jest, aby przedsiębiorstwa dostosowały swoje środki ochronne do specyficznych wymogów każdej

kategorii danych, w tym certyfikacji systemów i poświadczeń bezpieczeństwa dla pracowników odpowiedzialnych za ich przetwarzanie. Ocena ryzyka informacyjnego powinna obejmować analizę potencjalnych zagrożeń, takich jak utrata, ujawnienie, zmiana danych lub ograniczenia dostępu do nich. Konieczne jest rozważenie wszystkich możliwych wektorów ataku oraz ryzyka związanego z dostępnością danych. Przy tym istotne jest rozpatrzenie lokalizacji przechowywania danych – niektóre z nich muszą być dostępne zdalnie, na przykład dla klientów chcących zarządzać swoimi kontami, podczas gdy inne, takie jak systemy fakturowania czy CRM, powinny być dostępne tylko wewnątrz organizacji i odpowiednio zabezpieczone. Niezbędne jest również monitorowanie aktywności użytkowników oraz wykrywanie wszelkich nieprawidłowości, które mogą świadczyć o próbach nieautoryzowanego dostępu. Wszelkie odstępstwa od normalnego wzorca dostępów powinny skutkować natychmiastowymi alertami. Ponadto, ocena ryzyka powinna uwzględniać zarówno wewnętrzny, jak i zewnętrzny transfer danych, wymagając zastosowania odpowiednich środków bezpieczeństwa, takich jak systemy śledzenia działań, zabezpieczenia typu DLP, kontrole dostępu, a także tworzenie kopii zapasowych i migawek danych, które powinny być przechowywane zarówno lokalnie, jak i zewnętrznie, aby zapewnić możliwość szybkiego przywrócenia systemów w przypadku awarii. Ostatecznie, bezpieczeństwo informacji musi być ciągle dostosowywane do zmieniających się ram prawnych i technologicznych, aby zapewnić skuteczną ochronę danych w dynamicznym środowisku.

Ekspert 8.

Ocena ryzyka związanego z bezpieczeństwem informacji w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych powinna opierać się na kompleksowym podejściu, które uwzględnia zarówno techniczne, jak i organizacyjne aspekty bezpieczeństwa. Proces ten powinien rozpocząć się od identyfikacji wszystkich aktywów, takich jak dane, systemy i infrastruktura, które wymagają ochrony. Następnie, konieczne jest zidentyfikowanie potencjalnych zagrożeń dla tych aktywów, w tym ataków cybernetycznych, błędów ludzkich, awarii sprzętu i innych. Każde zagrożenie należy ocenić pod kątem prawdopodobieństwa jego wystąpienia oraz potencjalnego wpływu na organizację. Po zidentyfikowaniu i ocenie zagrożeń, przedsiębiorstwo powinno ustalić odpowiednie środki zaradcze i kontrolne, aby zminimalizować ryzyko i jego wpływ. Te środki mogą obejmować zarówno technologie bezpieczeństwa, jak i procedury operacyjne, a także szkolenia dla pracowników. Kluczowe jest regularne przeprowadzanie audytów bezpieczeństwa i aktualizacja oceny ryzyka, aby zapewnić, że strategie bezpieczeństwa nadal skutecznie chronią przed zmieniającym się krajobrazem zagrożeń.

Ekspert 9.

Ocena ryzyka w kontekście bezpieczeństwa osobowego powinna skupić się na identyfikacji potencjalnych zagrożeń dla bezpieczeństwa pracowników oraz wrażliwych danych osobowych. Proces ten wymaga dokładnego zrozumienia, jakie dane są przetwarzane, przechowywane i transmitowane w organizacji, a także kto ma do nich dostęp. Ważne jest, aby analizować nie tylko ryzyka zewnętrzne, ale także potencjalne zagrożenia wewnętrzne, takie jak nieautoryzowany dostęp czy wycieki informacji spowodowane przez pracowników. Należy wdrożyć odpowiednie procedury weryfikacji tożsamości i kontroli dostępu, a także promować kulturę bezpieczeństwa wśród personelu przez regularne szkolenia i kampanie

świadomościowe. Strategia oceny ryzyka powinna również uwzględniać odpowiednie protokoły reagowania na incydenty, które umożliwią szybką reakcję w przypadku naruszenia bezpieczeństwa.

Ekspert 10.

Ocena ryzyka z perspektywy bezpieczeństwa fizycznego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych powinna koncentrować się na fizycznej ochronie zasobów. Należy dokładnie analizować lokalizacje i stan infrastruktury krytycznej, identyfikować potencjalne słabe punkty w zabezpieczeniach fizycznych, takie jak dostęp do niezabezpieczonych wejść, okien czy systemów wentylacyjnych. Ważne jest również rozważenie zagrożeń naturalnych, takich jak powodzie czy trzęsienia ziemi, które mogą wpłynąć na fizyczne struktury przedsiębiorstwa. Po zidentyfikowaniu wszystkich potencjalnych zagrożeń, firma powinna opracować plany zabezpieczeń obejmujące zarówno prewencyjne środki bezpieczeństwa, jak i procedury reagowania na awarie, aby zapewnić ciągłość działania i minimalizację skutków ewentualnych incydentów.

Ekspert 11.

Przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych powinno ocenić ryzyko związane z bezpieczeństwem informacji poprzez wdrożenie kompleksowego procesu zarządzania ryzykiem. Proces ten powinien zaczynać się od identyfikacji wszystkich potencjalnych zagrożeń, które mogą wpłynąć na bezpieczeństwo informacji, takich jak ataki cybernetyczne, awarie systemów, czy błędy ludzkie. Następnie, każdemu zidentyfikowanemu zagrożeniu powinno się przypisać prawdopodobieństwo wystąpienia oraz potencjalny wpływ na organizację. Analiza ryzyka powinna uwzględniać zarówno techniczne aspekty, takie jak podatności systemów i aplikacji, jak i operacyjne aspekty, takie jak procedury zarządzania incydentami. Kluczowe jest również wykorzystanie zaawansowanych narzędzi analitycznych i systemów do monitorowania bezpieczeństwa, które mogą pomóc w ciągłym śledzeniu zagrożeń i szybkim reagowaniu na nie. Ostatecznie, przedsiębiorstwo powinno regularnie przeglądać i aktualizować swoją analizę ryzyka, aby dostosować się do zmieniającego się krajobrazu zagrożeń i technologii.

Ekspert 12.

Ocena ryzyka związana z bezpieczeństwem informacji w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych powinna obejmować kilka kluczowych kroków. Pierwszym krokiem jest przeprowadzenie dokładnej analizy zagrożeń, która identyfikuje potencjalne wektory ataków, zarówno wewnętrznych, jak i zewnętrznych. Należy również przeprowadzić szczegółową ocenę zabezpieczeń, aby zidentyfikować luki w obecnych systemach i procedurach. Ważnym elementem jest również analiza ryzyka związanego z działaniami pracowników, w tym ich zachowania online i zgodności z politykami bezpieczeństwa przedsiębiorstwa. Przedsiębiorstwo powinno wdrożyć polityki dostępowe i procedury zarządzania uprawnieniami, które ograniczają dostęp do wrażliwych informacji tylko do osób, które ich potrzebują do wykonywania swoich obowiązków. Regularne szkolenia z zakresu bezpieczeństwa informacji i budowanie świadomości zagrożeń wśród pracowników są kluczowe. Dodatkowo, regularne testy penetracyjne i audyty bezpieczeństwa mogą pomóc w identyfikacji słabości systemu i ocenie gotowości organizacji do reagowania na incydenty.

Wszystkie te działania powinny być skoordynowane w ramach kompleksowego programu zarządzania ryzykiem, który jest regularnie aktualizowany i dostosowywany do nowych zagrożeń.

e)

Jakie aspekty są kluczowe dla polityki bezpieczeństwa informacji, które powinny być implementowane w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych?

Ekspert 1.

Główną rolę odgrywa zakres dostępu do informacji. Access policy management i access policy lists są dwiema głównymi metodami pozwalającymi przedsiębiorcy na monitorowanie obiegu informacji w firmie, kontrolę dostępu oraz nadzór nad prawidłowym dostępem wyznaczonych pracowników do określonych informacji. Dodatkowo, istotnym jest monitoring dostępu pracowników do domeny głównej funkcjonującej w przedsiębiorstwie, służbowej poczty elektronicznej oraz dostępu do usług w chmurze. W ramach organizacji pewne procedury dostępowe zostały narzucone odgórnie i każda zmiana zakresu dostępu do informacji realizowana jest na odpowiednio uzasadniony wniosek. Odnotowywane są próby dostępu do obszarów poza zakresem dostępu pracownika, lecz są one sporadyczne i wynikają bardziej użytkownika niż ze świadomego działania.

Ekspert 2.

Proces zapewniania bezpieczeństwa informacji obejmuje kilka kluczowych etapów. Po pierwsze, konieczna jest klasyfikacja informacji, czyli ich podział na różne kategorie, uwzględniając ich charakter i poufność. Po drugie, istotne jest ustalenie, kto ma dostęp do poszczególnych informacji, w oparciu o określone zasady i uprawnienia. Należy precyzyjnie określić, jakie osoby lub grupy mają prawo do jakich danych. Kolejnym krokiem jest zdefiniowanie, w jaki sposób sklasyfikowane informacje mogą być udostępniane zarówno wewnątrz organizacji, jak i na zewnątrz. Konieczne jest opracowanie odpowiednich procedur i zasad, które regulują proces udostępniania danych. W przypadku kontaktów z partnerami biznesowymi, dostawcami czy innymi podmiotami zewnętrznymi, konieczne jest zapewnienie, że polityka bezpieczeństwa informacji jest stosowana również na tych interfejsach. Ostatecznym etapem jest implementacja odpowiednich środków zabezpieczających. Polityka bezpieczeństwa informacji powinna być wdrożona wewnątrz organizacji, tak aby wszyscy pracownicy mieli świadomość jej istnienia i przestrzegali jej postanowień. Ponadto, powinny zostać podjęte działania mające na celu zabezpieczenie informacji w relacjach zewnętrznych, tak aby zapewnić, że przedsiębiorstwo działa zgodnie z przyjętymi standardami bezpieczeństwa we współpracy z partnerami biznesowymi, dostawcami itp. Podsumowując, proces zapewniania bezpieczeństwa informacji wymaga przeprowadzenia klasyfikacji, ustalenia zasad dostępu, rozważenia sposobów udostępniania danych oraz implementacji odpowiednich środków zabezpieczających. Ważne jest, aby polityka bezpieczeństwa informacji była konsekwentnie stosowana zarówno wewnątrz organizacji, jak i we wszystkich interakcjach zewnętrznych, zapewniając ochronę danych na wszystkich poziomach.

Ekspert 3.

Polityka bezpieczeństwa informacji stanowi fundament ochrony danych i systemów w każdym przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych, a jej skuteczność zależy od kompleksowości i dostosowania do specyfiki organizacji oraz otoczenia, w jakim funkcjonuje. Istotne elementy, które powinny być uwzględnione w takiej polityce, to między innymi zarządzanie tożsamością i kontrola dostępu, co oznacza zapewnienie, że tylko uprawnione osoby mają dostęp do określonych informacji i zasobów przez implementację wielopoziomowej weryfikacji tożsamości oraz zasad minimalnych uprawnień. Ochrona infrastruktury i zabezpieczenia techniczne, w tym stosowanie firewalli, systemów wykrywania i zapobiegania intruzom, szyfrowania danych oraz regularne aktualizacje i łatki bezpieczeństwa, są kluczowe do ochrony przed atakami zewnętrznymi i wewnętrznymi. Opracowanie i wdrożenie procedur reagowania na incydenty bezpieczeństwa, w tym procesy identyfikacji, zgłaszania, analizy, reakcji na incydenty oraz odzyskiwania po awarii, są niezbędne do zarządzania incydentami bezpieczeństwa. Regularne szkolenia pracowników na temat bezpieczeństwa informacji, w tym bezpiecznych praktyk online i rozpoznawania prób phishingu, są kluczowe dla podnoszenia świadomości bezpieczeństwa. Ponadto, przeprowadzanie regularnych ocen ryzyka i audytów bezpieczeństwa pozwala na identyfikację słabości i zagrożeń dla systemów informacyjnych oraz opracowywanie planów zarządzania ryzykiem. Ważne jest także implementowanie środków ochrony danych osobowych i prywatności zgodnych z lokalnymi i międzynarodowymi przepisami, takimi jak GDPR, oraz zabezpieczanie fizyczne infrastruktury IT przed dostępem nieautoryzowanymi osobami. Zarządzanie ciągłością działania, w tym opracowanie i utrzymanie planów ciągłości działania i odzyskiwania po awarii, minimalizuje przerwy w dostępie do usług i danych. Współpraca z partnerami i dostawcami, szczególnie przy outsourcingu usług i przetwarzaniu danych poza organizacją, wymaga zapewnienia odpowiednich środków bezpieczeństwa. Regularne przeglądy i aktualizacje polityki bezpieczeństwa informacji dostosowują ją do zmieniającego się otoczenia, nowych zagrożeń i regulacji prawnych. Implementacja tych zasad w polityce bezpieczeństwa informacji pozwala stworzyć solidne fundamenty dla ochrony zasobów informacyjnych przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych, zwiększając jednocześnie zaufanie klientów i partnerów biznesowych do organizacji.

Ekspert 4.

Polityka bezpieczeństwa informacji przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych powinna obejmować kompleksowe podejście do zarządzania dostępem, gdzie dostęp do informacji jest ograniczony do osób, które faktycznie go potrzebują, zgodnie z zasadami minimalnych uprawnień. Stosowanie silnych algorytmów szyfrowania jest kluczowe do ochrony danych przechowywanych i przesyłanych, zwłaszcza tych wrażliwych lub regulowanych prawem. Warto również zabezpieczyć infrastrukturę krytyczną i zasoby fizyczne przed nieautoryzowanym dostępem, kradzieżą czy uszkodzeniem. Implementacja zaawansowanych rozwiązań takich jak firewall'e, systemy wykrywania i zapobiegania intruzom, pomoże chronić przed zagrożeniami zarówno zewnętrznymi, jak i wewnętrznymi. Opracowanie efektywnych procedur reagowania na incydenty umożliwia szybkie identyfikowanie, analizowanie i reagowanie na zagrożenia. Ponadto, regularne szkolenia z zakresu bezpieczeństwa informacji są niezbędne, aby pracownicy byli świadomi potencjalnych zagrożeń i znali sposoby ich minimalizowania. Nie można też zapomnieć o zarządzaniu ciągłością działania i utrzymaniu planów odzyskiwania po awarii, które są

kluczowe dla funkcjonowania przedsiębiorstwa w przypadku poważnych incydentów. Zgodność z przepisami prawnymi i standardami branżowymi, takimi jak GDPR czy Dyrektywa o bezpieczeństwie sieci i systemów informacyjnych, jest fundamentalna dla utrzymania legalności działań i zaufania klientów. Regularne oceny ryzyka są niezbędne do identyfikacji i zarządzania zagrożeniami. Zarządzanie dostawcami i partnerami biznesowymi również wymaga zapewnienia, że spełniają oni odpowiednie wymogi bezpieczeństwa, szczególnie przy outsourcingu usług lub przetwarzaniu danych. Skuteczna polityka bezpieczeństwa informacji jest niezbędna do ochrony przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych przed różnorodnymi zagrożeniami i zapewnia zgodność z przepisami, co przyczynia się do utrzymania zaufania klientów.

Ekspert 5.

Implementacja skutecznej polityki bezpieczeństwa informacji w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych jest kluczowa dla ochrony wrażliwych danych i infrastruktury krytycznej przed zagrożeniami. Polityka ta powinna zaczynać się od klasyfikacji danych, która umożliwia określenie rodzajów danych przetwarzanych przez firmę oraz ustalenie poziomu poufności i znaczenia tych danych dla działalności organizacji. Ważnym elementem jest zarządzanie dostępem, które opiera się na zasadzie najmniejszych uprawnień, zapewniając pracownikom dostęp jedynie do tych zasobów, które są im niezbędne do pracy. Zastosowanie technik szyfrowania chroni dane podczas przesyłania i przechowywania, zapobiegając nieautoryzowanemu dostępowi. Wdrażanie środków ochrony fizycznej oraz zabezpieczeń sieciowych, takich jak zapory ogniowe i systemy wykrywania włamań, jest niezbędne do ochrony infrastruktury. Opracowanie procedur reagowania na incydenty bezpieczeństwa pozwala na szybką identyfikację i neutralizację zagrożeń. Planowanie ciągłości działania i odzyskiwania danych po awarii jest kluczowe dla przywrócenia funkcji biznesowych po incydentach bezpieczeństwa. Regularne szkolenia z zakresu bezpieczeństwa informacji są niezbędne, aby zwiększyć świadomość pracowników na temat zagrożeń i nauczyć ich, jak zapobiegać incydentom. Ponadto, przeprowadzanie regularnych audytów bezpieczeństwa i przeglądów polityk oraz procedur gwarantuje, że są one aktualne i efektywne w obliczu ciągle zmieniających się zagrożeń. Taka kompleksowa polityka bezpieczeństwa jest niezbędna dla ochrony przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych w dzisiejszym dynamicznie zmieniającym się środowisku zagrożeń.

Ekspert 6.

Kluczowe aspekty polityki bezpieczeństwa informacji w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych obejmują różnorodne elementy zarządzania dostępem do informacji oraz monitorowanie aktywności użytkowników. Zarządzanie dostępem do informacji to fundamentalny element polityki bezpieczeństwa, który polega na definiowaniu, kto może mieć dostęp do jakich informacji w organizacji. Jest to kluczowe do zapobiegania nieautoryzowanemu dostępowi do wrażliwych danych. Ustanowienie list polityk dostępu, które określają, jakie zasoby są dostępne dla poszczególnych użytkowników lub grup, pomaga kontrolować przepływ informacji i powinny być one regularnie aktualizowane oraz przeglądane w odpowiedzi na zmieniające się potrzeby biznesowe i zagrożenia. Monitorowanie, kto i kiedy uzyskuje dostęp do kluczowych zasobów, takich jak domena główna, służbowa poczta elektroniczna oraz usługi w chmurze, jest niezwykle ważne do wykrywania

nieautoryzowanych lub nietypowych prób dostępu, co jest istotne dla wczesnego rozpoznawania potencjalnych zagrożeń. Jasne procedury dotyczące zmian w uprawnieniach dostępowych są niezbędne do tego, by każda zmiana była dokładnie analizowana i uzasadniona, co zapobiega przypadkowym błędom lub celowym nadużyciom. System powinien również być wyposażony w mechanizmy umożliwiające szybką reakcję na próby nieautoryzowanego dostępu. Regularne szkolenia dla pracowników dotyczące polityk bezpieczeństwa, najlepszych praktyk dostępu oraz metod rozpoznawania i reagowania na incydenty bezpieczeństwa są kluczowe do zwiększenia świadomości zagrożeń i zachęcania do odpowiedzialnego postępowania. Implementacja tych aspektów wymaga ciągłego zaangażowania i monitorowania przez zespoły IT oraz bezpieczeństwa, oraz współpracy z pracownikami, co znacząco przyczynia się do ochrony przedsiębiorstwa przed cyberzagrożeniami oraz zapewnia jego bezpieczne funkcjonowanie.

Ekspert 7.

Zapewnienie bezpieczeństwa informacji to złożony proces, który rozpoczyna się od klasyfikacji danych według ich poufności i znaczenia, co umożliwia ich podział na odpowiednie kategorie. Ważnym krokiem jest ustalenie, które osoby lub grupy mają uprawnienia do dostępu do poszczególnych kategorii danych, co wymaga precyzyjnych zasad dostępu. Następnie, należy zdefiniować, jak informacje mogą być udostępniane zarówno wewnątrz przedsiębiorstwa, jak i na zewnątrz, co obejmuje opracowanie procedur regulujących ten proces. Kluczowe jest również zapewnienie, by polityka bezpieczeństwa informacji była przestrzegana przy każdym kontakcie z partnerami biznesowymi, dostawcami i innymi zewnętrznymi podmiotami. Ostatnim etapem jest wdrożenie środków ochronnych, które mają na celu zabezpieczenie informacji przed nieuprawnionym dostępem i zagrożeniami. Polityka bezpieczeństwa informacji powinna być jasna i zrozumiała dla wszystkich pracowników, a także stosowana konsekwentnie we wszystkich działaniach organizacji, zarówno wewnętrznych, jak i w relacjach zewnętrznych, aby zapewnić skuteczną ochronę danych na każdym etapie ich przetwarzania.

Ekspert 8.

Polityka bezpieczeństwa informacji w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych powinna koncentrować się na kilku kluczowych aspektach, aby zapewnić skuteczną ochronę danych i systemów. Pierwszym jest identyfikacja i klasyfikacja danych, która umożliwia rozumienie, jakie informacje są krytyczne i wymagają szczególnej ochrony. Kolejny ważny element to zabezpieczenia techniczne, takie jak szyfrowanie danych, firewalle, systemy wykrywania i zapobiegania intruzom oraz zabezpieczenia antywirusowe. Niezwykle ważne jest także zarządzanie dostępem, które obejmuje implementację zasad minimalnych uprawnień i autoryzacji dwuskładnikowej. Polityka powinna również zawierać procedury reagowania na incydenty bezpieczeństwa, które określają, jak organizacja powinna postępować w przypadku naruszenia bezpieczeństwa, w tym protokoły komunikacji, oceny szkód i działań naprawczych. Wymagana jest także ciągła edukacja i szkolenie pracowników, aby podnosić ich świadomość na temat potencjalnych zagrożeń i właściwych praktyk bezpieczeństwa.

Ekspert 9.

Polityka bezpieczeństwa informacji z punktu widzenia bezpieczeństwa osobowego powinna uwzględniać procedury weryfikacji i kontrolowania tożsamości pracowników oraz

kontrahentów, co jest kluczowe dla ograniczenia dostępu do wrażliwych danych i systemów tylko do autoryzowanych osób. Ważnym aspektem jest również rozwijanie kultury bezpieczeństwa wśród pracowników poprzez regularne szkolenia, które podnoszą świadomość zagrożeń i uczą odpowiednich reakcji na potencjalne incydenty. Polityka powinna również obejmować ścisłe procedury dotyczące korzystania z urządzeń mobilnych i pracy zdalnej, co ma na celu zapobieganie nieautoryzowanemu dostępowi do sieci firmowej z niezabezpieczonych urządzeń. Kluczowe jest także stworzenie jasnych wytycznych dotyczących procedur zgłaszania naruszeń bezpieczeństwa, aby pracownicy wiedzieli, jak postępować w przypadku wykrycia potencjalnego zagrożenia.

Ekspert 10.

W kontekście polityki bezpieczeństwa informacji, z punktu widzenia fizycznego bezpieczeństwa, kluczowe są środki zabezpieczające infrastrukturę przedsiębiorstwa, takie jak kontrola dostępu do obiektów, monitorowanie wizyjne oraz systemy alarmowe. Ważne jest zabezpieczenie fizyczne serwerowni, centrów danych i innych krytycznych punktów, które mogą być celami dla ataków fizycznych lub aktów wandalizmu. Implementacja środków przeciwpożarowych oraz planów ewakuacyjnych jest również niezbędna, aby zapewnić ochronę w przypadku pożarów lub innych zagrożeń. Polityka powinna uwzględniać również zarządzanie kluczami i dostępami, zapewniając, że tylko autoryzowany personel posiada dostęp do kluczowych zasobów fizycznych. Regularne przeglądy i testy systemów bezpieczeństwa fizycznego są niezbędne, aby utrzymać ich skuteczność i adekwatność do ewoluujących zagrożeń.

Ekspert 11.

Kluczowe aspekty polityki bezpieczeństwa informacji, które powinny być implementowane w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych, obejmują zarządzanie dostępem do informacji oraz integrację zaawansowanych technologii zabezpieczeń. Przede wszystkim, polityka powinna określać jasne zasady dotyczące zarządzania dostępem do danych, wykorzystując access policy management i access policy lists. Te narzędzia pozwalają na skuteczne monitorowanie i kontrolowanie dostępu pracowników do wrażliwych informacji. Wdrożenie zaawansowanych technologii, takich jak systemy wykrywania intruzów (IDS/IPS), rozwiązania DLP (Data Loss Prevention) oraz narzędzia do monitorowania aktywności użytkowników, jest kluczowe dla zabezpieczenia infrastruktury informacyjno-komunikacyjnej. Polityka powinna również uwzględniać regularne aktualizacje oprogramowania i systemów, aby chronić przed nowymi zagrożeniami.

Ekspert 12.

Kluczowe aspekty polityki bezpieczeństwa informacji w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych obejmują zarządzanie dostępem, szkolenia pracowników oraz procedury reagowania na incydenty. Polityka powinna jasno określać, kto ma dostęp do jakich danych i na jakich warunkach, a zarządzanie dostępem powinno być oparte na zasadzie najmniejszych uprawnień (least privilege). Regularne szkolenia z zakresu bezpieczeństwa informacji są niezbędne, aby zwiększyć świadomość pracowników na temat zagrożeń i najlepszych praktyk. Polityka powinna również obejmować procedury reagowania na incydenty, które umożliwiają szybkie i skuteczne działanie w przypadku wykrycia naruszenia bezpieczeństwa. Monitorowanie aktywności pracowników, szczególnie tych, którzy mają dostęp

do krytycznych systemów, jest kluczowe dla wykrywania i zapobiegania nieautoryzowanym działaniom. Wreszcie, polityka powinna zawierać zasady dotyczące przechowywania i szyfrowania danych, aby zapewnić ich ochronę przed nieautoryzowanym dostępem i kradzieżą.

f)

W jaki sposób przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych powinno zarządzać dostępem do poufnych informacji i danych?

Ekspert 1.

Odpowiednia i świadoma polityka dostępu do informacji i danych wdrożona przez przedsiębiorstwo oraz efektywnie funkcjonująca kancelaria tajna, która odpowiada za nadzór nad prawidłowym obiegiem dokumentacji niejawnej przetwarzanej w przedsiębiorstwie. Istotnym jest również zarządzanie dostępem do informacji na podstawie aktualnych certyfikatów i poświadczeń bezpieczeństwa. Ponadto, przedsiębiorstwo stosuje przepisy wynikające z przepisów unijnych i krajowych dotyczących ochrony danych osobowych. W kwestii uregulowań wewnętrznych przedsiębiorstwa, są to głównie działania podejmowane przez architektów bezpieczeństwa oraz administratorów, którzy odpowiadają za projektowanie odpowiednich grup mających dostęp do dedykowanych informacji oraz nadzór prawidłowym przyznawaniem, odbieraniem oraz uzyskiwaniem wglądu do dokumentów, danych oraz informacji przez poszczególnych użytkowników systemów wewnętrznych.

Ekspert 2.

Jeśli omawiamy kwestie poufności informacji, istnieje szereg regulacji, które specyfikują wymagania do wdrożenia. Dotyczą one zarówno samych systemów dostępu, jak i określają kto ma / może mieć dostęp do tych informacji lub jakie zlecenia / aktywności mogą się pojawić w kontekście takich informacji/danych. Należy określić, w jaki sposób należy rejestrować pojawiające się zlecenia, jak przygotować dane, skąd je pobrać i jak je odpowiednio przekazać, a następnie zarejestrować, że takie działanie miało miejsce. W przypadku informacji poufnych, chronionych lub strategicznych, klasyfikacja informacji określa, kto ma dostęp do jakich danych. Osoby, którym nie przysługuje dostęp do tych informacji, nie mogą uzyskać odpowiednich uprawnień umożliwiających im np. przeglądanie tych danych. W przypadku awarii systemu konieczne są systemy monitorujące, które rejestrują, kto, w jaki sposób i kiedy korzystał z danych. Tego rodzaju dzienniki są wysyłane do innych systemów, do których administratorzy nie mają dostępu, aby w razie potrzeby zweryfikować działania administratorów w przypadku zleceń dotyczących aktualizacji systemu lub jego awarii. Wdrażane są również systemy śledzenia sesji, które nagrywają sesje w celu późniejszego odtworzenia historii aktywności w przypadku naruszenia lub niewłaściwego użycia danych. Systemy DLP są stosowane zarówno wewnętrznie, aby uniemożliwić przesyłanie strategicznych informacji do wszystkich w firmie, jak i na interfejsach zewnętrznych, aby np. uniemożliwić wysyłanie chronionych danych poza firmę (np. e-mailem). Przedsiębiorstwo musi również opracować jasną i precyzyjną politykę informacyjną, określającą cel przetwarzania informacji / danych, w tym regulującą zasady dostępu do informacji / danych. Następnie konieczne jest wdrożenie procesów określających, jak przydzielane są, odbierane i kontrolowane uprawnienia dostępu zgodnie z tą polityką. Oczywiście konieczne jest również zdefiniowanie wyjątków,

ponieważ awarie wymagają czasowego dostępu dla innych osób. Muszą być również monitorowane wszelkie potencjalne incydenty nieuprawnionego dostępu do danych, jak również nieuprawnionego przekazywania danych na zewnątrz lub importu danych do wewnątrz oraz prób ich przetwarzania w systemach, które pracują na danych wewnętrznych lub przetwarzają dane przychodzące z zewnątrz od partnerów biznesowych lub klientów. Zarówno polityka, jak i procesy i narzędzia muszą dbać o to, aby w ramach tych automatycznych procesów nie pojawiły się nieprawidłowości, takie jak manipulacja danymi lub zniszczenie struktury danych. Cykliczne weryfikacje należy przeprowadzać, na przykład raz w roku, aby sprawdzić przydzielanie uprawnień, tak aby w przypadku odejścia pracownika odpowiednie działania były podejmowane np. blokowanie dostępów do danych / informacji.

Ekspert 3.

Zarządzanie dostępem do poufnych informacji i danych w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych wymaga wdrożenia złożonych i wielowarstwowych środków bezpieczeństwa, co jest kluczowe dla ochrony przed nieautoryzowanym dostępem, nadużyciami oraz zapewnieniem integralności i poufności przetwarzanych danych. W efektywnym zarządzaniu dostępem kluczowa jest polityka minimalnych uprawnień, która zapewnia, że pracownicy mają dostęp tylko do tych zasobów i informacji, które są niezbędne do wykonywania ich zadań, minimalizując tym samym ryzyko nadużyć i nieautoryzowanego dostępu. Stosowanie solidnych metod uwierzytelniania, w tym wieloskładnikowego uwierzytelniania (MFA), które wymaga od użytkowników potwierdzenia swojej tożsamości przy użyciu co najmniej dwóch różnych metod, jest równie ważne. Implementacja zaawansowanych systemów zarządzania tożsamością i dostępem (IAM) umożliwia centralne zarządzanie tożsamościami użytkowników, politykami dostępu, rolami i uprawnieniami, co ułatwia nadawanie, zmianę i odbieranie uprawnień dostępu, a także monitorowanie i audytowanie dostępu do systemów. Szyfrowanie danych, zarówno przechowywanych, jak i przesyłanych, za pomocą silnych algorytmów szyfrowania, gwarantuje, że dane pozostaną nieczytelne dla nieautoryzowanych osób nawet w przypadku naruszenia. Segregacja sieci i zasobów, poprzez fizyczne lub wirtualne oddzielenie środowisk pracy, sieci i danych, ogranicza dostęp i potencjalny wpływ naruszeń bezpieczeństwa. Regularne przeglądy i audyty dostępu są niezbędne do identyfikacji i korygowania nieprawidłowości, takich jak nadmierne uprawnienia, konta nieaktywne lub nieautoryzowany dostęp, a także weryfikacji zgodności z przepisami prawnymi i politykami wewnętrznymi. Regularne szkolenia dla pracowników na temat bezpieczeństwa informacji i najlepszych praktyk w zakresie zarządzania dostępem zwiększają świadomość zagrożeń i pomagają zapobiegać nieintencjonalnym naruszeniom bezpieczeństwa. Zarządzanie dostępem do poufnych informacji i danych wymaga ciągłego zobowiązania do stosowania najlepszych praktyk, inwestycji w zaawansowane technologie i narzędzia oraz promowania kultury organizacyjnej, która kładzie nacisk na bezpieczeństwo informacji. Tylko poprzez kompleksowe podejście przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych może skutecznie chronić swoje zasoby przed rosnącymi zagrożeniami cybernetycznymi.

Ekspert 4.

Zarządzanie dostępem do poufnych informacji i danych w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych jest kluczowe dla zapewnienia bezpieczeństwa i ochrony przed

nieautoryzowanym dostępem. Na podstawie zdobytego doświadczenia, niezwykle ważne jest wprowadzenie polityki minimalnych uprawnień, która zapewnia pracownikom dostęp tylko do tych zasobów i danych, które są niezbędne do wykonania ich zadań. Takie podejście minimalizuje ryzyko nieautoryzowanego dostępu do wrażliwych danych. Implementacja silnych mechanizmów uwierzytelniania, takich jak uwierzytelnianie wieloskładnikowe, zapewnia, że dostęp do poufnych informacji mają tylko uprawnione osoby. Ważne jest także utrzymanie aktualnej bazy danych użytkowników i ich uprawnień oraz szybkie deaktywowanie kont osób, które już nie pracują w przedsiębiorstwie. Dobrze zdefiniowane zasady dostępu dla różnych systemów i aplikacji, z wykorzystaniem systemów zarządzania tożsamością i dostępem, umożliwiają centralizację procesów nadawania, monitorowania i cofania uprawnień. Użycie silnego szyfrowania chroni poufne dane przechowywane i przesyłane zarówno wewnątrz, jak i poza siecią przedsiębiorstwa, co jest kluczowe dla zapewnienia ich poufności i integralności. Implementacja narzędzi do monitorowania i rejestrowania prób dostępu do poufnych informacji oraz regularne przeglądy logów dostępu pomagają w wykrywaniu nieautoryzowanych lub podejrzanych działań. Przeprowadzanie regularnych audytów i przeglądów uprawnień dostępu pozwala na upewnienie się, że zasady dostępu są nadal adekwatne do roli i odpowiedzialności użytkownika oraz że nie ma nadmiernych lub nieuzasadnionych uprawnień. Organizowanie regularnych szkoleń dla pracowników podnosi ich świadomość znaczenia ochrony danych i dobrych praktyk bezpieczeństwa. Opracowanie i wdrożenie procedur reagowania na incydenty bezpieczeństwa określa kroki do podjęcia w przypadku naruszenia bezpieczeństwa danych, co pozwala na szybką reakcję, minimalizując szkody i przywracając normalne operacje. Zarządzanie dostępem jest ciągłym procesem, który musi być regularnie przeglądany i aktualizowany, aby odpowiadać na zmieniające się zagrożenia i potrzeby biznesowe. Wymaga to zintegrowanego podejścia i zaangażowania na wszystkich poziomach organizacji, od kierownictwa po zwykłych pracowników.

Ekspert 5.

Przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych powinno efektywnie zarządzać dostępem do poufnych informacji, stosując zintegrowane podejście, które obejmuje dokładne zidentyfikowanie i sklasyfikowanie poufnych informacji według ich wrażliwości, aby można było określić odpowiednie zabezpieczenia dla różnych typów danych. Kluczowe jest zapewnienie dostępu do danych jedynie tym pracownikom, którzy rzeczywiście potrzebują tych informacji do wykonania swoich zadań, co minimalizuje ryzyko nieautoryzowanego dostępu i potencjalnych wycieków. Ważne jest zastosowanie silnych metod uwierzytelniania, takich jak uwierzytelnianie wieloskładnikowe, które wymaga od użytkowników weryfikacji tożsamości za pomocą więcej niż jednej metody. Autoryzacja powinna być następnie przyznawana zgodnie z zasadami zdefiniowanymi dla różnych ról i uprawnień w organizacji. Implementacja silnych algorytmów szyfrowania chroni poufne informacje przechowywane i przesyłane w sieci przedsiębiorstwa, zapewniając, że dane są bezużyteczne dla nieautoryzowanych osób, nawet w przypadku ich przechwycenia. Ciągłe monitorowanie i rejestrowanie prób dostępu do poufnych danych umożliwia szybkie wykrywanie i reagowanie na podejrzane działania, a analiza logów dostępu może pomóc w identyfikacji wzorców naruszeń bezpieczeństwa. Regularne szkolenia z zakresu bezpieczeństwa informacji dla wszystkich pracowników są niezbędne, aby zwiększyć ich świadomość potencjalnych zagrożeń i nauczyć ich najlepszych praktyk ochrony danych. Pracownicy muszą być świadomi konsekwencji naruszeń

bezpieczeństwa oraz swojej roli w ochronie poufnych informacji. Ponadto, system zarządzania dostępem powinien być regularnie przeglądany i aktualizowany, aby uwzględniać nowe zagrożenia bezpieczeństwa, zmiany w strukturze organizacyjnej przedsiębiorstwa oraz ewolucję technologiczną. Taka strategia pozwoli skutecznie zarządzać dostępem do poufnych informacji, minimalizując ryzyko nieautoryzowanego dostępu i potencjalnych naruszeń bezpieczeństwa.

Ekspert 6.

Zarządzanie dostępem do poufnych informacji i danych w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych wymaga starannego podejścia, które opiera się na różnych kluczowych zasadach i praktykach, aby zapewnić ochronę tych zasobów oraz zgodność z obowiązującymi przepisami. Istotne jest, aby polityka dostępu do informacji była jasno określona, świadomie wdrożona i regularnie aktualizowana, określając kto, w jakich okolicznościach i w jaki sposób może uzyskać dostęp do danych, a także jak ten dostęp jest monitorowany i kontrolowany. Jeśli przedsiębiorstwo przetwarza informacje niejawne, kluczową rolę odgrywa funkcjonowanie kancelarii tajnej, która nadzoruje obieg i ochronę takich dokumentów, zapewniając, że dostęp do nich jest ściśle kontrolowany i ograniczony do osób uprawnionych. Zarządzanie dostępem do informacji na podstawie aktualnych certyfikatów bezpieczeństwa jest kluczowe, co oznacza, że tylko osoby z odpowiednimi poświadczeniami mogą uzyskać dostęp do określonych zasobów. Przestrzeganie przepisów dotyczących ochrony danych osobowych, jak ogólne rozporządzenie o ochronie danych (RODO) w Unii Europejskiej, wymaga implementacji odpowiednich środków technicznych i organizacyjnych mających na celu ochronę danych osobowych. Działania architektów bezpieczeństwa i administratorów są kluczowe dla zapewnienia, że dostęp do poufnych informacji jest odpowiednio projektowany i zarządzany, z wyraźnie określonymi rolami i odpowiedzialnościami oraz nadzorem nad procesem przyznawania, odbierania i monitorowania dostępu. Regularne przeglądy i audyty systemów informacyjnych, przeprowadzane przez wewnętrzne zespoły lub zewnętrzne organizacje audytorskie, pomagają w identyfikacji potencjalnych słabości i luk w zabezpieczeniach. Ponadto, szkolenia dotyczące bezpieczeństwa informacji dla wszystkich pracowników są niezbędne do podnoszenia świadomości na temat odpowiedzialnego postępowania z poufnymi danymi i zagrożeń związanych z ich przetwarzaniem. Implementacja tych zasad i praktyk umożliwia przedsiębiorstwu sektora technologii informacyjno-komunikacyjnych nie tylko ochronę swoich zasobów informacyjnych, ale również budowanie zaufania wśród klientów i partnerów biznesowych przez demonstrację odpowiedzialnego i profesjonalnego podejścia do zarządzania poufnymi informacjami.

Ekspert 7.

Omawiając kwestie poufności informacji, należy zwrócić uwagę na szereg regulacji określających wymagania dotyczące systemów dostępu oraz uprawnienia do korzystania z danych. Istotne jest ustalenie, jak rejestrowane są zlecenia, przygotowywanie i przekazywanie danych, a także jak odnotowywane są te działania. W przypadku informacji poufnych, systemy klasyfikacji określają, kto ma dostęp do poszczególnych danych. Osoby nieuprawnione nie powinny mieć możliwości dostępu do tych informacji. W sytuacji awarii systemu kluczowe są mechanizmy monitorujące, które rejestrują aktywność użytkowników, co pozwala na

weryfikację działań administratorów. Implementuje się także systemy śledzenia sesji, które zapisują aktywność użytkowników, aby można było odtworzyć historię w przypadku naruszeń. Systemy ochrony przed utratą danych (DLP) są używane zarówno wewnętrznie, by zapobiegać rozpowszechnianiu strategicznych informacji, jak i na interfejsach zewnętrznych, by ograniczać wysyłanie poufnych danych poza organizację. Firma musi opracować wyraźną politykę dotyczącą przetwarzania danych, w tym zasady dostępu i zarządzania nimi. Należy także wdrożyć procedury określające, jak przydzielane są uprawnienia dostępu i jak są one kontrolowane. Ważne jest zdefiniowanie procedur na wypadek awarii, które umożliwiają tymczasowy dostęp do danych, a także monitoring potencjalnych incydentów związanych z nieuprawnionym dostępem czy przekazywaniem informacji. Systemy muszą zapewniać, że procesy te są wolne od nieprawidłowości, takich jak manipulacja danymi. Regularne weryfikacje, np. roczne, są niezbędne do sprawdzenia czy uprawnienia są właściwie przydzielane i zarządzane, szczególnie po odejściu pracowników, aby odpowiednio zarządzać dostępem do informacji.

Ekspert 8.

Zarządzanie dostępem do poufnych informacji i danych w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych powinno opierać się na solidnych zasadach kontroli dostępu i ścisłych politykach bezpieczeństwa. Kluczowe jest stosowanie modelu minimalnych uprawnień (Least Privilege), który zapewnia, że pracownicy mają dostęp tylko do tych zasobów, które są niezbędne do wykonania ich zadań. Implementacja uwierzytelniania wieloskładnikowego (MFA) jest niezbędna do zabezpieczania dostępu do systemów i danych, szczególnie w obszarach, gdzie przetwarzane są informacje wrażliwe. Zarządzanie tożsamościami i dostępami (IAM) powinno być wspierane przez zaawansowane technologie, takie jak biometria czy inteligentne karty dostępu. Warto także rozważyć zastosowanie rozwiązań do zarządzania kluczami szyfrującymi oraz stosowanie szyfrowania danych w spoczynku i w transmisji, co zapewnia dodatkową warstwę ochrony. Regularne przeglądy i audyty dostępów oraz działań użytkowników są niezbędne do monitorowania i reagowania na wszelkie nieautoryzowane próby dostępu.

Ekspert 9.

Zarządzanie dostępem do poufnych informacji powinno być integralną częścią polityk bezpieczeństwa przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych. Obejmuje to zarówno fizyczne, jak i cyfrowe aspekty bezpieczeństwa. Wszystkie działania powinny być regulowane przez wyraźne procedury dotyczące weryfikacji tożsamości i autoryzacji pracowników oraz kontrahentów. Wprowadzenie regularnych szkoleń dotyczących ochrony danych osobowych i poufnych oraz promowanie świadomości bezpieczeństwa wśród pracowników może znacznie zmniejszyć ryzyko naruszeń danych. Istotne jest również stosowanie odpowiednich umów o poufności z pracownikami oraz zewnętrznymi dostawcami usług, które określają zasady i konsekwencje związane z dostępem do wrażliwych informacji. Monitorowanie i rewidowanie dostępów do poufnych obszarów, zarówno w formie fizycznej, jak i cyfrowej, powinno być przeprowadzane regularnie, aby upewnić się, że wszystkie środki bezpieczeństwa są aktualne i skuteczne.

Ekspert 10.

W kontekście zarządzania dostępem do poufnych informacji z perspektywy bezpieczeństwa fizycznego, kluczowe jest zabezpieczenie fizyczne miejsc, w których przechowywane są wrażliwe dane. Obejmuje to zastosowanie zaawansowanych systemów kontroli dostępu do budynków, pomieszczeń technicznych i serwerowni, które mogą wykorzystywać technologie identyfikacji, takie jak skanery biometryczne. Ważne jest również zabezpieczenie infrastruktury krytycznej przed nieautoryzowanym dostępem fizycznym poprzez stosowanie monitoringu wizyjnego, systemów alarmowych i ochrony fizycznej. Oprócz zabezpieczeń fizycznych, niezwykle istotne jest także tworzenie odpowiednich procedur w przypadku naruszenia zabezpieczeń, które umożliwią szybkie i skuteczne reagowanie na incydenty. Regularne przeglądy bezpieczeństwa fizycznego i aktualizacja protokołów są niezbędne, aby dostosować się do zmieniających się zagrożeń i nowych technologii zabezpieczeń.

Ekspert 11.

Przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych powinno zarządzać dostępem do poufnych informacji i danych poprzez wdrożenie zaawansowanych technologii i narzędzi do zarządzania dostępem, takich jak systemy IAM (Identity and Access Management). Systemy te pozwalają na kontrolowanie, kto i kiedy ma dostęp do danych, oraz zapewniają, że dostęp jest przyznawany tylko tym, którzy mają odpowiednie uprawnienia i potrzebę biznesową. Wdrożenie wielopoziomowego uwierzytelniania (MFA) dodatkowo zabezpiecza dostęp do wrażliwych informacji. Regularne audyty i przeglądy uprawnień są niezbędne, aby zapewnić, że uprawnienia użytkowników są zgodne z ich aktualnymi rolami i obowiązkami. Dane powinny być również szyfrowane zarówno w spoczynku, jak i w trakcie przesyłania, aby zabezpieczyć je przed nieautoryzowanym dostępem w przypadku przechwycenia.

Ekspert 12.

Zarządzanie dostępem do poufnych informacji i danych w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych powinno zaczynać się od precyzyjnie określonych polityk dostępu. Polityka ta powinna opierać się na zasadzie najmniejszych uprawnień (least privilege), co oznacza, że pracownicy mają dostęp tylko do tych danych, które są niezbędne do wykonywania ich obowiązków. Proces zarządzania dostępem powinien obejmować weryfikację i zatwierdzanie wniosków o dostęp przez odpowiednie osoby decyzyjne. Monitorowanie i rejestrowanie wszystkich prób dostępu do poufnych informacji jest kluczowe, aby móc wykrywać i reagować na podejrzane działania. W przypadku pracowników odchodzących z przedsiębiorstwa, ważne jest szybkie wycofanie ich uprawnień oraz przegląd wszelkich danych, które mogłyby zostać wyniesione. Regularne szkolenia z zakresu bezpieczeństwa informacji pomagają pracownikom zrozumieć znaczenie ochrony danych oraz konsekwencje ich nieautoryzowanego ujawnienia.

g)

Jakie narzędzia i technologie są najskuteczniejsze w zapobieganiu atakom na bezpieczeństwo informacji?

Ekspert 1.

Odnośnie kwestii bezpieczeństwa osobowego, głównym wysiłek skupia się na monitorowaniu procesów lojalnościowych pracowników. Możliwym do wykorzystania w tej sferze są branżowe portale społecznościowe, za których pomocą można nawiązywać pozorowane kontakty z pracownikiem i sprawdzić jego reakcję na intratną ofertę pracy. Monitorowanie informacji zwrotnej uzyskanej na podstawie tak przeprowadzonych działań może posłużyć do dalszej analizy sytuacji pracownika pod kątem jego lojalności. Kolejnym aspektem jest wdrożenie odpowiedniej polityki, która skutecznie budowałaby lojalność pracownika. Osoba, która jest zadowolona i utożsamia się ze swoim miejscem pracy będzie mniej skłonna do zdrady, kradzieży informacji przedsiębiorstwa czy korzystniejszej zmiany pracy. Specyfika polskiego rynku technologii informacyjno-komunikacyjnych warunkuje to, iż pracownik odchodzący z jednego przedsiębiorstwa często zabiera ze sobą pewien zasób informacyjny, który stanowić będzie wartość dodaną u nowego pracodawcy. W kwestii środków technicznych, główny wysiłek powinien zostać położony na zabezpieczenie stacji końcowej. Należy wykorzystać programy antywirusowe, proxy, DLP (Data Leak/Leakage/Loss Protection/Prevention), IDS/IPS (Intrusion Detection System, Intrusion Prevention System). Ponadto, na określonych stanowiskach funkcjonują specjalne zapisy umowne, które zakazują podejmowania pracy w konkurencyjnym przedsiębiorstwie.

Ekspert 2.

Należy dysponować różnorodnymi narzędziami w celu zapewnienia bezpieczeństwa systemów. Ataki mogą przybierać różne formy. Po pierwsze, konieczne jest zabezpieczenie wszelkich punktów styku zewnętrznego przed atakami typu DOS i DDOS. Takie ataki mogą prowadzić do różnorodnych skutków. Jeśli dany system zostanie skutecznie zaatakowany, a w tym samym czasie przetwarza określone informacje, może zaniechać ich przetwarzania lub zostać zainfekowany złośliwym oprogramowaniem. W takim przypadku konieczne jest przeprowadzenie odpowiednich czynności „czyszczących". Dlatego na wszystkich możliwych punktach styku należy zastosować ochronę anty-DDoS oraz ochronę przed botami. Obecnie ilość botów oraz ich skuteczność w udawaniu normalnych użytkowników lub procesów jest bardzo wysoka, dlatego jeśli nie zostaną wykryte i zablokowane aktywności złośliwych botów, może dojść do wycieku informacji przez dłuższy czas, co może prowadzić do naruszenia danych. Kolejnym krokiem jest zabezpieczenie systemów dostępowych, szczególnie tych, które mają dostęp z zewnątrz. W przypadku tych systemów, uwierzytelnienie dwuskładnikowe jest niezbędne. Jeśli uprawnienia zostaną przejęte, brak drugiego czynnika uwierzytelniania znacznie osłabia bezpieczeństwo. Ważne jest również zaimplementowanie systemu zapobiegania utracie danych (DLP), który umożliwia monitorowanie i blokowanie działań zgodnie z politykami zdefiniowanymi dla systemu. Czasami osoba może intencjonalnie próbować coś zrobić, a czasami po prostu się myli, dlatego istnieje potrzeba wsparcia w przypadku takich sytuacji. Ponadto, konieczna jest ochrona antymalware, która jest bardziej skuteczna niż tradycyjne oprogramowanie antywirusowe. Kolejnym aspektem jest ochrona w warstwach sieciowych, takich jak zapory ogniowe, które powinny działać na kilku poziomach. Dodatkowo, istnieją specjalne zapory ogniowe dla interfejsów informacyjno-komunikacyjnych, takich jak Diameter lub SS7, które są specyficzne dla branży sektora technologii informacyjno-komunikacyjnych i wymagają specjalnej ochrony. Te zapory powinny przepuszczać tylko ruch zgodny z zdefiniowanymi zasadami, blokując pozostały ruch. Konieczne jest również blokowanie możliwości nadmiernych uprawnień na stacjach roboczych

poprzez implementację rozwiązań takich jak PAM, gdzie uprzywilejowane uprawnienia są przechowywane, a użytkownicy pracują na swoich standardowych kontach, otrzymując dodatkowe uprawnienia tylko wtedy, gdy są potrzebne. Ważne jest także utrzymanie dobrych relacji z dostawcami usług, szczególnie jeśli dostawca oferuje również wsparcie. W przypadku awarii konieczne jest umożliwienie dostępu zewnętrznemu dostawcy do systemu na określonych uprawnieniach, a jednocześnie monitorowanie jego działań i ochrona przed potencjalnymi zagrożeniami. Monitorowanie trendów, takie jak ustalenie określonych wskaźników wydajności, pozwala na obserwowanie sytuacji i identyfikację nieprawidłowości. Jeśli na przykład system antymalware blokuje tylko 90% automatycznych ataków przychodzących, a reszta trafia do kwarantanny, a następnie zauważymy spadek tej liczby, może to wskazywać na pojawienie się nowych typów malware lub błędnej konfiguracji rozwiązania. Dlatego ważne jest, aby monitorować i regularnie sprawdzać działanie zaimplementowanych systemów zabezpieczeń. Automatyzacja działań za pomocą narzędzi takich jak SOAR ułatwia pracę personelu odpowiedzialnego za bezpieczeństwo, umożliwiając automatyczne wykonywanie pewnych czynności. Systemy powinny być tak skonfigurowane, aby blokowały działania, które są znane i zgodne z określonymi zasadami, z możliwością przejścia na ręczne działanie w przypadku potrzeby. Przykładem może być blokowanie stron hazardowych lub blokowanie domen na podstawie list ostrzeżeń NASK. Ręczne przeprowadzenie tych działań byłoby bardzo czasochłonne, dlatego należy wprowadzić automatyzację procesów bezpieczeństwa z możliwością ręcznej interwencji w razie potrzeby.

Ekspert 3.

Skuteczne zapobieganie atakom na bezpieczeństwo informacji wymaga zintegrowanego podejścia, które łączy zarówno narzędzia techniczne, jak i strategie organizacyjne. Przedsiębiorstwa, w tym te z branży sektora technologii informacyjno-komunikacyjnych, powinny wykorzystywać szeroki wachlarz narzędzi i technologii do ochrony swoich zasobów cyfrowych. Firewalle, czyli zapory sieciowe, są kluczowe do monitorowania i kontrolowania ruchu sieciowego, blokując nieautoryzowany dostęp i potencjalnie szkodliwe ruchy. Systemy wykrywania i zapobiegania intruzom (IDS/IPS) monitorują ruch sieciowy w celu wykrywania podejrzanych aktywności i działają prewencyjnie, blokując potencjalne ataki zanim dojdzie do naruszenia bezpieczeństwa. Szyfrowanie danych chroni dane w stanie spoczynku i w trakcie transmisji poprzez zastosowanie silnych algorytmów szyfrowania, zapewniając prywatność i bezpieczeństwo informacji. Wieloskładnikowe uwierzytelnianie (MFA) zwiększa bezpieczeństwo, wymagając od użytkowników weryfikacji tożsamości za pomocą co najmniej dwóch niezależnych form uwierzytelnienia. Regularne skanowanie systemów w poszukiwaniu luk w zabezpieczeniach oraz automatyczne stosowanie aktualizacji i łatek zabezpieczeń zapewniają ochronę przed znanymi zagrożeniami i exploitami. Sandboxing i wirtualizacja izolują aplikacje i procesy w bezpiecznym, kontrolowanym środowisku, co może zapobiegać rozprzestrzenianiu się złośliwego oprogramowania i umożliwia analizę podejrzanych plików bez ryzyka dla głównego systemu. Zarządzanie dostępem i tożsamością (IAM) umożliwia precyzyjne zarządzanie uprawnieniami użytkowników i kontrolę dostępu do zasobów. Antywirusy i oprogramowanie antymalware są niezbędne do wykrywania, izolowania i usuwania złośliwego oprogramowania, a nowoczesne rozwiązania wykorzystują zaawansowane techniki, takie jak uczenie maszynowe, do identyfikowania nowych zagrożeń. Wykorzystanie sztucznej inteligencji i uczenia maszynowego do analizy wzorców zachowań

użytkowników i ruchu w sieci może pomóc w wykrywaniu anomalii sugerujących potencjalne ataki lub naruszenia bezpieczeństwa. Szkolenia z cyberbezpieczeństwa i podnoszenie świadomości są kluczowe dla zapobiegania atakom socjotechnicznym, takim jak phishing, chociaż nie są to narzędzia techniczne. Ostatecznie, skuteczna obrona przed atakami na bezpieczeństwo informacji wymaga nie tylko zintegrowanego podejścia łączącego różne narzędzia i technologie, ale także elastyczności i gotowości na adaptację do ewoluującego krajobrazu zagrożeń cybernetycznych.

Ekspert 4.

Zapobieganie atakom na bezpieczeństwo informacji w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych wymaga zastosowania wielowarstwowych środków obronnych, które obejmują różnorodne narzędzia i technologie. Do najskuteczniejszych metod należy stosowanie firewalli, które kontrolują ruch sieciowy wchodzący i wychodzący z organizacji i mogą blokować niebezpieczny ruch. Systemy wykrywania i zapobiegania włamaniom monitorują sieć w poszukiwaniu podejrzanych wzorców i mogą aktywnie blokować ataki w czasie rzeczywistym. Szyfrowanie danych zarówno w spoczynku, jak i w transmisji zapewnia, że dane będą nieczytelne bez odpowiedniego klucza, nawet jeśli zostaną przechwycone. Wieloskładnikowe uwierzytelnianie znacząco utrudnia nieautoryzowany dostęp, wymagając od użytkowników potwierdzenia tożsamości przez co najmniej dwie niezależne metody. Ponadto, regularne zarządzanie łatami i aktualizacjami oprogramowania minimalizuje ryzyko wykorzystania znanych podatności. Oprogramowanie antywirusowe i antymalware skutecznie wykrywa, izoluje i usuwa złośliwe oprogramowanie. Technika sandboxing pozwala uruchamiać podejrzane aplikacje lub pliki w izolowanym środowisku, minimalizując ryzyko zainfekowania reszty systemu. Systemy zarządzania dostępem i tożsamością kontrolują dostęp do zasobów, zapewniając, że tylko uprawnione osoby mają dostęp do poufnych informacji. Zastosowanie zaawansowanych technologii, takich jak uczenie maszynowe i sztuczna inteligencja do monitorowania i analizy zachowań użytkowników, pozwala na wykrywanie niezwykłych aktywności, które mogą wskazywać na atak. Regularne szkolenia z zakresu bezpieczeństwa informacji dla pracowników pomagają również zapobiegać atakom wynikającym z błędów ludzkich lub niedbałości. Implementacja tych narzędzi i technologii, w połączeniu z ciągłym monitorowaniem, przeglądem i doskonaleniem strategii bezpieczeństwa, jest kluczowa dla ochrony przedsiębiorstw sektora technologii informacyjno-komunikacyjnych przed różnorodnymi zagrożeniami cyfrowymi.

Ekspert 5.

Wśród najbardziej efektywnych narzędzi i technologii stosowanych do zapobiegania atakom na bezpieczeństwo informacji znajdują się systemy wykrywania i zapobiegania włamaniom, które monitorują ruch sieciowy w poszukiwaniu podejrzanych wzorców mogących świadczyć o próbach ataku i są zdolne do automatycznego blokowania takich działań. Zapory ogniowe ochraniają sieć przed nieautoryzowanym dostępem poprzez kontrolę ruchu przychodzącego i wychodzącego zgodnie z określonymi zasadami. Oprogramowanie antywirusowe i antymalware chroni przed szkodliwym oprogramowaniem przez skanowanie systemów i aplikacji w celu wykrycia i usunięcia złośliwego kodu. Narzędzia do zarządzania tożsamością i dostępem umożliwiają kontrolę dostępu do zasobów organizacji, często poprzez uwierzytelnianie wieloskładnikowe i zarządzanie uprawnieniami. Szyfrowanie danych

zapewnia ochronę ich poufności, uniemożliwiając odczytanie danych przez nieuprawnione osoby, nawet jeśli uzyskają one dostęp do tych danych. Zaawansowane narzędzia analityczne, wykorzystujące uczenie maszynowe i sztuczną inteligencję, identyfikują nietypowe wzorce zachowań, które mogą wskazywać na próbę naruszenia bezpieczeństwa. Rozwiązania typu Zero Trust zakładają brak zaufania do żadnego użytkownika czy urządzenia bez weryfikacji, co zwiększa bezpieczeństwo przez minimalizowanie ryzyka nieautoryzowanego dostępu. Zarządzanie łatami i aktualizacjami oprogramowania jest kluczowe dla utrzymania ochrony przed znanymi lukami w zabezpieczeniach. Wykorzystanie tych narzędzi i technologii, połączone z najlepszymi praktykami, takimi jak ciągłe szkolenia pracowników i audyty bezpieczeństwa, jest niezbędne dla skutecznej ochrony przed atakami na bezpieczeństwo informacji.

Ekspert 6.

W kontekście zapobiegania atakom na bezpieczeństwo informacji kluczowe jest połączenie odpowiednich narzędzi i technologii z efektywnymi strategiami zarządzania personelem i politykami bezpieczeństwa. W odpowiedzi na pytanie o najskuteczniejsze narzędzia i technologie można zauważyć, że zarządzanie lojalnością pracowników, obejmujące monitorowanie i analizę ich zachowań oraz budowanie lojalności poprzez uczciwe wynagradzanie, możliwości rozwoju kariery i transparentność działań organizacji, jest fundamentem w minimalizowaniu ryzyka wycieków informacji. Kolejnym istotnym elementem jest zabezpieczenie stacji końcowej, w tym programy antywirusowe, antymalware, systemy zapobiegania wyciekom danych (DLP) oraz systemy wykrywania i zapobiegania intruzjom (IDS/IPS), które są kluczowe w ochronie przed złośliwym oprogramowaniem i atakami zewnętrznymi. W obszarze kontroli dostępu i zarządzania tożsamościami, implementacja wielopoziomowego uwierzytelniania, zarządzanie tożsamościami i kontrola dostępu do zasobów IT oraz użycie silnego szyfrowania są niezbędne do ochrony wrażliwych danych i ograniczania dostępu tylko do autoryzowanych osób. Dodatkowo, korporacyjne polityki i procedury, takie jak umowy z klauzulami poufności, które zabraniają podejmowania pracy u konkurencji lub rozpowszechniania wiedzy nabytej w firmie, są istotne w zmniejszaniu ryzyka przenoszenia wiedzy do konkurentów. Podsumowując, skuteczna ochrona przed atakami na bezpieczeństwo informacji wymaga zastosowania zaawansowanych technologii oraz przemyślanych strategii zarządzania zasobami ludzkimi i rygorystycznych polityk korporacyjnych, co jest kluczowe dla stworzenia zintegrowanego systemu bezpieczeństwa, który skutecznie chroni przed zagrożeniami zewnętrznymi i wewnętrznymi.

Ekspert 7.

W zapewnianiu bezpieczeństwa systemów kluczowe jest dysponowanie różnorodnymi narzędziami, aby skutecznie odpowiadać na różne formy ataków, takie jak ataki typu DOS i D-DOS, które mogą poważnie zaszkodzić infrastrukturze i przetwarzanym informacjom. Należy chronić wszystkie punkty styku zewnętrznego, stosując ochronę anty-DDoS oraz ochronę przed botami, które mogą imitować normalne działania użytkowników i niezauważone prowadzić do naruszenia danych. Ważne jest zabezpieczenie systemów dostępowych, zwłaszcza tych z dostępem z zewnątrz, przez wdrożenie uwierzytelnienia dwuskładnikowego, które znacząco zwiększa bezpieczeństwo. Implementacja systemów zapobiegania utracie danych (DLP) pozwala na monitorowanie i kontrolowanie działań zgodnie z ustalonymi politykami, chroniąc

przed nieautoryzowanym przesyłaniem wrażliwych informacji. Konieczna jest także ochrona antymalware, zapewniająca lepszą ochronę niż standardowe oprogramowanie antywirusowe. Bezpieczeństwo sieciowe powinno być wzmacniane przez zastosowanie wielopoziomowych zapór ogniowych, w tym specjalistycznych dla branży sektora technologii informacyjno-komunikacyjnych, które regulują ruch sieciowy i blokują niezgodne działania. Ważne jest także zarządzanie uprawnieniami użytkowników za pomocą systemów typu PAM, które ograniczają nadmierne uprawnienia i pozwalają na kontrolowane przydzielanie dostępu, gdy jest to niezbędne. Utrzymanie dobrych relacji z dostawcami usług, którzy mogą wspierać w zarządzaniu awariami, jest istotne dla szybkiego reagowania na incydenty. Regularne monitorowanie i analiza wydajności systemów bezpieczeństwa pozwalają na wczesne wykrywanie potencjalnych słabości i adaptację do nowych zagrożeń. Automatyzacja bezpieczeństwa, przy użyciu narzędzi takich jak SOAR, wspomaga personel odpowiedzialny za bezpieczeństwo poprzez automatyzację rutynowych zadań i umożliwienie skupienia się na bardziej złożonych problemach, co znacząco poprawia efektywność procesów ochrony danych.

Ekspert 8.

W dziedzinie bezpieczeństwa informatycznego istnieje wiele narzędzi i technologii, które mogą skutecznie zapobiegać atakom na bezpieczeństwo informacji. Kluczowymi technologiami są firewalle, które służą do filtrowania ruchu sieciowego i blokowania nieautoryzowanych prób dostępu. Równie ważne są systemy wykrywania i zapobiegania intruzom (IDS/IPS), które monitorują sieć w poszukiwaniu podejrzanych aktywności i mogą automatycznie reagować na wykryte zagrożenia. Bardzo skuteczne są również narzędzia do skanowania podatności, które pomagają identyfikować i eliminować luki w zabezpieczeniach przed atakami. Szyfrowanie danych, zarówno przechowywanych (Data at Rest), jak i przesyłanych (Data in Transit), jest niezbędne do ochrony poufności informacji. Uwierzytelnianie wieloskładnikowe (MFA) znacząco zwiększa bezpieczeństwo poprzez wymaganie dodatkowego potwierdzenia tożsamości użytkownika. Oprogramowanie antywirusowe i antymalware, regularnie aktualizowane, także odgrywa kluczową rolę w ochronie przed złośliwym oprogramowaniem.

Ekspert 9.

W kontekście bezpieczeństwa osobowego, skuteczne narzędzia i technologie muszą obejmować zarówno fizyczne, jak i cyfrowe aspekty ochrony. Systemy zarządzania tożsamością i dostępem (IAM) są kluczowe dla zarządzania uprawnieniami użytkowników i monitorowania ich działalności. Edukacja i świadomość bezpieczeństwa wśród pracowników są niezbędne i mogą być wspierane przez platformy e-learningowe, które oferują szkolenia z cyberbezpieczeństwa. Ponadto, technologie biometryczne, takie jak skanery odcisków palców czy rozpoznawanie twarzy, mogą zwiększyć bezpieczeństwo poprzez bardziej skuteczną weryfikację tożsamości przy dostępie do wrażliwych obszarów. Monitoring wizyjny i inne systemy kontroli dostępu fizycznego również odgrywają ważną rolę w zapobieganiu nieautoryzowanemu dostępowi.

Ekspert 10.

W aspekcie bezpieczeństwa fizycznego, najskuteczniejsze są technologie kontroli dostępu, które ograniczają fizyczny dostęp do krytycznej infrastruktury. Systemy kontroli dostępu oparte na kartach dostępu, kodach PIN, a także rozwiązania biometryczne, są niezbędne do ochrony przed nieautoryzowanym dostępem. Monitoring CCTV, alarmy antywłamaniowe i systemy

detekcji ruchu znacznie zwiększają zdolność do wczesnego wykrywania i reagowania na próby naruszenia bezpieczeństwa. Dodatkowo, technologie zarządzania kluczami i sejfami danych pomagają w bezpiecznym przechowywaniu fizycznych nośników informacji, takich jak dyski twarde i dokumenty. W odpowiedzi na zagrożenia naturalne i katastrofy, niezbędne jest również wdrożenie zaawansowanych systemów przeciwpożarowych i planów awaryjnych, które zapewniają ochronę i możliwość szybkiej reakcji w sytuacji kryzysowej.

Ekspert 11.

Najskuteczniejsze narzędzia i technologie w zapobieganiu atakom na bezpieczeństwo informacji to przede wszystkim zaawansowane systemy do zarządzania tożsamościami i dostępem (IAM), które kontrolują, kto ma dostęp do jakich zasobów i kiedy. Ważnym elementem są również rozwiązania klasy SIEM (Security Information and Event Management), które zbierają i analizują logi z różnych źródeł w czasie rzeczywistym, umożliwiając szybkie wykrywanie i reagowanie na incydenty. Wprowadzenie wielopoziomowego uwierzytelniania (MFA) znacznie utrudnia nieautoryzowany dostęp, nawet w przypadku skompromitowania haseł. Technologie szyfrowania danych, zarówno w spoczynku, jak i w trakcie przesyłania, chronią poufne informacje przed przechwyceniem przez osoby nieuprawnione. Narzędzia do monitorowania sieci, takie jak systemy IDS/IPS (Intrusion Detection/Prevention Systems), są kluczowe w wykrywaniu i zapobieganiu nieautoryzowanemu dostępowi i atakom sieciowym. Wreszcie, regularne audyty bezpieczeństwa i testy penetracyjne pomagają identyfikować i naprawiać luki w zabezpieczeniach.

Ekspert 12.

Najskuteczniejsze narzędzia i technologie w zapobieganiu atakom na bezpieczeństwo informacji obejmują różne systemy monitorowania i analizy aktywności pracowników oraz wykrywania anomalii. Programy antywirusowe i antymalware są podstawą ochrony stacji końcowych przed szkodliwym oprogramowaniem. Systemy DLP (Data Loss Prevention) pomagają monitorować i kontrolować przepływ informacji, aby zapobiegać ich nieautoryzowanemu wyciekom. Ważne są również narzędzia do zarządzania i monitorowania aktywności pracowników na różnych platformach, w tym proxy serwery, które kontrolują dostęp do Internetu i blokują podejrzane strony. Systemy wykrywania i zapobiegania intruzjom (IDS/IPS) umożliwiają szybkie reagowanie na nietypowe działania w sieci. Dodatkowo, szkolenia z zakresu bezpieczeństwa dla pracowników oraz symulowane ataki phishingowe pomagają zwiększyć świadomość zagrożeń i przygotować personel na rzeczywiste incydenty. Kombinacja tych narzędzi i technologii zapewnia kompleksową ochronę przed różnorodnymi zagrożeniami dla bezpieczeństwa informacji.

W jaki sposób przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych może skutecznie monitorować i wykrywać potencjalne przypadki szpiegostwa korporacyjnego, zarówno we własnej organizacji, jak i ze strony podmiotów zewnętrznych?

Ekspert 1.

W kwestii zabezpieczeń korporacyjnych, pierwszą linią weryfikacji sytuacji wewnętrznej w przedsiębiorstwie powinien być dział kadr, który powinien nie tylko odpowiadać za sprawdzenie pracownika pod kątem bezpieczeństwa w ramach rekrutacji, ale również monitorować jego zachowania w ramach dalszego rozwoju w przedsiębiorstwie. Powinny funkcjonować również odpowiednie procedury, mające na celu informowanie osoby decyzyjne o niepożądanym zachowaniu pracownika lub pracowników mogących świadczyć o chęci zmiany pracy. Czynnikami, które mogą również zostać wykorzystane w celu poprawy sytuacji pracowniczej, to wymiana kadry zarządzającej, wprowadzenie jasnych procesów motywacyjnych, wdrożenie klarownej polityki rozwoju pracownika. Ponadto, również należałoby się posiłkować przytoczonymi wcześniej działaniami pozorowanymi, mającymi na celu sprawdzenie lojalności i wiarygodności pracowników. Działania te powinny być oczywiście prowadzone z poszanowaniem obowiązujących przepisów kodeksu pracy. Kadra zarządzająca powinna również zwracać uwagę na nagłą zmianę zachowania oraz sytuacji materialnej pracowników, co może świadczyć o pojawieniu się w ich życiu sytuacji problematycznych mogących mieć wpływ na bezpieczeństwo informacji przedsiębiorstwa. Nie należy wykluczyć, iż w takich przypadkach dany pracownik jest szantażowany, ma problemy finansowe związane z hazardem, zadłużeniem lub chorobą najbliższej osoby. Zatem umiejętność obserwacji przełożonych w tym zakresie jest również kluczowym elementem przeciwdziałania szpiegostwu korporacyjnemu. Odnośnie kwestii personalnych, duży nacisk kładziony jest na kwestie psychologiczne – odpowiednie szkolenia z zakresu umiejętnego radzenia sobie ze stresem, priorytetyzacji czynności wykonywanych podczas czasu pracy czy asertywności. Przedsiębiorstwo kładzie duży nacisk na odpowiednie przygotowanie pracowników do wykonywania swoich obowiązków w trudnym i stresującym środowisku informacyjno-komunikacyjnym. W kwestii zabezpieczeń technicznych, sytuacja jest analogiczna jak w przypadku zapewnienia bezpieczeństwa cybernetycznego. Wykorzystuje się w tym przypadku testowanie funkcjonujących zabezpieczeń fizycznych oraz sieciowych. Dokonuje się audytu procedur i środków technicznych pod kątem możliwego miejsca wycieku lub kradzieży informacji gromadzonych przez przedsiębiorstwo.

Ekspert 2.

W przypadku tej tematyki nie ma jednego jednoznacznego rozwiązania. Jeśli chodzi o wewnętrzne zagrożenia, istotne jest analizowanie, kto ma dostęp do jakich informacji oraz w jaki sposób korzysta z tych uprawnień. Nagłe zmiany w zachowaniu użytkownika, na przykład otwieranie większej liczby plików, kopiowanie ich na zewnętrzne nośniki lub na prywatne konta, mogą stanowić sygnał, że dzieje się coś niepokojącego. Nie zawsze oznacza to szpiegostwo, ale może wskazywać na nieuczciwe działania pracownika przygotowującego się do odejścia z przedsiębiorstwa. Intencje mogą być różne i trudne do ustalenia w takich sytuacjach. Ważne jest monitorowanie wszelkich dostępów do informacji oraz wyszukiwanie odchyleń w tych dostępach. Jeśli w danym momencie pracownik nagle uzyskuje nadmierne uprawnienia, należy sprawdzić, czy jest to związane z nowym projektem, do którego został przydzielony, czy może jest to niezgodne z jego dotychczasowymi obowiązkami. W przypadku zewnętrznego szpiegostwa istnieją organizacje konkurencyjne, które próbują przekupić pracowników, oferując im korzyści. Jeśli pracownik zaakceptuje taką ofertę, firma może nie być w stanie zatrzymać go. Istnieją również bardziej wysublimowane metody, takie jak stworzenie fałszywych profili na platformach społecznościowych, na przykład na LinkedInie. Takie profile

są dobrze przygotowane i zapraszają określone osoby do dyskusji na tematy związane z ich specjalizacją, aby pozyskać wiedzę. Inna forma to fałszywe rekrutacje na fikcyjne stanowiska. Przedsiębiorstwa wynajmują profesjonalistów, którzy przeprowadzają wywiady z potencjalnymi kandydatami, w celu zdobycia określonych informacji. W tym przypadku firma zewnętrzna, która nie prowadzi rzeczywistej rekrutacji, interesuje się tylko pozyskaniem informacji od osób zainteresowanych takim stanowiskiem. Inny sposób to włamania przy użyciu skradzionych danych uwierzytelniających. Istnieją organizacje specjalizujące się w tego typu działaniach, które wykradają informacje i następnie mogą szantażować właścicieli tych danych lub przekazywać informacje osobom zainteresowanym. Jeśli chodzi o skuteczne monitorowanie i wykrywanie takich działań, istotne jest edukowanie pracowników na temat możliwości wystąpienia takich sytuacji. Jeśli pracownicy nie są świadomi, że mogą zostać pytani o informacje w grupach eksperckich lub podczas rekrutacji, które wykraczają poza ich wiedzę, mogą nie zdawać sobie sprawy, że uczestniczą w ujawnianiu poufnych informacji i mogą ponieść odpowiedzialność prawną. Dlatego ważne jest, aby takie informacje były przekazywane na szkoleniach, podczas rekrutacji, szkoleń związanych z RODO, cyberbezpieczeństwem, a także przy omawianiu incydentów i wyciąganiu z nich wniosków. Przedsiębiorca, który takich działań nie podejmuje, traci możliwość zapobieżenia incydentom, ponieważ nie wszyscy pracownicy będą w stanie zauważyć, co się tak naprawdę dzieje, jeśli nie zostaną poinformowani o możliwych zagrożeniach.

Ekspert 3.

Skuteczne monitorowanie i wykrywanie potencjalnych przypadków szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych wymaga kompleksowego podejścia, które łączy zaawansowane technologie, procedury operacyjne oraz kulturę organizacyjną opartą na świadomości bezpieczeństwa. Istotne jest implementowanie zaawansowanych systemów IDS (Intrusion Detection Systems) i SIEM (Security Information and Event Management), które analizują ruch sieciowy i aktywność systemów w poszukiwaniu niezwykłych wzorców mogących wskazywać na próby szpiegostwa, przetwarzając duże ilości danych w czasie rzeczywistym, aby identyfikować podejrzane zachowania i potencjalne zagrożenia. Wykorzystanie systemów UBA (User Behavior Analytics) do monitorowania i analizy zachowań użytkowników pomaga w wykrywaniu anomalii, takich jak nieautoryzowany dostęp do poufnych danych czy niezwykła aktywność poza standardowymi godzinami pracy, podczas gdy systemy zarządzania tożsamością i dostępem (IAM) pomagają ograniczyć dostęp do krytycznych zasobów tylko do uprawnionych użytkowników. Zastosowanie silnych metod szyfrowania chroni dane przechowywane i przesyłane, zapewniając, że informacje pozostaną nieczytelne i bezużyteczne dla nieautoryzowanych osób, nawet jeśli dane zostaną przechwycone. Wzmocnienie fizycznych środków bezpieczeństwa, w tym systemy kontroli dostępu i monitoring wideo, jest kluczowe dla ochrony krytycznej infrastruktury i danych. Regularne szkolenia z zakresu bezpieczeństwa informacji zwiększają świadomość pracowników na temat potencjalnych zagrożeń i uczą ich, jak postępować w przypadku wykrycia podejrzanych działań, budując kulturę bezpieczeństwa wśród personelu. Ponadto, regularne oceny ryzyka i audyty bezpieczeństwa są niezbędne do identyfikacji słabych punktów w infrastrukturze i procesach, umożliwiając ciągłe doskonalenie środków bezpieczeństwa. W przypadku wykrycia prób szpiegostwa, szybka reakcja i współpraca z lokalnymi organami ścigania oraz branżowymi grupami ds. bezpieczeństwa może pomóc w

identyfikacji sprawców i zapobieganiu dalszym próbom ataków. Wdrożenie polityk dotyczących korzystania z urządzeń mobilnych i pracy zdalnej, w tym zasad bezpiecznego połączenia z siecią firmową, jest niezwykle ważne w kontekście wzrostu pracy zdalnej i mobilności pracowników. Przyjęcie tych strategii wymaga zaangażowania na wszystkich poziomach organizacji i stanowi nieustanny proces dostosowywania się do ewoluujących zagrożeń w dziedzinie bezpieczeństwa informacji.

Ekspert 4.

Skuteczne monitorowanie i wykrywanie potencjalnych przypadków szpiegostwa korporacyjnego wymaga holistycznego podejścia, łączącego narzędzia technologiczne, procedury operacyjne i strategie organizacyjne. Wdrażanie ścisłych procedur zarządzania dostępem jest kluczowe, aby zapewnić, że tylko upoważnione osoby mają dostęp do poufnych informacji, z wykorzystaniem wieloskładnikowego uwierzytelniania i zarządzania tożsamościami. Zaawansowane narzędzia analityczne, takie jak analiza zachowań użytkowników i urządzeń, pomagają wykrywać anomalie mogące wskazywać na nieautoryzowane działania. Szyfrowanie danych zarówno w spoczynku, jak i w trakcie transmisji jest niezbędne do minimalizowania ryzyka wycieku informacji. Segmentacja sieci pozwala na izolację poufnych danych i zasobów, ograniczając ryzyko ich skompromitowania. Systemy wykrywania i zapobiegania włamaniom monitorują ruch sieciowy i automatycznie reagują na zagrożenia. Zarządzanie dziennikami i ich analiza w czasie rzeczywistym są istotne dla identyfikacji nieautoryzowanych prób dostępu i innych podejrzanych działań. Regularna ocena podatności i zarządzanie łatkami zapewniają adresowanie znanych luk w zabezpieczeniach. Programy świadomości bezpieczeństwa uczą pracowników rozpoznawania potencjalnych zagrożeń i działań mogących ułatwić szpiegostwo korporacyjne. Współpraca z organami ścigania i branżowymi grupami ds. bezpieczeństwa umożliwia wymianę informacji o zagrożeniach i najlepszych praktykach, a także szybkie reagowanie na incydenty. Regularne audyty bezpieczeństwa i testy penetracyjne przeprowadzane przez zewnętrzne organizacje mogą ujawnić słabe punkty, które mogłyby zostać wykorzystane przez szpiegów korporacyjnych. Implementacja tych strategii pozwala przedsiębiorstwom sektora technologii informacyjno-komunikacyjnych znacząco zmniejszyć ryzyko szpiegostwa korporacyjnego, zwiększając ich odporność na ataki wewnętrzne i zewnętrzne.

Ekspert 5.

Skuteczne monitorowanie i wykrywanie potencjalnych przypadków szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych wymaga zintegrowanego podejścia, łączącego techniczne i organizacyjne aspekty bezpieczeństwa. Wprowadzenie zaawansowanych systemów wykrywania i zapobiegania intruzom, które monitorują ruch sieciowy w poszukiwaniu podejrzanych działań, jest kluczowe. Te systemy powinny być regularnie aktualizowane o nowe sygnatury zagrożeń. Dodatkowo, wykorzystanie narzędzi do analizy zachowań użytkowników pozwala na wykrywanie nieoczekiwanych zmian w aktywnościach, co może sugerować szpiegostwo. Ścisłe zarządzanie uprawnieniami dostępu poprzez zasady najmniejszych uprawnień i wieloskładnikowe uwierzytelnianie ograniczają ryzyko nieautoryzowanego dostępu. Rozwiązania chroniące przed utratą danych umożliwiają kontrolę nad przepływem informacji wewnątrz przedsiębiorstwa i na zewnątrz, zapobiegając ich nieautoryzowanemu udostępnianiu.

Regularne audyty bezpieczeństwa, przeglądy konfiguracji systemów informatycznych i ciągłe monitorowanie zdarzeń bezpieczeństwa pozwalają na szybkie wykrywanie i reagowanie na zagrożenia. Organizowanie regularnych szkoleń z zakresu bezpieczeństwa informacji zwiększa świadomość pracowników o zagrożeniach cyberbezpieczeństwa i najlepszych praktykach obronnych. Ponadto, utrzymanie bliskiej współpracy z lokalnymi i międzynarodowymi organami ścigania oraz innymi agencjami rządowymi ułatwia wymianę informacji o zagrożeniach i współpracę w zakresie obrony. Implementacja tych strategii umożliwia przedsiębiorstwom sektora technologii informacyjno-komunikacyjnych efektywną ochronę przed szpiegostwem korporacyjnym, chroniąc ich zasoby informacyjne i infrastrukturę krytyczną.

Ekspert 6.

Przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych może efektywnie monitorować i wykrywać potencjalne przypadki szpiegostwa korporacyjnego, stosując kombinację różnorodnych podejść, które łączą aspekty personalne i techniczne. Kluczowe metody obejmują dokładną weryfikację kandydatów podczas rekrutacji, sprawdzając ich przeszłość zawodową i osobistą, w tym referencje i historię zatrudnienia, a także potencjalną przeszłość kryminalną. Regularne obserwowanie zachowań pracowników, szczególnie tych z dostępem do wrażliwych danych, pomaga wykryć zmiany mogące sygnalizować potencjalne ryzyko, takie jak nagła zmiana sytuacji materialnej czy lojalności. Wsparcie szkoleniowe w zakresie bezpieczeństwa informacji i motywowanie pracowników poprzez jasno określone ścieżki kariery oraz odpowiednie motywatory może także zwiększyć ich lojalność i zadowolenie, co zmniejsza ryzyko szpiegostwa. Dodatkowo, pozorowane działania, takie jak testy lojalności, mogą ujawnić skłonności pracowników do dzielenia się poufnymi informacjami. Na poziomie technicznym, systemy Data Loss Prevention (DLP), regularne audyty bezpieczeństwa oraz środki zabezpieczenia fizycznego, jak kontrola dostępu i monitoring wizyjny, pomagają kontrolować przepływ informacji i zapobiegać nieautoryzowanemu dostępowi. Dodatkowo, szkolenia z zarządzania stresem i asertywności mogą przygotować pracowników do lepszego radzenia sobie w sytuacjach stresujących, czyniąc ich mniej podatnymi na wpływy zewnętrzne mogące prowadzić do nieetycznych zachowań. Integracja tych metod i ich konsekwentne stosowanie jako część szeroko zakrojonej strategii bezpieczeństwa korporacyjnego jest kluczem do skuteczności, przy jednoczesnym zachowaniu poszanowania przepisów prawnych, kodeksu pracy i ochrony prywatności, co gwarantuje, że działania monitorujące i wykrywające nie naruszają praw pracowników.

Ekspert 7.

W kwestii bezpieczeństwa informacji, nie istnieje uniwersalne rozwiązanie, a różnorodne wyzwania wymagają indywidualnego podejścia. Istotne jest monitorowanie, kto ma dostęp do konkretnych danych i w jaki sposób z tego dostępu korzysta. Nagłe zmiany w zachowaniu użytkowników, takie jak masowe otwieranie plików lub ich kopiowanie na zewnętrzne nośniki, mogą sygnalizować potencjalne ryzyko, niekoniecznie związane z szpiegostwem, ale możliwe nieuczciwe zamiary, na przykład przygotowania do odejścia z organizacji. Warto zatem bacznie obserwować wszelkie odchylenia od normalnych wzorców działania, które mogą wskazywać na nadużycia uprawnień, szczególnie gdy są one związane z nowymi projektami czy zmianami w zakresie obowiązków pracownika. Zagrożenia zewnętrzne również stanowią poważne ryzyko,

włączając w to próby przekupstwa pracowników przez konkurencyjne organizacje. Metody takie jak tworzenie fałszywych profili na platformach społecznościowych czy fikcyjne oferty pracy są używane do pozyskiwania cennych informacji. Takie działania mogą prowadzić do uzyskania dostępu do wrażliwych danych poprzez wykorzystanie skradzionych poświadczeń logowania. Aby skutecznie przeciwdziałać tym zagrożeniom, kluczowe jest szeroko zakrojone szkolenie pracowników, które powinno uwzględniać aspekty związane z ochroną danych, cyberbezpieczeństwem oraz procedurami odpowiedzi na incydenty. Edukacja powinna obejmować informowanie pracowników o ryzykach związanych z udziałem w nieformalnych grupach dyskusyjnych czy podczas rekrutacji, gdzie mogą nieświadomie ujawnić wrażliwe informacje. Prowadzenie regularnych szkoleń, omawianie realnych incydentów oraz konsekwentne informowanie o potencjalnych zagrożeniach to klucz do skutecznej ochrony przedsiębiorstwa przed wewnętrznymi i zewnętrznymi zagrożeniami.

Ekspert 8.

Skuteczne monitorowanie i wykrywanie przypadków szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych wymaga zastosowania zaawansowanych narzędzi i strategii. Przede wszystkim należy wdrożyć systemy wykrywania i zapobiegania intruzom (IDS/IPS), które monitorują ruch sieciowy i mogą identyfikować podejrzane działania wskazujące na próby szpiegostwa. Ważne jest również stosowanie narzędzi do analizy zachowań użytkowników (UBA/UEBA), które potrafią wykrywać nietypowe wzorce działania mogące sugerować wewnętrzne próby wykradzenia danych. Zastosowanie kompleksowych systemów zarządzania informacją i zdarzeniami bezpieczeństwa (SIEM) umożliwia agregację danych z różnych źródeł i skuteczniejsze wykrywanie zagrożeń. Dodatkowo, regularne audyty bezpieczeństwa oraz testy penetracyjne mogą ujawnić potencjalne słabości w zabezpieczeniach, które mogłyby być wykorzystane do szpiegostwa.

Ekspert 9.

Zarządzanie ryzykiem szpiegostwa korporacyjnego z perspektywy bezpieczeństwa osobowego obejmuje ścisłe procedury weryfikacji tożsamości oraz monitorowania pracowników i kontrahentów. Wprowadzenie szkoleń z zakresu bezpieczeństwa informacji pomoże podnieść świadomość pracowników o zagrożeniach i metodach ochrony danych. Stosowanie umów o zachowaniu poufności i regularne przeglądy procedur dostępu do poufnych informacji są kluczowe. Niezwykle ważne jest także utrzymanie ścisłej kontroli nad fizycznym i cyfrowym dostępem do wrażliwych obszarów, włączając monitoring wizyjny i systemy logowania działalności użytkowników, które mogą wykryć nieautoryzowany dostęp lub nieprawidłowe użycie danych.

Ekspert 10.

W kontekście fizycznego bezpieczeństwa, monitoring i wykrywanie szpiegostwa korporacyjnego wymagają zintegrowanego podejścia obejmującego zarówno zaawansowane technologie, jak i tradycyjne metody ochrony. Instalacja systemów CCTV, szczególnie z funkcjami analizy obrazu i rozpoznawania twarzy, umożliwia bieżące monitorowanie i szybką reakcję na wszelkie podejrzane działania. Implementacja systemów kontroli dostępu z autoryzacją wielopoziomową do krytycznych obszarów technicznych zapobiega nieautoryzowanemu dostępowi. Regularne przeglądy bezpieczeństwa, w tym inspekcje fizyczne i testy systemów

alarmowych, wzmacniają obronę przed próbami szpiegostwa. Integracja fizycznego i cyfrowego monitoringu z systemami zarządzania bezpieczeństwem może znacząco zwiększyć zdolności przedsiębiorstwa do identyfikacji i reagowania na incydenty szpiegowskie.

Ekspert 11.
Przedsiębiorstwo sektora technologii informacyjno-komunikacyjnych może skutecznie monitorować i wykrywać potencjalne przypadki szpiegostwa korporacyjnego poprzez wdrożenie zaawansowanych narzędzi do monitorowania i analizy danych. Kluczowym elementem jest implementacja systemów SIEM (Security Information and Event Management), które zbierają i analizują logi z różnych źródeł w czasie rzeczywistym, identyfikując podejrzane wzorce aktywności. Wykorzystanie technologii sztucznej inteligencji i uczenia maszynowego do wykrywania anomalii w ruchu sieciowym oraz zachowaniach użytkowników może również pomóc w identyfikacji nietypowych działań wskazujących na szpiegostwo. Systemy DLP (Data Loss Prevention) są niezbędne do monitorowania i kontrolowania przepływu poufnych informacji, zapobiegając ich nieautoryzowanemu wyciekom. Regularne audyty bezpieczeństwa i testy penetracyjne pozwalają na ocenę skuteczności istniejących zabezpieczeń i identyfikację potencjalnych luk.

Ekspert 12.
Skuteczne monitorowanie i wykrywanie przypadków szpiegostwa korporacyjnego wymaga zastosowania wielu metod i narzędzi. Przede wszystkim, przedsiębiorstwo powinno prowadzić stały monitoring aktywności pracowników poprzez systemy do zarządzania tożsamościami i dostępem (IAM), które śledzą, kto i kiedy uzyskuje dostęp do wrażliwych danych. Regularne przeglądy uprawnień oraz monitorowanie logów z systemów mogą pomóc w wykrywaniu nietypowych działań, takich jak próby dostępu do danych poza zakresem obowiązków pracownika. Działania pozorowane, takie jak symulowane ataki phishingowe, mogą sprawdzić czujność pracowników i ich reakcje na próby wyłudzenia informacji. Ważne jest również prowadzenie regularnych szkoleń z zakresu bezpieczeństwa informacji, aby pracownicy byli świadomi zagrożeń i wiedzieli, jak reagować na podejrzane działania. Współpraca z zewnętrznymi firmami zajmującymi się cyberbezpieczeństwem może dostarczyć dodatkowych narzędzi i wiedzy eksperckiej do monitorowania zagrożeń i reagowania na incydenty.

h)

Jaką rolę odgrywają agencje rządowe i organy ścigania w zapobieganiu i reagowaniu na przypadki szpiegostwa korporacyjnego?

Ekspert 1.
Obecnie, sytuacja związana z partycypacją agencji rządowych i organów ścigania w procesie przeciwdziałania szpiegostwu korporacyjnemu jest w zasadzie znikoma. W ramach branży znane są przypadki, gdy przedsiębiorstwa jawnie ze sobą konkurują stosując przy tym nieczyste posunięcia i pozostaje to bez reakcji. Również w kwestii organów ścigania, reakcja na incydenty bezpieczeństwa jest zawsze post factum i związana jest głównie z zawiadomieniem wystosowanym przez przedsiębiorstwo. Sytuacja znacząco poprawia się w przypadku prowadzenia kampanii informacyjnych mających na celu wzrost świadomości jednostki na temat zagrożeń cybernetycznych. Jednak mimo wszystko, są to działania nieskoordynowane,

cechujące się niskim zasięgiem odbiorców końcowych oraz wąskim ujęciem tematyki. Dodatkowo, materiały te powinny obejmować również informacje dotyczące zachowania oraz dobrych praktyk podczas wyjazdów zagranicznych związanych ze szkoleniem lub udziałem w branżowych targach. Potrzebne jest rozwiązanie systemowe, które pozwalałoby na organizowanie kompleksowych szkoleń zarówno dla kadry kierowniczej jak i pracowników, mających na celu pełne zapoznanie z problematyką bezpieczeństwa w kontekście zagrożeń wynikających z działalności obcych służb specjalnych, zorganizowanych grup przestępczych oraz nielegalnej konkurencji pomiędzy przedsiębiorstwami z branży sektora technologii informacyjno-komunikacyjnych.

Ekspert 2.

Należy przede wszystkim wprowadzić odpowiednie przepisy prawne i ustawy, które jednoznacznie określają nielegalność takich działań. Brak jasnego zakazu w przepisach i brak ich zastosowania do wszystkich przypadków może sugerować osobie próbującej przeprowadzić tego rodzaju działania, że nie popełnia czynu niezgodnego z prawem. Konieczne jest wyraźne określenie, że takie działania są zabronione i niezgodne z obowiązującymi przepisami. W przypadku braku jasnych uregulowań, osoba, która podejmuje takie działania, może po prostu uznać, że próbuje pozyskać informacje, które uważa za potrzebne, nie zdając sobie sprawy, że jej działania są niezgodności z prawem.

Ekspert 3.

Agencje rządowe i organy ścigania odgrywają kluczową rolę w zapobieganiu i reagowaniu na przypadki szpiegostwa korporacyjnego, co stanowi istotne wsparcie zarówno dla sektora prywatnego, jak i dla ogólnego bezpieczeństwa narodowego. Ich działalność obejmuje tworzenie i wdrażanie przepisów prawnych mających na celu ochronę przed szpiegostwem korporacyjnym, w tym ustaw o ochronie tajemnic handlowych i własności intelektualnej. Przykłady takich aktów prawnych to Ustawa o Ochronie Tajemnic Handlowych (Defend Trade Secrets Act) w Stanach Zjednoczonych. Organy ścigania takie jak FBI w USA czy Europol w Europie, dysponują specjalnymi jednostkami zajmującymi się cyberprzestępczością i szpiegostwem gospodarczym, prowadząc dochodzenia i ścigając sprawców zarówno na poziomie krajowym, jak i międzynarodowym. Ważną częścią ich działań jest również współpraca międzynarodowa w celu wymiany informacji, koordynacji działań oraz wzajemnego wsparcia w walce ze szpiegostwem korporacyjnym, co jest kluczowe w obliczu globalnego zasięgu zagrożeń. Ponadto, agencje te organizują kampanie informacyjne, szkolenia i warsztaty dla przedsiębiorstw na temat zagrożeń związanych ze szpiegostwem korporacyjnym oraz sposobów ich minimalizacji, zwiększając wiedzę i świadomość najlepszych praktyk bezpieczeństwa. Budują także partnerstwa i kanały komunikacji między sektorem publicznym a prywatnym, co umożliwia szybką wymianę informacji o nowych zagrożeniach i metodach ich przeciwdziałania, przykładem czego mogą być publiczno-prywatne ośrodki reagowania na incydenty bezpieczeństwa cybernetycznego. Rola tych agencji obejmuje również zbieranie, analizowanie i udostępnianie informacji wywiadowczych na temat potencjalnych zagrożeń szpiegowskich, co jest kluczowe dla wczesnego wykrywania i zapobiegania szpiegostwu korporacyjnemu. Udzielają także wsparcia technologicznego i doradczego przedsiębiorstwom w zakresie zabezpieczeń i metod ochrony przed szpiegostwem, w tym poprzez udostępnianie narzędzi, zasobów i najlepszych praktyk w dziedzinie

cyberbezpieczeństwa. Współpraca i dialog między sektorem publicznym a prywatnym są kluczowe dla skutecznego adresowania tych wyzwań, zapewniając bezpieczeństwo ekonomiczne i ochronę przed nielegalnym pozyskiwaniem wiedzy oraz tajemnic handlowych przez konkurencję lub państwa.

Ekspert 4.

Agencje rządowe i organy ścigania odgrywają istotną rolę w zapobieganiu i reagowaniu na przypadki szpiegostwa korporacyjnego zarówno na poziomie krajowym, jak i międzynarodowym. Ich zaangażowanie manifestuje się poprzez tworzenie i egzekwowanie przepisów prawnych dotyczących ochrony tajemnic handlowych, własności intelektualnej oraz danych osobowych, co ma na celu odstraszanie potencjalnych szpiegów poprzez surowe kary. Prowadzą oni także śledztwa, zbierają dowody i ścigają sprawców, a także wspierają przedsiębiorstwa w dochodzeniu swoich praw na drodze sądowej. Istotna jest również ich rola w międzynarodowej współpracy, która pozwala na zwalczanie szpiegostwa korporacyjnego o zasięgu transgranicznym. Agencje te zajmują się także edukacją i podnoszeniem świadomości wśród przedsiębiorstw na temat ryzyka i metod ochrony przed szpiegostwem korporacyjnym. Współpracują z sektorem prywatnym, wymieniając informacje o zagrożeniach i najlepszych praktykach, doradzając w zakresie środków bezpieczeństwa. Ponadto, mogą rozwijać lub wspierać rozwój narzędzi i technologii wykrywających i zapobiegających szpiegostwu, udostępniając je przedsiębiorstwom. Szczególną uwagę przykładają do ochrony infrastruktury krytycznej, co jest kluczowe dla bezpieczeństwa narodowego. Organizują także szkolenia i warsztaty dla przedsiębiorstw, ucząc, jak chronić się przed szpiegostwem i jak reagować na incydenty. Działania te są niezbędne dla utrzymania bezpiecznego środowiska biznesowego, a wsparcie prawne, operacyjne i edukacyjne oferowane przez agencje rządowe i organy ścigania stanowi wielowymiarową ochronę przed szpiegostwem korporacyjnym.

Ekspert 5.

Agencje rządowe i organy ścigania pełnią kluczową rolę w zapobieganiu i reagowaniu na szpiegostwo korporacyjne, co jest niezbędne dla ochrony zasobów i know-how przedsiębiorstw. Działają one w kilku kluczowych obszarach, od edukacji i prewencji poprzez organizowanie kampanii informacyjnych, które mają na celu podnoszenie świadomości na temat zagrożeń oraz sposobów ich minimalizowania. Organizują również szkolenia, warsztaty i konferencje, które koncentrują się na cyberbezpieczeństwie i ochronie własności intelektualnej. Ponadto, oferują porady i wsparcie techniczne, pomagając firmom w ocenie ryzyka i wdrażaniu efektywnych zabezpieczeń. Równie ważna jest koordynacja wymiany informacji o zagrożeniach, co umożliwia firmom dostęp do aktualnych danych o potencjalnych zagrożeniach i incydentach. W przypadku wykrycia aktów szpiegostwa, przedsiębiorstwa mogą liczyć na wsparcie w prowadzeniu dochodzeń i ściganiu sprawców. Organy te uczestniczą także w rozwijaniu i wdrażaniu regulacji prawnych, które zabezpieczają przed nowymi wyzwaniami w sferze cyberbezpieczeństwa i szpiegostwa korporacyjnego. Dzięki temu złożonemu podejściu, agencje rządowe i organy ścigania stanowią solidne wsparcie dla przedsiębiorstw w ochronie ich kluczowych zasobów przed zagrożeniami zewnętrznymi i wewnętrznymi, zapewniając jednocześnie wsparcie prawne i techniczne.

Ekspert 6.

Agencje rządowe i organy ścigania odgrywają kluczową rolę w zapobieganiu i reagowaniu na przypadki szpiegostwa korporacyjnego, jednak jak wynika z dotychczasowej praktyki, ich obecne zaangażowanie i skuteczność działania mogą być niewystarczające w niektórych sytuacjach. Te instytucje mogą pełnić ważne role w prewencji poprzez organizowanie kampanii informacyjnych, które podnoszą świadomość na temat zagrożeń cybernetycznych i korporacyjnych wśród przedsiębiorstw oraz ich pracowników, a także oferowanie konsultacji i wsparcia technicznego w zakresie najlepszych praktyk zabezpieczeń i strategii obronnych. W reakcji na zgłoszone incydenty, odpowiedzialność organów ścigania obejmuje prowadzenie śledztw, identyfikację sprawców i wdrażanie odpowiednich środków prawnych, a także współpracę międzynarodową, co jest kluczowe ze względu na często międzynarodowy wymiar szpiegostwa korporacyjnego. Edukacja i szkolenia również stanowią istotny element, gdzie agencje rządowe mogą brać udział w projektowaniu i realizacji szkoleń dla pracowników i kadry zarządzającej w zakresie identyfikacji i reagowania na szpiegostwo. Tworzenie i aktualizacja regulacji prawnych w zakresie ochrony danych osobowych i tajemnic handlowych również należą do kluczowych zadań agencji rządowych, wpływających na poziom ochrony prawnej dostępnego dla firm. Obecne działania są często nieskoordynowane i reaktywne, co podkreśla potrzebę systemowych rozwiązań mających na celu zwiększenie skuteczności interwencji rządowych. Poprawa koordynacji, rozszerzenie działań prewencyjnych oraz zwiększone zaangażowanie w edukację i szkolenia mogą znacznie wzmocnić rolę tych instytucji w zapobieganiu i reagowaniu na szpiegostwo korporacyjne.

Ekspert 7.

Istotne jest stworzenie i wdrożenie odpowiednich przepisów prawnych, które jednoznacznie zakazują nielegalnych działań. Obecnie brak jednoznacznych zakazów i niedostateczne zastosowanie istniejących przepisów do wszystkich możliwych przypadków może skutkować błędnym przekonaniem osób podejmujących nielegalne działania, że ich postępowanie jest zgodne z prawem. Dlatego niezbędne jest, aby prawo jednoznacznie zakazywało takich działań i było konsekwentnie stosowane, eliminując wszelkie niejasności. W sytuacji, gdy regulacje są niejasne, osoby te mogą nie zdawać sobie sprawy z naruszenia prawa, przekonane, że ich działania są usprawiedliwione pozyskaniem niezbędnych informacji.

Ekspert 8.

Agencje rządowe i organy ścigania odgrywają kluczową rolę w zapobieganiu i reagowaniu na przypadki szpiegostwa korporacyjnego, szczególnie w kontekście naruszeń, które mogą mieć wpływ na bezpieczeństwo narodowe lub gospodarcze. Wspierają one przedsiębiorstwa poprzez udostępnianie informacji o aktualnych zagrożeniach i trendach w cyberprzestępczości. Agencje te często prowadzą programy współpracy z sektorem prywatnym, oferując szkolenia, narzędzia do oceny ryzyka oraz wspierając w implementacji najlepszych praktyk w zakresie cyberbezpieczeństwa. W przypadku ataku, organy ścigania współpracują z przedsiębiorstwami w celu identyfikacji sprawców, zapewnienia odpowiedniej odpowiedzi prawnej i minimalizacji szkód. Dodatkowo, mogą one również przeprowadzać operacje pod przykrywką w celu wykrywania i rozbijania zorganizowanych grup przestępczych zaangażowanych w szpiegostwo korporacyjne.

Ekspert 9.

Agencje rządowe i organy ścigania pełnią istotną rolę w edukacji i przeciwdziałaniu szpiegostwu korporacyjnemu poprzez promowanie standardów bezpieczeństwa oraz wspieranie firm w rozwijaniu kompetencji związanych z ochroną danych. Organizują one warsztaty, konferencje i seminaria, w których eksperci mogą dzielić się wiedzą i doświadczeniami z zakresu ochrony informacji i reagowania na incydenty. W sytuacjach, gdy dojdzie do naruszenia bezpieczeństwa, agencje te mogą również współpracować z przedsiębiorstwami w zakresie dochodzeń, oferując dostęp do zaawansowanych narzędzi i metod śledczych, które pomagają w ustaleniu, jak doszło do naruszenia oraz kto za nim stoi.

Ekspert 10.
W aspekcie fizycznego bezpieczeństwa, agencje rządowe i organy ścigania odgrywają rolę zarówno prewencyjną, jak i reaktywną w przypadku szpiegostwa korporacyjnego. Zapewniają one wsparcie w postaci zaleceń dotyczących fizycznego zabezpieczenia infrastruktury krytycznej, a także mogą dostarczać specjalistyczne urządzenia i technologie, które pomagają w monitorowaniu i ochronie przed fizycznym dostępem nieautoryzowanych osób. W przypadku ataku, agencje te współpracują z przedsiębiorstwami w celu zabezpieczenia miejsca zdarzenia, zbierania dowodów i prowadzenia dochodzeń mających na celu ściganie i pociągnięcie do odpowiedzialności osób odpowiedzialnych za naruszenia bezpieczeństwa.

Ekspert 11.
Agencje rządowe i organy ścigania odgrywają kluczową rolę w zapobieganiu i reagowaniu na przypadki szpiegostwa korporacyjnego, szczególnie w kontekście technologii i infrastruktury krytycznej. Przede wszystkim, agencje te dostarczają przedsiębiorstwom wytyczne i standardy bezpieczeństwa, które pomagają w tworzeniu i utrzymywaniu bezpiecznych systemów informatycznych. Organy rządowe często prowadzą kampanie informacyjne i szkolenia, mające na celu podnoszenie świadomości na temat zagrożeń związanych ze szpiegostwem korporacyjnym i cyberatakami. W przypadku wykrycia szpiegostwa, agencje rządowe mogą również udzielić wsparcia technicznego w analizie i śledzeniu ataków, korzystając z zaawansowanych narzędzi i technologii, które mogą nie być dostępne dla prywatnych przedsiębiorstw. Dodatkowo, agencje rządowe mogą działać na arenie międzynarodowej, współpracując z innymi krajami w celu ścigania sprawców i ograniczenia międzynarodowego szpiegostwa korporacyjnego.

Ekspert 12.
Agencje rządowe i organy ścigania odgrywają istotną rolę w zapobieganiu i reagowaniu na przypadki szpiegostwa korporacyjnego poprzez zapewnianie wsparcia prawnego i operacyjnego. Organy te mogą prowadzić dochodzenia w sprawie przypadków szpiegostwa, zbierać dowody i identyfikować sprawców, co jest kluczowe dla pociągnięcia ich do odpowiedzialności. Współpraca z agencjami rządowymi może również pomóc w wymianie informacji o zagrożeniach i najlepszych praktykach ochrony, co jest niezbędne dla przedsiębiorstw w celu skuteczniejszej obrony przed szpiegostwem. Agencje rządowe mogą również prowadzić audyty i kontrole bezpieczeństwa, identyfikując luki w zabezpieczeniach i zalecając odpowiednie środki naprawcze. W przypadku incydentów, organy ścigania mogą zapewnić wsparcie w zakresie zarządzania kryzysowego i odzyskiwania danych, co pomaga

przedsiębiorstwom w minimalizowaniu skutków szpiegostwa i przywracaniu normalnego funkcjonowania.

i)

W jaki sposób aktualny konflikt rosyjsko-ukraiński wpłynął na postrzeganie i reagowanie na zagrożenia szpiegostwem korporacyjnym w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych?

Ekspert 1.

Aktualny konflikt rosyjsko-ukraiński zdecydowanie zintensyfikował świadomość przedsiębiorstw sektora technologii informacyjno-komunikacyjnych na temat zagrożeń szpiegostwem korporacyjnym, skłaniając do przemyślenia i wzmocnienia ich strategii bezpieczeństwa. Oto kilka kluczowych zmian w podejściu do tych zagrożeń: Konflikt podkreślił znaczenie zaawansowanych stałych zagrożeń (APT), szczególnie tych pochodzących z Rosji i Chin, co skłoniło przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych do bardziej skrupulatnej analizy i identyfikacji potencjalnych wektorów ataku. W rezultacie, inwestycje w zaawansowane technologie obronne i narzędzia analityczne do monitorowania i wykrywania takich zagrożeń wzrosły. W odpowiedzi na rosnące ryzyko, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych skoncentrowały się na wzmocnieniu zarówno zabezpieczeń cybernetycznych, jak i fizycznych swoich infrastruktur. Wdrożono bardziej zaawansowane systemy zapobiegania intruzjom, systemy wykrywania anomalii oraz ulepszono fizyczne środki ochrony krytycznej infrastruktury. Konflikt uwypuklił także potrzebę dostosowania się do szybko zmieniających regulacji ustawowych i dyrektyw, takich jak NIS 2, wymuszając na przedsiębiorstwach szybką adaptację do nowych wymogów w zakresie cyberbezpieczeństwa i ochrony danych. Przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych zwiększyły nacisk na szkolenia pracowników w zakresie bezpieczeństwa informacji, podnosząc ich świadomość na temat potencjalnych zagrożeń i najlepszych praktyk obronnych. Szczególną uwagę poświęcono zagrożeniom wewnętrznym i zwiększeniu lojalności pracowników. Konflikt skłonił przedsiębiorstwa do przeprowadzenia dokładniejszych analiz ryzyka, oceny najczęściej odnotowywanych zagrożeń i opracowania skutecznych strategii reagowania. To obejmuje zarówno ryzyka cybernetyczne, jak i te wynikające z niestabilności politycznej oraz działań sił natury. Zwiększyła się współpraca pomiędzy przedsiębiorstwami sektora technologii informacyjno-komunikacyjnych, organami ścigania i agencjami rządowymi w celu lepszego przeciwdziałania i reagowania na przypadki szpiegostwa korporacyjnego. Umożliwiło to lepszą wymianę informacji o zagrożeniach i skoordynowane działania obronne.

Ekspert 2.

Konflikt zintensyfikował percepcję zagrożeń cybernetycznych i szpiegostwa korporacyjnego, skłaniając przedsiębiorstwa do przeglądu i wzmocnienia swoich strategii bezpieczeństwa. Przedsiębiorstwa stały się bardziej świadome możliwości wykorzystania wojen informacyjnych i cyberataków jako narzędzi w konfliktach geopolitycznych, co przekłada się na wzrost inwestycji w ochronę danych i infrastruktury krytycznej. W odpowiedzi na rosnące zagrożenie, przedsiębiorstwa dokładnie oceniły swoje systemy i procedury w celu identyfikacji słabych punktów i potencjalnych wektorów ataków. To doprowadziło do wzmocnienia zabezpieczeń, w tym lepszego zarządzania dostępem, wprowadzenia bardziej zaawansowanych systemów

uwierzytelniania i szyfrowania danych, a także rozbudowy zdolności do wykrywania i reagowania na incydenty bezpieczeństwa. Konflikt rosyjsko-ukraiński podkreślił znaczenie współpracy międzynarodowej i wymiany informacji o zagrożeniach między przedsiębiorstwami, branżami i rządami. Dzięki temu możliwa jest szybsza identyfikacja i neutralizacja nowych zagrożeń, a także lepsze przygotowanie na przyszłe ataki. Wzrost świadomości bezpieczeństwa wśród pracowników został uznany za kluczowy element strategii obronnych. Przedsiębiorstwa zainwestowały w szkolenia i programy edukacyjne, mające na celu uświadomienie pracownikom potencjalnych zagrożeń i nauczenie ich, jak rozpoznawać i reagować na próby szpiegostwa czy ataki socjotechniczne. Organizacje zaczęły postrzegać bezpieczeństwo jako integralną część każdego aspektu działalności, a nie tylko jako zabezpieczenie techniczne. To podejście obejmuje zarządzanie ryzykiem, ciągłość działania, ochronę danych osobowych i własności intelektualnej, jak również zabezpieczenia fizyczne i cybernetyczne. Przedsiębiorstwa zwiększyły swoje zdolności do szybkiego reagowania i adaptacji w przypadku ataków, poprzez rozwój planów awaryjnych i ciągłości działania. Uwzględnienie różnych scenariuszy ataków w planowaniu pozwala na lepsze przygotowanie i minimalizację potencjalnych szkód.

Ekspert 3.

Konflikt rosyjsko-ukraiński znacząco wpłynął na postrzeganie i reagowanie na zagrożenia szpiegostwem korporacyjnym w międzynarodowych przedsiębiorstwach, skłaniając je do przewartościowania i zintensyfikowania działań w zakresie bezpieczeństwa informacji. Zwrócił uwagę na wzrost świadomości dotyczącej cyberzagrożeń, pokazując, że mogą one służyć jako narzędzia w konfliktach geopolitycznych. W rezultacie organizacje stały się bardziej świadome potencjalnego wykorzystania ich infrastruktury i danych w szerszym kontekście działań wojennych lub jako celów strategicznych. To przełożyło się na przyspieszenie inwestycji w cyberbezpieczeństwo, w tym na wdrażanie zaawansowanych technologii ochronnych, rozwijanie kompetencji zespołów bezpieczeństwa oraz zwiększenie budżetów dedykowanych na te cele. Konflikt spowodował także rewizję polityk bezpieczeństwa oraz procedur reagowania na incydenty w wielu organizacjach, skłaniając do bardziej ryzykownych scenariuszy zarządzania. Przedsiębiorstwa stały się bardziej zorientowane na ryzyko, co skłoniło do lepszego zrozumienia i zarządzania ryzykiem szpiegostwa korporacyjnego. Wzmocniła się również współpraca międzysektorowa i międzynarodowa, ponieważ przedsiębiorstwa uznały, że zagrożenia cybernetyczne nie znają granic. Wymiana informacji o zagrożeniach, najlepszych praktykach i strategiach obronnych stała się powszechniejsza. Dodatkowo, konflikt przyczynił się do zwiększenia inwestycji w szkolenia pracowników z zakresu bezpieczeństwa informacji i świadomości cyberbezpieczeństwa, podkreślając, że pracownicy są pierwszą linią obrony przed atakami cybernetycznymi i szpiegostwem. Przedsiębiorstwa dokonały również przeglądu swoich łańcuchów dostaw pod kątem potencjalnych słabości i ryzyka szpiegostwa, zwracając uwagę na konieczność dywersyfikacji dostawców i zabezpieczenia łańcuchów dostaw przed możliwymi przerwaniami lub manipulacjami.

Ekspert 4.

Konflikt rosyjsko-ukraiński wywarł istotny wpływ na postrzeganie zagrożeń szpiegostwa korporacyjnego w międzynarodowych przedsiębiorstwach, zmuszając je do adaptacji ich strategii bezpieczeństwa. W odpowiedzi na te wyzwania, przedsiębiorstwa sektora technologii

informacyjno-komunikacyjnych i inne sektory krytyczne podjęły szereg kluczowych działań. Zwiększają świadomość i edukację pracowników na temat metod szpiegostwa korporacyjnego i technik inżynierii społecznej, inwestując w szkolenia, które mają na celu nauczenie pracowników rozpoznawania potencjalnych prób szpiegostwa i odpowiednich metod obrony. Skoncentrowały się również na ciągłym monitorowaniu i analizie ryzyka, aby szybko identyfikować i reagować na nowe zagrożenia. Wzmocnienie cyberbezpieczeństwa stało się priorytetem, z inwestycjami w zaawansowane technologie i narzędzia zabezpieczające. W obliczu globalnego charakteru zagrożeń, zacieśniono współpracę międzynarodową, wymieniając informacje na temat zagrożeń i najlepszych praktyk. Bezpieczeństwo łańcucha dostaw również zostało podkreślone, z rygorystycznymi procedurami weryfikacji dostawców. Przedsiębiorstwa dbają o zgodność z międzynarodowymi i krajowymi przepisami dotyczącymi bezpieczeństwa, a wzmożone napięcia geopolityczne skierowały większą uwagę na ochronę fizyczną i bezpieczeństwo pracowników, zwłaszcza w regionach uznanych za ryzykowne. Reagowanie na te zagrożenia wymaga holistycznego podejścia, elastyczności oraz ciągłego doskonalenia strategii bezpieczeństwa, z proaktywnym podejściem i inwestycją w nowoczesne technologie i szkolenia jako kluczowymi elementami skutecznego zarządzania ryzykiem.

Ekspert 5.

Konflikt rosyjsko-ukraiński miał znaczący wpływ na podejście przedsiębiorstw sektora technologii informacyjno-komunikacyjnych do zagrożeń szpiegostwem korporacyjnym, co skłoniło je do zrewidowania i wzmocnienia swoich strategii bezpieczeństwa na wielu poziomach. Wzrost świadomości o możliwościach cyberataków jako narzędzia wojennego i destabilizacji przekłada się na zwiększone inwestycje w zaawansowane technologie obronne i systemy reagowania na incydenty, w tym systemy wykrywania i reagowania na incydenty, oraz na rozbudowę kompetencji w zakresie cyberbezpieczeństwa wśród pracowników. Równocześnie, organizacje intensyfikują współpracę z organami rządowymi i międzynarodowymi organizacjami, co obejmuje wymianę informacji o zagrożeniach i wspólne inicjatywy mające na celu zwiększenie odporności cybernetycznej. Przedsiębiorstwa te również przeprowadzają przegląd i aktualizację swoich polityk i procedur bezpieczeństwa, aby lepiej radzić sobie z ewoluującymi zagrożeniami i zabezpieczyć ciągłość działania w razie ataków. Istotne stało się także rozwijanie umiejętności analitycznych i wywiadowczych, co pozwala na głębsze zrozumienie metod działania cyberprzestępców oraz na skuteczną obronę przed szpiegostwem korporacyjnym. Dodatkowo, konflikt uwydatnił wagę ochrony informacji niejawnych, skłaniając organizacje do wprowadzenia dodatkowych środków ochrony swoich tajemnic handlowych i własności intelektualnej. W efekcie, konflikt rosyjsko-ukraiński przyczynił się do głębokiej transformacji w podejściu do bezpieczeństwa informacji w branży sektora technologii informacyjno-komunikacyjnych, z naciskiem na ciągłe monitorowanie, analizę zagrożeń oraz inwestycje w nowoczesne technologie i rozwój umiejętności, co ma na celu efektywne przeciwdziałanie zagrożeniom szpiegowskim.

Ekspert 6.

Aktualny konflikt rosyjsko-ukraiński znacząco wpłynął na sposób, w jaki przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych postrzegają i reagują na zagrożenia szpiegostwem korporacyjnym. Konflikt ten podkreślił ryzyko ataków, szczególnie pochodzących z Rosji i Chin, co skłoniło organizacje do zwiększenia inwestycji w zaawansowane technologie

obronne i narzędzia analityczne służące do monitorowania i wykrywania takich zagrożeń. W odpowiedzi na wzrost ryzyka, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych skoncentrowały się na wzmocnieniu swoich zabezpieczeń, zarówno w cyberprzestrzeni, jak i fizycznie, wprowadzając bardziej zaawansowane systemy zapobiegania intruzjom i systemy wykrywania anomalii oraz ulepszając fizyczne środki ochrony infrastruktury krytycznej. Konieczność szybkiej adaptacji do nowych regulacji, takich jak dyrektywa NIS 2, wymusiła aktualizację i wzmocnienie strategii dotyczących cyberbezpieczeństwa i ochrony danych. Ponadto, przedsiębiorstwa zwiększyły nacisk na szkolenia pracowników w zakresie bezpieczeństwa informacji, podnosząc ich świadomość odnośnie potencjalnych zagrożeń i najlepszych praktyk obronnych, z szczególnym uwzględnieniem zagrożeń wewnętrznych i zwiększenia lojalności pracowników. Wzmocnienie współpracy z organami ścigania i agencjami rządowymi pozwoliło na lepszą wymianę informacji o zagrożeniach i koordynację działań obronnych. W rezultacie, konflikt rosyjsko-ukraiński zmusił przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych do głębokiej refleksji nad swoimi strategiami bezpieczeństwa i przyczynił się do wdrożenia szeregu zmian mających na celu zwiększenie odporności na zagrożenia szpiegostwem korporacyjnym i cyberatakami, co obejmuje zarówno aspekty technologiczne, jak i organizacyjne, stanowiąc kompleksowe podejście do zarządzania bezpieczeństwem informacji w coraz bardziej niepewnym globalnym środowisku.

Ekspert 7.

Konflikt rosyjsko-ukraiński wywarł znaczący wpływ na międzynarodowe przedsiębiorstwa, zwiększając świadomość zagrożeń szpiegostwa korporacyjnego i cybernetycznych. Przedsiębiorstwa zaczęły bardziej koncentrować się na zagrożeniach wynikających z wojen informacyjnych i cyberataków, co skłoniło je do zintensyfikowania inwestycji w ochronę danych oraz infrastruktury krytycznej. W odpowiedzi na zwiększone ryzyko, przedsiębiorstwa dokładnie przeanalizowały swoje systemy w poszukiwaniu luk bezpieczeństwa, co doprowadziło do lepszego zarządzania dostępem, wdrożenia zaawansowanych metod uwierzytelniania, szyfrowania oraz rozwoju zdolności do wykrywania i reagowania na incydenty. Rosyjsko-ukraińska konfrontacja podkreśliła także wagę międzynarodowej współpracy i wymiany informacji, co ułatwia szybsze identyfikowanie nowych zagrożeń. Zwiększono również świadomość bezpieczeństwa wśród pracowników poprzez szkolenia, co pomaga im rozpoznawać i efektywnie reagować na potencjalne próby szpiegostwa i ataki socjotechniczne. Bezpieczeństwo stało się istotnym elementem operacyjnym firm, obejmując zarządzanie ryzykiem, ciągłość działalności oraz ochronę danych i własności intelektualnej. Przedsiębiorstwa poprawiły również swoją zdolność do szybkiej reakcji i adaptacji na ataki dzięki rozwijaniu planów awaryjnych. W konsekwencji, międzynarodowe organizacje przykładają teraz większą wagę do cyberbezpieczeństwa i ochrony przed szpiegostwem, inwestując w nowoczesne technologie i rozwijając współpracę międzynarodową, aby lepiej przygotować się na przyszłe wyzwania.

Ekspert 8.

Aktualny konflikt rosyjsko-ukraiński znacząco wpłynął na postrzeganie zagrożeń szpiegostwem korporacyjnym, szczególnie w kontekście cyberbezpieczeństwa. Przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych na całym świecie stały się bardziej świadome

potencjalnych cyberataków, które mogą być sponsorowane przez państwa lub pochodzić od grup hakerskich związanych z konfliktami geopolitycznymi. Wzrosło zainteresowanie zaawansowanymi technologiami obronnymi, takimi jak zaawansowane systemy wykrywania i zapobiegania intruzom (IDS/IPS), cyberwywiad oraz zwiększona współpraca międzynarodowa w wymianie informacji o zagrożeniach. Konflikt uwydatnił również potrzebę przemyślanej analizy ryzyka i gotowości na ataki hybrydowe, które mogą łączyć elementy cybernetyczne, dezinformację oraz tradycyjne metody szpiegostwa.

Ekspert 9.

W kontekście bezpieczeństwa osobowego, konflikt rosyjsko-ukraiński przyczynił się do zwiększonego nacisku na weryfikację i monitorowanie pracowników oraz współpracowników w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych, szczególnie w regionach geograficznie lub politycznie bliskich obszarom konfliktu. Przedsiębiorstwa te mogą doświadczać zwiększonej potrzeby ochrony przed potencjalnym wewnętrznym szpiegostwem oraz wzmocnienia procedur dotyczących kontroli dostępu i przeprowadzania bardziej rygorystycznych badań bezpieczeństwa. Takie środki mają na celu nie tylko ochronę przed szpiegostwem, ale również przed możliwością manipulacji pracownikami przez zewnętrzne siły.

Ekspert 10.

W aspekcie fizycznego bezpieczeństwa, konflikt rosyjsko-ukraiński uwypuklił potrzebę zabezpieczenia kluczowej infrastruktury telekomunikacyjnej przed aktami sabotażu, które mogą mieć związek z działaniami szpiegowskimi lub wojnami hybrydowymi. Przedsiębiorstwa zaczęły przykładać większą wagę do zabezpieczania fizycznego swoich obiektów, stosując bardziej zaawansowane technologie monitoringu, kontroli dostępu oraz zabezpieczeń antyterrorystycznych. Dodatkowo, zwiększono inwestycje w redundancję i odporność krytycznej infrastruktury, aby zapewnić ciągłość działania w przypadku prób zakłócenia usług, co jest kluczowe w świetle potencjalnych zagrożeń wynikających z konfliktu.

Ekspert 11.

Aktualny konflikt rosyjsko-ukraiński znacząco wpłynął na postrzeganie i reagowanie na zagrożenia szpiegostwem korporacyjnym w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych. Konflikt podkreślił znaczenie zaawansowanych stałych zagrożeń (APT), szczególnie tych pochodzących z Rosji i innych państw, co skłoniło przedsiębiorstwa z branży do bardziej skrupulatnej analizy i identyfikacji potencjalnych wektorów ataku. W wyniku tych działań, inwestycje w zaawansowane technologie obronne i narzędzia analityczne do monitorowania i wykrywania takich zagrożeń znacznie wzrosły. Przedsiębiorstwa skoncentrowały się na wzmocnieniu zarówno zabezpieczeń cybernetycznych, jak i fizycznych swoich infrastruktur. Wdrożono bardziej zaawansowane systemy zapobiegania intruzjom, systemy wykrywania anomalii oraz ulepszono fizyczne środki ochrony krytycznej infrastruktury. Konflikt uwypuklił także potrzebę dostosowania się do szybko zmieniających regulacji ustawowych i dyrektyw, takich jak NIS 2, co wymusiło na przedsiębiorstwach szybką adaptację do nowych wymogów w zakresie cyberbezpieczeństwa i ochrony danych.

Ekspert 12.

Aktualny konflikt rosyjsko-ukraiński zintensyfikował świadomość przedsiębiorstw sektora technologii informacyjno-komunikacyjnych na temat zagrożeń związanych ze szpiegostwem korporacyjnym, skłaniając do przemyślenia i wzmocnienia strategii bezpieczeństwa. Organizacje zwiększyły nacisk na szkolenia pracowników w zakresie bezpieczeństwa informacji, podnosząc ich świadomość na temat potencjalnych zagrożeń i najlepszych praktyk obronnych. Szczególną uwagę poświęcono zagrożeniom wewnętrznym i zwiększeniu lojalności pracowników, aby zminimalizować ryzyko wycieków informacji. Konflikt skłonił przedsiębiorstwa do przeprowadzenia dokładniejszych analiz ryzyka, oceny najczęściej odnotowywanych zagrożeń i opracowania skutecznych strategii reagowania. Zwiększyła się również współpraca pomiędzy przedsiębiorstwami sektora technologii informacyjno-komunikacyjnych, organami ścigania i agencjami rządowymi, co umożliwiło lepszą wymianę informacji o zagrożeniach i skoordynowane działania obronne. W sumie, konflikt rosyjsko-ukraiński zmotywował przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych do głębokiej refleksji nad swoimi strategiami bezpieczeństwa, skłaniając do wprowadzenia szeregu zmian mających na celu zwiększenie odporności na zagrożenia szpiegostwem korporacyjnym i cyberataki.

j)

Jakich zmian należałoby dokonać w zakresie uregulowań ustawowych?

Ekspert 1.

Głównym obszarem zmiany w kwestii szeroko rozumianego bezpieczeństwa przedsiębiorstwa powinno być umożliwienie przez ustawodawcę prowadzenia tzw. hack back'u. Działanie te polega na przeprowadzeniu przez instytucję lub podmiot gospodarczy działań odwetowych lub ofensywnych ukierunkowanych na źródło ataku. Obecnie prekursorem takich rozwiązań są Stany Zjednoczonego, gdzie ustawodawca uregulował prawnie takie działania i wiele podmiotów gospodarczych oraz instytucji szeroko wykorzystuje wachlarz narzędzi, które otrzymała. Podjęte działania pozwalają podmiotowi nie tylko na ochronę gromadzonych informacji, ale również na zgromadzenie i przekazanie właściwym organom ścigania dowodów lub informacji umożliwiających ściganie sprawców takich ataków.

Ekspert 2.

W kontekście polskiego prawodawstwa, należy szczerze powiedzieć, że brakuje wyraźnych i precyzyjnych przepisów dotyczących ochrony przed działaniami szpiegowskimi. Obecne przepisy są często ogólne i niejasne, co utrudnia ściganie sprawców i w oparciu o konkretne zapisy z aktów prawnych. Ponadto, brakuje jasnych wytycznych dotyczących skutecznych środków, jakie przedsiębiorstwa mogą zaimplementować w celu ochrony przed działaniami szpiegowskimi. Nie istnieje żaden standard postępowania w tej kwestii. Każda firma musi samodzielnie opracowywać i wprowadzać swoje procedury najczęściej w formie kodeksu postępowania. Obejmuje on zazwyczaj podział pracowników na różne grupy, a wymagania są zdefiniowana per określona grupa np. zdecydowanie większej ilości wymagań podlegają członkowie zarządu lub dyrektorzy. Jednak nawet w takim kodeksie trudno jest precyzyjnie określić, jakie konsekwencje grożą za złamanie zasad. Jedyne, co można wskazać, to kary przewidziane w określonych ustawach i kodeksach, co często nie jest wystarczająco

przekonujące dla pracowników. W związku z tym, istnieje potrzeba, aby ustawodawca wprowadził akt prawny ułatwiający firmom funkcjonowanie w tym obszarze.

Ekspert 3.

W obliczu dynamicznie zmieniającego się środowiska cyberbezpieczeństwa i rosnącego zagrożenia szpiegostwem korporacyjnym, istnieje konieczność ciągłego dostosowywania ram prawnych, aby skutecznie chronić przedsiębiorstwa i infrastrukturę krytyczną. Zaleca się przegląd i aktualizację obowiązujących ustaw w celu uwzględnienia nowych technologii i metod ataków, takich jak AI i IoT, które mogą być wykorzystywane w celach szpiegowskich. Ustawodawstwo powinno być na tyle elastyczne, by umożliwić szybką reakcję na zmieniające się zagrożenia. Istotne jest również wzmocnienie ochrony tajemnic handlowych i własności intelektualnej poprzez wprowadzenie bardziej rygorystycznych przepisów, w tym surowszych kar za naruszenie, co może obejmować także lepszą ochronę przed nieuczciwą konkurencją i kradzieżą danych. Równie ważna jest poprawa współpracy międzynarodowej, rozwój i harmonizacja regulacji na poziomie międzynarodowym, co ułatwi ściganie sprawców szpiegostwa korporacyjnego działających transgranicznie i umożliwi skuteczną wymianę informacji i zasobów. Warto także zaostrzyć wymagania dotyczące raportowania incydentów bezpieczeństwa, w tym przypadków szpiegostwa korporacyjnego, zarówno wobec organów regulacyjnych, jak i wobec klientów i partnerów biznesowych. Promowanie standardów i najlepszych praktyk w zakresie bezpieczeństwa przez wprowadzenie wymogów dotyczących wdrożenia określonych standardów w kluczowych przedsiębiorstwach dla bezpieczeństwa gospodarczego i infrastruktury krytycznej jest kluczowe, podobnie jak rozwój mechanizmów wsparcia dla ofiar szpiegostwa korporacyjnego, takich jak specjalistyczne jednostki doradcze czy fundusze odszkodowawcze, które pomagają przedsiębiorstwom w szybkiej reakcji i minimalizacji szkód. Ponadto, inicjatywy ustawowe promujące edukację i podnoszenie świadomości w zakresie cyberbezpieczeństwa wśród przedsiębiorstw i społeczeństwa zwiększą odporność na szpiegostwo korporacyjne i cyberataki. Realizacja tych zmian wymaga zaangażowania zarówno na poziomie krajowym, jak i międzynarodowym, oraz współpracy między rządami, sektorem prywatnym i organizacjami międzynarodowymi, zachowując przy tym równowagę między ochroną a nieograniczaniem innowacji i rozwoju gospodarczego.

Ekspert 4.

Wprowadzenie zmian w przepisach ustawowych jest niezbędne dla zwiększenia skuteczności ochrony przed szpiegostwem korporacyjnym oraz wzmocnienia bezpieczeństwa informacji w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych. W świetle mojego doświadczenia, zalecałbym przeprowadzenie aktualizacji obecnych przepisów tak, aby odzwierciedlały one zmieniający się krajobraz cyberbezpieczeństwa i technologii. Ważne jest rozszerzenie ochrony na nowe formy danych i technologie, takie jak cloud computing, big data, sztuczna inteligencja i Internet Rzeczy. Istotne jest również wprowadzenie bardziej przejrzystych mechanizmów współpracy międzynarodowej w zwalczaniu szpiegostwa korporacyjnego, co ma kluczowe znaczenie w kontekście globalnego charakteru działalności wielu firm. Wzmocnienie ochrony tajemnic handlowych i własności intelektualnej poprzez wprowadzenie surowszych przepisów i kar za ich naruszenie również wydaje się być konieczne. Ponadto, przedsiębiorstwa powinny być zobowiązane do zgłaszania incydentów bezpieczeństwa w wyznaczonym czasie i współpracować z organami ścigania, co może

przyczynić się do szybszego reagowania na zagrożenia i minimalizacji szkód. Regulacje powinny angażować różne podmioty rynkowe, w tym małe i średnie przedsiębiorstwa, które mogą być szczególnie narażone na cyberataki i szpiegostwo. Zachęcanie do wdrażania standardów bezpieczeństwa i uzyskiwania certyfikacji, wspieranie innowacji w zakresie bezpieczeństwa oraz ustanowienie inicjatyw edukacyjnych to kolejne kroki, które mogą pomóc w budowaniu zintegrowanego systemu ochrony. Takie działania są kluczowe dla dostosowania się do szybko ewoluującego środowiska technologicznego i biznesowego.

Ekspert 5.

W odpowiedzi na rosnące zagrożenia dla bezpieczeństwa informacji, kluczowe staje się przystosowanie ram prawnych do dynamicznie zmieniającego się środowiska cyberbezpieczeństwa. Istnieje potrzeba wprowadzenia zmian w zakresie uregulowań ustawowych, które uwzględnią nowe wyzwania technologiczne i umożliwią skuteczną ochronę przedsiębiorstw sektora technologii informacyjno-komunikacyjnych przed szpiegostwem korporacyjnym oraz innymi formami ataków cybernetycznych. Zmiany te powinny obejmować wzmocnienie ochrony danych i prywatności poprzez dostosowanie przepisów do nowoczesnych technologii, zaostrzenie kontroli nad przepływem informacji oraz zwiększenie sankcji za naruszenia ochrony danych osobowych. Należy również rozszerzyć zakres odpowiedzialności podmiotów gospodarczych za zapewnienie odpowiedniego poziomu bezpieczeństwa informacji, w tym wprowadzenie jasnych wytycznych dotyczących obowiązków związanych z raportowaniem incydentów bezpieczeństwa. Konieczne jest także uregulowanie działalności centrów operacji bezpieczeństwa (SOC), określenie ich standardów działania, zakresu obowiązków i uprawnień. Ważne jest wzmocnienie współpracy międzynarodowej poprzez rozwijanie mechanizmów współpracy w zakresie cyberbezpieczeństwa, wzajemną wymianę informacji o zagrożeniach i wspólne działania przeciwdziałające. Ponadto, warto zapewnić wsparcie i ochronę dla sygnalistów poprzez wprowadzenie rozwiązań chroniących osoby zgłaszające naruszenia przepisów, zapewniając im anonimowość i ochronę przed reperkusjami. Promocja standardów i najlepszych praktyk w dziedzinie cyberbezpieczeństwa również jest niezbędna, aby ułatwić dostęp do wiedzy i narzędzi potrzebnych do skutecznego zabezpieczenia. Te zmiany wymagają zaangażowania ustawodawców oraz całego środowiska związanego z cyberbezpieczeństwem, aby stworzyć spójny, elastyczny i skuteczny system prawno-regulacyjny, który odpowie na bieżące i przyszłe wyzwania w ochronie przed zagrożeniami cyfrowymi.

Ekspert 6.

Wprowadzenie regulacji umożliwiających działania hacking'u zwrotnego w kontekście ustawowym stanowi znaczące wyzwanie z punktu widzenia prawa i etyki, mogąc głęboko wpłynąć zarówno na bezpieczeństwo przedsiębiorstw, jak i na ogólny krajobraz cyberbezpieczeństwa. Przepisy powinny dokładnie określać, co jest dozwolone pod pojęciem hacking zwrotny, w tym warunki, pod którymi takie działania mogą być prowadzone, kto może je wykonywać, oraz jakie są oczekiwane protokoły postępowania, z jednoczesnym zdefiniowaniem granic tych działań, aby uniknąć eskalacji konfliktów w cyberprzestrzeni oraz przypadkowego naruszania praw innych podmiotów lub państw. Ważne jest również rozważenie wprowadzenia mechanizmów nadzoru, które zapewniałyby, że działania te są prowadzone odpowiedzialnie i zgodnie z prawem, oraz ustanowienie organu kontrolnego, który

by monitorował te działania, zapewniając, że nie są nadużywane ani nie prowadzą do niezamierzonych konsekwencji. Regulacje powinny również zawierać wytyczne dotyczące współpracy między przedsiębiorstwami a organami ścigania, zapewniając, że informacje zebrane podczas działań hacking'u zwrotnego mogą być wykorzystane do dalszego ścigania przestępców w sposób zgodny z prawem, oraz uregulowanie sposobu, w jaki dowody są zbierane i przekazywane, aby były one akceptowalne w procesach sądowych. Należy także rozważyć wpływ działań hacking'u zwrotnego na międzynarodowe prawa i umowy, aby działania te nie prowadziły do naruszenia suwerenności innych państw ani międzynarodowych norm prawnych, co mogłoby obejmować tworzenie umów bilateralnych lub multilateralnych regulujących te działania. Ponadto, zapewnienie, że przedsiębiorstwa i ich pracownicy są odpowiednio szkoleni w zakresie legalnych metod hacking'u zwrotnego oraz wiedzy na temat ich potencjalnych ryzyk i odpowiedzialności, a także rozwój programów certyfikacyjnych lub licencyjnych dla specjalistów od cyberbezpieczeństwa upoważnionych do prowadzenia tych działań, jest kluczowe. Zmiany w uregulowaniach ustawowych dotyczących pozwolenia na hacking zwrotny wymagają kompleksowego przemyślenia i ostrożności, aby zapewnić, że takie działania są prowadzone w sposób etyczny, odpowiedzialny i zgodny z międzynarodowymi standardami, co powinno być poprzedzone szeroką debatą publiczną oraz konsultacjami z ekspertami w dziedzinie prawa, cyberbezpieczeństwa oraz stosunków międzynarodowych.

Ekspert 7.

W kontekście polskiego systemu prawnego istnieje wyraźny brak precyzyjnych regulacji, które definiowałyby ochronę przed działaniami szpiegowskimi w przedsiębiorstwie. Obecne przepisy, charakteryzujące się ogólnikowością i niejasnościami, często utrudniają efektywne ściganie sprawców oparte na konkretnych zapisach prawnych. Również nie istnieją wyraźne wytyczne, które wskazywałyby organizacjom, jakie środki ochronne powinny wdrożyć, by ustrzec się przed szpiegostwem. W rezultacie, przedsiębiorstwa są zmuszone do samodzielnego opracowywania procedur, które najczęściej przyjmują formę kodeksu postępowania, różnicującego wymagania w zależności od grupy pracowniczej, przy czym najwyższe wymogi dotyczą często kadry zarządzającej. Niestety, takie wewnętrzne kodeksy rzadko precyzyjnie określają konsekwencje naruszeń, co sprawia, że przewidziane kary nie zawsze są wystarczająco odstraszające. Pojawia się zatem nagląca potrzeba, by ustawodawca stworzył prawo, które uprościłoby przedsiębiorcom zabezpieczanie swojej działalności przed działaniami szpiegowskimi.

Ekspert 8.

W zakresie uregulowań ustawowych, istnieje potrzeba aktualizacji i dostosowania przepisów dotyczących cyberbezpieczeństwa do rozwijających się technologii i zmieniającego się krajobrazu zagrożeń. Wprowadzenie bardziej rygorystycznych wymogów dotyczących raportowania incydentów bezpieczeństwa może przyczynić się do szybszej reakcji i lepszego rozumienia zagrożeń na poziomie krajowym. Ponadto, warto rozważyć stworzenie ram prawnych wspierających współpracę między sektorem publicznym a prywatnym w zakresie wymiany informacji o zagrożeniach i najlepszych praktykach, co może znacząco poprawić ogólną reaktywność na incydenty cybernetyczne. Regulacje powinny również uwzględniać zasady ochrony danych osobowych, zwłaszcza w kontekście rosnącej liczby urządzeń IoT i gromadzenia dużych ilości danych.

Ekspert 9.

Wymagane są zmiany w przepisach dotyczących wewnętrznej kontroli i szkoleń z zakresu bezpieczeństwa informacji, które powinny stać się standardem w każdej organizacji, niezależnie od jej wielkości. Uregulowania powinny zobowiązywać przedsiębiorstwa do regularnego przeprowadzania audytów bezpieczeństwa i szkoleń dla pracowników, co zwiększy świadomość zagrożeń i wzmocni kulturę bezpieczeństwa w przedsiębiorstwach. Ponadto, zasadne byłoby wprowadzenie bardziej szczegółowych wytycznych dotyczących zarządzania dostępem do informacji poufnych, w tym wymogów dotyczących autoryzacji wieloskładnikowej i szyfrowania danych.

Ekspert 10.

Należałoby wzmocnić uregulowania dotyczące fizycznego zabezpieczenia infrastruktury krytycznej. Możliwe jest wprowadzenie bardziej rygorystycznych standardów dotyczących kontroli dostępu do kluczowych obiektów, jak również wymóg stosowania zaawansowanych systemów monitoringu i alarmowych. Również zwiększenie wymagań odnośnie do planowania ciągłości działania i reagowania na kryzysy może przyczynić się do lepszej ochrony przed potencjalnymi zagrożeniami fizycznymi. Takie zmiany prawne mogłyby również wspierać rozwój i implementację nowoczesnych technologii bezpieczeństwa, które są kluczowe w ochronie przed szpiegostwem korporacyjnym i innymi formami zagrożeń.

Ekspert 11.

W zakresie uregulowań ustawowych, kluczową zmianą, którą należałoby rozważyć, jest umożliwienie przez ustawodawcę prowadzenia tzw. hack back'u. Działania te polegają na przeprowadzeniu przez instytucję lub podmiot gospodarczy działań odwetowych lub ofensywnych ukierunkowanych na źródło ataku. Umożliwiłoby to przedsiębiorstwom nie tylko ochronę gromadzonych informacji, ale także zgromadzenie i przekazanie właściwym organom ścigania dowodów lub informacji umożliwiających ściganie sprawców takich ataków. Aby jednak takie działania były skuteczne i odpowiedzialne, konieczne jest wprowadzenie precyzyjnych ram prawnych, które określają, kto może prowadzić takie działania, w jakich okolicznościach oraz jakie są ograniczenia i wymagania dotyczące zgłaszania i monitorowania tych działań. Ustawodawstwo powinno również uwzględniać mechanizmy nadzoru i audytu, aby zapewnić, że działania hack back są prowadzone zgodnie z prawem i nie prowadzą do eskalacji konfliktów w cyberprzestrzeni.

Ekspert 12.

W zakresie uregulowań ustawowych, kluczowe jest wprowadzenie zmian, które wspierają proaktywne podejście do bezpieczeństwa informacji. Jednym z takich kroków jest umożliwienie legalnego prowadzenia działań odwetowych, czyli hack back, które mogą pomóc w identyfikacji i neutralizacji źródeł ataków. Oczywiście, wprowadzenie takich przepisów musi być bardzo dobrze przemyślane i zrównoważone, aby nie dopuścić do nadużyć i eskalacji cyberkonfliktów. Wymaga to również ścisłej współpracy z organami ścigania i agencjami rządowymi, które powinny pełnić rolę nadzorczą i koordynacyjną. Ponadto, konieczne jest wprowadzenie przepisów, które nakładają na przedsiębiorstwa obowiązek regularnych audytów bezpieczeństwa oraz raportowania incydentów cybernetycznych. Umożliwi to lepszą

współpracę i wymianę informacji między sektorem prywatnym a organami publicznymi, co jest kluczowe dla skutecznej obrony przed cyberzagrożeniami. Wzmocnienie regulacji dotyczących ochrony danych osobowych oraz obowiązek stosowania zaawansowanych technologii zabezpieczeń, takich jak szyfrowanie i wielopoziomowe uwierzytelnianie, również przyczyniłyby się do zwiększenia poziomu bezpieczeństwa informacji.

k)

Co należałoby zmienić w zakresie szkolenia i doskonalenia pracowników przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych?

Ekspert 1.

Istotnym elementem szkolenia powinno być podnoszenie świadomości pracowników na temat potencjalnych zagrożeń. Umiejętne i przystępne wytłumaczenie wektorów ataków i sposobów ich przeprowadzenia jest kluczowym dla zapobieżenia większości potencjalnych prób nieautoryzowanego dostępu do informacji przedsiębiorstwa. Odnotowano zależność wśród pracowników przeszkolonych z zakresu zagrożeń cybernetycznych, polegającą na tym, iż z dużo większą ostrożnością podchodzą do np. wiadomości elektronicznych przysłanych z nieznanego źródła, ataków phishingowych czy innych prób uzyskania zdalnego dostępu do stacji roboczej oraz tego, iż dużo częściej przesyłają takie wiadomości do analizy przez właściwe komórki ds. cyberbezpieczeństwa przedsiębiorstwa. Równie ważną zmianą powinno być wprowadzenie tzw. kampanii testowych, czyli kontrolowanych działań własnych mających na celu sprawdzenie skuteczności funkcjonujących zabezpieczeń i procedur przy wykorzystaniu narzędzi i metod stosowanych przez cyberprzestępców. Takie działania pozwoliłby na zwiększenie świadomości pracowników w kontekście pojawiających się zagrożeń, jak również na udoskonalenie zabezpieczeń oraz procedur przez administratorów i architektów bezpieczeństwa.

Ekspert 2.

Po pierwsze, zanim pracownik rozpocznie pracę, należy zapewnić, że przeszedł odpowiednie szkolenia i edukację. Pracownicy powinni posiadać wiedzę zarówno na poziomie podstawowym, jak i zaawansowanym. Ważne jest, aby ocenić, jakie informacje są istotne, a które są już nieaktualne i niepotrzebne. Niezbędne jest poznanie podstawowych usług informacyjno-komunikacyjnych oraz zrozumienie, jak zostały wdrożone i jak funkcjonują po stronie klienta końcowego. Niestety, wielu pracowników, nawet po ukończeniu studiów związanych z elektroniką, telekomunikacją czy informatyką, nie potrafi wymienić podstawowych usług. Posiadają natomiast dużą ilość wiedzy technologicznej, która jest już przestarzała i nie jest już wykorzystywana. Dlatego warto wprowadzić przynajmniej kilkadziesiąt godzin szkolenia z zakresu cyberbezpieczeństwa na wszystkich szczeblach edukacji, od technikum po studia. Tego rodzaju szkolenia są niezbędne, ponieważ bez względu na branżę, w której pracuje się dzisiaj, każdy będzie miał styczność z zagrożeniami cybernetycznymi. Przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych powinny przekazywać tę wiedzę swoim pracownikom, którzy często mylnie sądzą, że posiadają wystarczającą wiedzę z uwagi na ukończone studia. Przedsiębiorcy z branży powinni również uczyć pracowników o usługach informacyjno-komunikacyjnych, ponieważ szkolnictwo nie zapewnia takiej wiedzy. Ważne jest również przekazanie informacji o procesach działania firm,

czego niestety również nie uczą w szkołach. Pracownicy muszą zrozumieć, że są częścią większego procesu i będą musieli podejmować odpowiednie działania w oparciu o to, co zostało im powierzone do wykonania. Należy również kształcić pracowników na temat różnych zagrożeń, takich jak phishing. Wszyscy muszą być świadomi tego rodzaju kampanii i wiedzieć, jak się przed nimi bronić. Ważne jest również uczenie pracowników o ochronie danych osobowych, ponieważ RODO (RODO) jest obowiązującym przepisem. Niestety, nie uczą o tym w szkołach / na uczelniach, co jest absurdem, ponieważ absolwenci będą pracować w branży, w której będą mieli styczność z danymi osobowymi klientów. Dodatkowo, pracownicy powinni być szkoleni w zakresie narzędzi i metodologii stosowanych w prowadzeniu projektów, zależnie od specyfiki przedsiębiorstwa. Istotne jest również zapewnienie specjalistycznego szkolenia dla pracowników związanych z konkretnymi technologiami lub obszarami, takimi jak zarządzanie informacjami poufnymi. Szkolenia powinny obejmować również zarządzanie stresem, radzenie sobie w sytuacjach kryzysowych oraz wyjaśnienie, czym jest sytuacja kryzysowa i dlaczego nie każdy incydent jest incydentem związanym z bezpieczeństwem informacji. Podsumowując, szkolenia powinny dostarczaj wiedzy o: podstawowych usługach informacyjno-komunikacyjnych, procesach działających w firmie, zagrożeniach cybernetycznych, ochronie danych osobowych, narzędziach i metodach prowadzenia projektów, specjalistycznych technologiach oraz radzeniu sobie ze stresem i sytuacjami kryzysowymi. Przedsiębiorstwa powinny angażować się w edukację swoich pracowników już na wcześniejszych etapach ich kariery, aby zapewnić odpowiednie przygotowanie i wiedzę niezbędną w kolejnych latach.

Ekspert 3.

W dziedzinie szkoleń i doskonalenia pracowników przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych, istnieje szereg kluczowych obszarów wymagających zmian lub ulepszeń, by skuteczniej odpowiadać na dynamicznie zmieniające się środowisko zagrożeń i wyzwania technologiczne. Zaleca się ustanowienie ciągłego procesu edukacyjnego, który będzie regularnie aktualizowany o nowe zagrożenia, technologie i najlepsze praktyki, co pozwoli pracownikom utrzymać wysoki poziom świadomości bezpieczeństwa. Ważne jest również dostosowanie treści szkoleniowych do różnych grup pracowników w zależności od ich ról, poziomów dostępu do danych oraz specyfiki wykonywanych zadań, co uczyni szkolenia bardziej celowanymi i efektywnymi. Dodatkowo, wprowadzenie większej liczby ćwiczeń praktycznych, symulacji ataków cybernetycznych i warsztatów znacznie zwiększy zaangażowanie i zrozumienie tematu przez pracowników. Kluczowe jest także regularne szkolenie dotyczące nowych technologii i trendów w branży sektora technologii informacyjno-komunikacyjnych, takich jak 5G, IoT czy AI, aby zwiększyć świadomość ryzyka i sposoby ochrony związane z wdrażaniem i użytkowaniem tych technologii. Szczególny nacisk należy również położyć na ochronę danych osobowych i prywatności w szkoleniach, z uwzględnieniem lokalnych i międzynarodowych regulacji, takich jak GDPR, aby pracownicy rozumieli swoje obowiązki i konsekwencje naruszeń. Ponadto, rozwój umiejętności miękkich, takich jak zarządzanie stresującymi sytuacjami czy efektywna komunikacja w sytuacjach kryzysowych, może okazać się kluczowy podczas realnych incydentów bezpieczeństwa. Organizacja szkoleń międzydziałowych, które promują lepszą współpracę i zrozumienie między zespołami IT, bezpieczeństwa, operacji i innymi kluczowymi działami, pozwala na lepsze zrozumienie wspólnych celów i zwiększa efektywność w zarządzaniu ryzykiem. Korzystanie z zewnętrznych ekspertów i współpraca z instytucjami akademickimi czy branżowymi wzbogaca programy

szkoleniowe o nowe perspektywy i najnowszą wiedzę. Te zmiany mają na celu nie tylko zwiększenie świadomości i gotowości pracowników na różne zagrożenia, ale również rozwijanie kultury bezpieczeństwa na wszystkich poziomach organizacji, co jest niezbędne dla zapewnienia długoterminowej ochrony i odporności przedsiębiorstwa w dynamicznie zmieniającym się świecie usług informacyjno-komunikacyjnych, gdzie nowe technologie i metody ataków pojawiają się regularnie.

Ekspert 4.

W dynamicznie zmieniającym się środowisku zagrożeń oraz w obliczu szybkiego rozwoju technologicznego, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych muszą nieustannie dostosowywać swoje programy szkoleniowe dla pracowników. Istotne jest rozszerzenie treści programów szkoleniowych o najnowsze zagrożenia cybernetyczne, metody ataków i techniki obronne, przy czym szkolenia te powinny być regularnie aktualizowane, aby odzwierciedlać ewoluujące techniki ataków i obrony. Ważne jest także wprowadzenie większej liczby ćwiczeń praktycznych i symulacji ataków, które pozwolą pracownikom lepiej zrozumieć, jak reagować w realnych scenariuszach zagrożeń, z możliwością zastosowania grywalizacji dla zwiększenia zaangażowania i skuteczności nauki. Szkolenia powinny być dostosowane do różnych grup pracowników w zależności od ich roli i poziomu dostępu do poufnych informacji, a treści szkoleniowe powinny być personalizowane. Ważne jest również włączenie modułów dotyczących bezpieczeństwa fizycznego, które obejmują procedury dostępu i ochronę przed nieautoryzowanym dostępem do pomieszczeń. Ponadto, każdy pracownik powinien być świadomy przepisów dotyczących ochrony danych, takich jak GDPR, oraz ich roli w ochronie danych osobowych klientów. Rozwój umiejętności miękkich, takich jak zarządzanie stresem, rozwiązywanie konfliktów czy komunikacja kryzysowa, również powinien być elementem szkoleń, gdyż są one niezbędne podczas zarządzania incydentami bezpieczeństwa. Wykorzystanie platform e-learningowych umożliwia ciągły dostęp do materiałów szkoleniowych i pozwala pracownikom na samodzielny rozwój w interesujących ich obszarach bezpieczeństwa. Wprowadzenie mechanizmów zbierania opinii od pracowników na temat szkoleń oraz regularna ocena efektywności programów szkoleniowych pozwoli na dostosowywanie ich do zmieniających się potrzeb i oczekiwań. Implementacja tych zmian pozwoli przedsiębiorstwu sektora technologii informacyjno-komunikacyjnych lepiej przygotować się do stawienia czoła współczesnym wyzwaniom w dziedzinie bezpieczeństwa, a pracownicy będą bardziej świadomi potencjalnych zagrożeń i sposobów ich przeciwdziałania.

Ekspert 5.

W dobie dynamicznie rozwijających się technologii i wzrostu zagrożeń cybernetycznych, kluczową rolę w ochronie bezpieczeństwa informacji odgrywa ciągłe szkolenie i doskonalenie pracowników przedsiębiorstw sektora technologii informacyjno-komunikacyjnych. Niezwykle ważne jest, aby programy szkoleniowe były regularnie aktualizowane i dostosowywane do ewoluującego środowiska zagrożeń. Powinny one obejmować podnoszenie świadomości na temat cyberbezpieczeństwa, co pozwoli pracownikom zrozumieć zagrożenia cyfrowe, nauczyć się jak identyfikować potencjalne wektory ataku i jak zabezpieczyć swoje urządzenia oraz dane. Programy szkoleniowe powinny być zróżnicowane w zależności od roli i odpowiedzialności pracownika, od głębokiej wiedzy technicznej dla techników i administratorów, po szkolenia

z ochrony danych osobowych dla personelu obsługującego klientów. Istotne jest wprowadzenie praktycznych elementów takich jak warsztaty czy symulacje ataków, które umożliwią pracownikom lepsze zrozumienie zagrożeń i metod reagowania na incydenty. Przedsiębiorstwo powinno organizować cykliczne szkolenia aktualizacyjne, aby na bieżąco dostosowywać wiedzę pracowników do nowych technologii i zagrożeń. Warto również współpracować z ekspertami zewnętrznymi, aby pracownicy mogli czerpać z doświadczeń liderów branży i stosować najlepsze praktyki. Promowanie kultury bezpieczeństwa w organizacji jako wspólnej odpowiedzialności wszystkich pracowników, a nie tylko działu IT, jest niezbędne do budowania silnych fundamentów cyberbezpieczeństwa. Implementacja tych inicjatyw pozwoli przedsiębiorstwu sektora technologii informacyjno-komunikacyjnych znacząco zwiększyć ochronę przed cyfrowymi zagrożeniami.

Ekspert 6.

W kontekście szkolenia i doskonalenia pracowników przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych, istnieje kilka kluczowych zmian, które mogłyby znacząco poprawić poziom świadomości i bezpieczeństwa w firmie. Szkolenia z bezpieczeństwa cybernetycznego powinny być regularne i kompleksowe, uwzględniające najnowsze zagrożenia, techniki ataku oraz metody obrony, dostosowane do różnych poziomów umiejętności i specyficznych ról w firmie. Zastosowanie interaktywnych metod nauczania, takich jak symulacje cyberataków, gry edukacyjne czy warsztaty praktyczne, może zwiększyć zaangażowanie i zrozumienie zagadnień bezpieczeństwa przez pracowników. Organizowanie kontrolowanych ataków symulacyjnych, znanych jako Red Teaming Exercises, pozwoli pracownikom doświadczyć realistycznych scenariuszy ataku, a następnie każda symulacja powinna być dokładnie analizowana, a wnioski omawiane z pracownikami, by wprowadzić potrzebne zmiany w procedurach i zabezpieczeniach. Kluczowe jest również wzmocnienie procedur raportowania, poprzez uproszczenie procedur zgłaszania podejrzanych działań, co umożliwi każdemu pracownikowi zrozumienie, jak i gdzie zgłosić podejrzaną wiadomość czy działanie. Można też wprowadzić system nagród dla pracowników, którzy skutecznie identyfikują zagrożenia, co może zachęcić do większej czujności i zaangażowania w procesy bezpieczeństwa. Ponadto, cykliczne przeglądy i aktualizacje szkoleniowe są niezbędne, aby materiały szkoleniowe odzwierciedlały najnowsze zagrożenia i najlepsze praktyki w branży, a szkolenia prowadzone przez zewnętrznych ekspertów i specjalistów mogą wprowadzić nowe perspektywy i wiedzę do organizacji.

Ekspert 7.

Przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych mają obowiązek nauczyć swoich pracowników o specyfikach usług, ponieważ instytucje edukacyjne często nie zapewniają takiej wiedzy. Jest to szczególnie ważne, aby personel był świadomy zarówno procesów biznesowych organizacji, jak i jego roli w ich ramach, co nie jest standardowo omawiane w szkołach. Szkolenia powinny również obejmować zagadnienia związane z cyberbezpieczeństwem, jak phishing, aby pracownicy wiedzieli, jak rozpoznawać i zapobiegać takim zagrożeniom. Kolejnym kluczowym elementem jest edukacja o ochronie danych osobowych zgodnie z RODO, co jest niezwykle istotne w branżach, gdzie pracownicy mają

dostęp do wrażliwych danych klientów. Edukacja powinna również obejmować naukę o narzędziach i metodologiach projektowych, które są używane w firmie, a także o specjalistycznych technologiach i obszarach, takich jak zarządzanie informacjami poufnymi. Ważne jest także szkolenie z zarządzania stresem i radzenia sobie w sytuacjach kryzysowych, ucząc pracowników rozpoznawania, co stanowi kryzys bezpieczeństwa informacji, a co nie. Pracodawcy powinni zapewnić, że pracownicy na wszystkich etapach kariery otrzymują potrzebne szkolenia, aby właściwie przygotować ich do przyszłych wyzwań zawodowych. To wszechstronne podejście do szkoleń pomoże pracownikom lepiej zrozumieć swoje role i obowiązki oraz zapewni przedsiębiorstwom lepszą ochronę przed różnymi zagrożeniami.

Ekspert 8.

W zakresie szkolenia i doskonalenia pracowników przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych, kluczowe jest uwzględnienie nowoczesnych metod szkoleniowych, które skupiają się na realistycznych symulacjach i warsztatach praktycznych. Powinno się zwiększyć nacisk na edukację dotyczącą najnowszych zagrożeń cybernetycznych, technik obronnych oraz metod reagowania na incydenty. Warto również wdrożyć programy świadomości bezpieczeństwa, które regularnie aktualizowane są o najnowsze informacje z branży. Pracownicy powinni być także szkoleni w zakresie korzystania z narzędzi analitycznych i technologii szyfrowania, co zwiększy ich zdolność do ochrony danych przedsiębiorstwa. Ważne jest, aby szkolenia były dopasowane do roli i odpowiedzialności każdego pracownika, zwiększając ich skuteczność.

Ekspert 9.

Wzmocnienie szkoleń z zakresu bezpieczeństwa osobowego jest niezbędne. Szkolenia powinny koncentrować się na rozwijaniu umiejętności rozpoznawania potencjalnych zagrożeń wewnętrznych i zewnętrznych, a także na uczciwości i etyce zawodowej. Pracownicy powinni być nauczani, jak rozpoznawać i reagować na sygnały ostrzegawcze dotyczące szpiegostwa korporacyjnego i innych form nadużyć. Wprowadzenie regularnych warsztatów dotyczących przeciwdziałania manipulacji i socjotechniki może również pomóc w zwiększeniu odporności na próby wywiadu gospodarczego. Kluczowe jest, aby każdy pracownik znał procedury zgłaszania podejrzanych działań i czuł się odpowiedzialny za bezpieczeństwo przedsiębiorstwa.

Ekspert 10.

Szkolenie w zakresie bezpieczeństwa fizycznego powinno obejmować bardziej szczegółowe procedury dotyczące kontroli dostępu do infrastruktury i monitorowania obiektów. Należy wprowadzić regularne ćwiczenia praktyczne, które pomogą pracownikom zrozumieć, jak skutecznie zabezpieczyć fizyczne zasoby przedsiębiorstwa przed nieautoryzowanym dostępem. Szkolenia powinny również obejmować zarządzanie sytuacjami kryzysowymi, w tym ewakuację, reakcje na alarmy bezpieczeństwa oraz procedury postępowania w przypadku naruszeń bezpieczeństwa. Ważne jest także, aby pracownicy mieli regularny dostęp do informacji o nowych technologiach bezpieczeństwa fizycznego i byli świadomi najlepszych praktyk w zakresie ochrony infrastruktury.

Ekspert 11.

W zakresie szkolenia i doskonalenia pracowników przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych, konieczne jest wprowadzenie bardziej zróżnicowanych i zaawansowanych programów edukacyjnych, które uwzględniają najnowsze zagrożenia i technologie. Przede wszystkim, szkolenia powinny być regularne i obowiązkowe dla wszystkich pracowników, z uwzględnieniem ich specyficznych ról i obowiązków. Powinny one obejmować szczegółowe wyjaśnienia dotyczące wektorów ataków oraz sposobów ich przeprowadzania, co jest kluczowe dla zwiększenia świadomości zagrożeń. Ważnym elementem jest również wprowadzenie interaktywnych metod nauczania, takich jak symulacje cyberataków i gry edukacyjne, które angażują uczestników i ułatwiają przyswajanie wiedzy. Dodatkowo, warto inwestować w zaawansowane szkolenia techniczne dla zespołów IT i bezpieczeństwa, aby były one na bieżąco z najnowszymi narzędziami i technologiami ochrony.

Ekspert 12.
Aby skutecznie poprawić szkolenie i doskonalenie pracowników w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych, konieczne jest wprowadzenie bardziej kompleksowych i praktycznych programów edukacyjnych. Szkolenia powinny zaczynać się już na etapie rekrutacji, aby budować świadomość bezpieczeństwa od pierwszych dni pracy. Regularne kampanie testowe, które symulują rzeczywiste ataki, mogą znacząco zwiększyć czujność pracowników i sprawdzić skuteczność istniejących procedur bezpieczeństwa. Ponadto, należy rozwijać programy szkoleniowe, które koncentrują się na rozpoznawaniu i reagowaniu na ataki socjotechniczne, takie jak phishing, oraz na praktykach bezpiecznego korzystania z technologii. Wprowadzenie systemu nagradzania pracowników za proaktywne zachowania związane z bezpieczeństwem może również zwiększyć zaangażowanie i odpowiedzialność. Kluczowe jest również ciągłe doskonalenie umiejętności poprzez udział w konferencjach branżowych, warsztatach oraz współpracę z zewnętrznymi ekspertami ds. cyberbezpieczeństwa, co pozwala na wymianę wiedzy i najlepszych praktyk.

l)

Jakie zmiany należałoby wprowadzić w obszarze organizacyjnym przedsiębiorstwa?

Ekspert 1.
Obecnie funkcjonujące zabezpieczenia w przedsiębiorstwie nie budzą żadnych zastrzeżeń. Jedyny element, na który należy zwrócić szczególną uwagę, w przypadku budowania takiego systemu w organizacji, to efektywniejsza korelacja danych gromadzonych na urządzeniach końcowych z regułami bezpieczeństwa oraz polityką bezpieczeństwa przedsiębiorstwa. Ponadto dane te powinny być odpowiednio przetworzone, tak aby skrócić czas reakcji na incydent bezpieczeństwa oraz uzyskać możliwie szeroką informację na temat jego charakteru, źródła i ewentualnego celu. Budowanie świadomości pracowników powinno zaczynać się już na etapie rekrutacji, zatem istotną rolę odgrywa właściwa polityka kadrowa. Odpowiedni proces selekcji kandydatów na dane stanowisko, a następnie zapewnienie im szerokiego spektrum szkoleń dotyczących bezpieczeństwa i zagrożeń przedsiębiorstwa.

Ekspert 2.
Jestem przekonany, że powinna istnieć jednolita regulacja w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych dotycząca przetwarzania informacji niejawnych.

Obecnie obowiązujące przepisy dotyczące tych informacji wymagają posiadania określonych certyfikatów bezpieczeństwa i innych uprawnień. Jednakże, ustawodawcy zdają się nie do końca rozumieć, że wiele informacji uznawanych za niejawne, wewnątrz organizacji są to po prostu dane informacyjno-komunikacyjne dostępne dla personelu obsługującego klientów, pracowników CRM czy działu rozliczeniowego – czyli są jawne dla osób z właściwymi uprawnieniami w firmie. Dlatego ważne byłoby, aby ktoś jednoznacznie określił, że tak naprawdę niejawne są wnioski, cele i kontekst przetwarzania tych informacji, a nie same gromadzone dane przekazywane w ramach zapytań uprawnionych podmiotów. Taka zmiana regulacyjna przyniosłaby wiele korzyści w przedsiębiorstwie np. przyczyniłaby się do łatwiejszego funkcjonowania przedsiębiorstwa. Podsumowując, definicja informacji niejawnych powinna obejmować to, kto i w jakim celu składa wniosek, a nie same gromadzone dane, które są w praktyce dostępne dla wielu pracowników w firmie w ramach innych/standardowych procesów. Uproszczenie definicji i w efekcie wewnętrznych procesów/procedur przyczyniłoby się do efektywniejszego funkcjonowania przedsiębiorstwa, bez uszczerbku dla procesów po stronie organów państwowych.

Ekspert 3.

W kontekście zapewnienia cyberbezpieczeństwa i ochrony przed szpiegostwem korporacyjnym, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych muszą podejmować kluczowe zmiany organizacyjne, które wzmacniają ich struktury zarządzania, procesy wewnętrzne oraz kulturę organizacyjną. Wprowadzenie dedykowanych stanowisk i działów zajmujących się cyberbezpieczeństwem, z jasno określonymi rolami i odpowiedzialnościami, jest niezbędne. Osoba na stanowisku Chief Information Security Officer powinna być odpowiedzialna za strategię bezpieczeństwa na najwyższym szczeblu zarządzania. Zintegrowanie kwestii bezpieczeństwa z kluczowymi procesami biznesowymi jest kluczowe, aby decyzje biznesowe uwzględniały aspekty bezpieczeństwa informacji i ryzyka cybernetycznego. Równie ważne jest budowanie świadomości i kultury bezpieczeństwa na wszystkich poziomach organizacji, co można osiągnąć poprzez regularne szkolenia, kampanie informacyjne oraz promowanie odpowiedzialności za ochronę danych i systemów. Dodatkowo, ustanowienie procesów ciągłego doskonalenia bezpieczeństwa, opartych na cyklu Plan-Do-Check-Act, umożliwi systematyczną ocenę i ulepszanie środków ochrony, polityk i procedur. Opracowanie zaawansowanego systemu zarządzania ryzykiem pozwoli na identyfikację, analizę i minimalizację ryzyk cybernetycznych i powinno być zintegrowane z ogólnym systemem zarządzania ryzykiem przedsiębiorstwa. Wzmocnienie współpracy i komunikacji między działami IT, bezpieczeństwa, prawnym, HR oraz innymi kluczowymi działami jest istotne dla lepszego zrozumienia i efektywnego zarządzania zagrożeniami dla bezpieczeństwa. Opracowanie i regularne testowanie planów ciągłości działania oraz reagowania na incydenty cyberbezpieczeństwa zapewni, że przedsiębiorstwo będzie przygotowane na różne scenariusze, w tym ataki cybernetyczne, utratę danych lub awarie infrastruktury. Kluczowe jest również systematyczne inwestowanie w nowoczesne technologie i narzędzia wspierające cyberbezpieczeństwo oraz rozwój kompetencji i umiejętności pracowników w zakresie obsługi tych narzędzi. Te zmiany mają na celu nie tylko zwiększenie odporności organizacji na zagrożenia i ataki cybernetyczne, ale również budowanie zrównoważonej i elastycznej struktury

organizacyjnej, zdolnej do szybkiego reagowania na zmieniające się otoczenie biznesowe i technologiczne. Integracja bezpieczeństwa na wszystkich poziomach organizacji oraz ciągłe doskonalenie praktyk i procesów są kluczem do zapewnienia długoterminowej ochrony przedsiębiorstwa.

Ekspert 4.

W ramach przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych, aby podnieść efektywność zarządzania bezpieczeństwem informacji, istotne są pewne modyfikacje w strukturze organizacyjnej i procesach. Kluczowe jest wzmocnienie funkcji bezpieczeństwa poprzez utworzenie lub rozwinięcie stanowisk dedykowanych temu obszarowi, jak dyrektor ds. bezpieczeństwa informacji, który miałby wyraźnie zdefiniowane obowiązki i szerokie uprawnienia, a także bezpośredni dostęp do najwyższego kierownictwa. Ważna jest również integracja kwestii bezpieczeństwa z codziennymi procesami biznesowymi, takimi jak rozwój produktu, jego wdrażanie, wsparcie klienta i utrzymanie. Promowanie kultury bezpieczeństwa poprzez regularne szkolenia i kampanie świadomościowe jest niezbędne do budowania świadomości bezpieczeństwa wśród pracowników. Dodatkowo, istotne jest wprowadzenie rygorystycznych procedur oceny dostawców i partnerów biznesowych pod kątem ich praktyk bezpieczeństwa, co powinno obejmować regularne audyty i oceny zgodności z wymogami bezpieczeństwa. Ulepszenie procesów zarządzania ryzykiem, opracowanie szczegółowych planów reagowania na incydenty bezpieczeństwa oraz ich regularne ćwiczenia to kolejne kroki ku zwiększeniu bezpieczeństwa. Znaczące są również inwestycje w zaawansowane narzędzia i technologie, które wspierają ochronę, a także regularny przegląd i aktualizacja polityk bezpieczeństwa, aby te skutecznie odpowiadały na zmieniające się zagrożenia. Zachęcanie do współpracy międzydziałowej, włączając dział IT, bezpieczeństwa, prawny, HR i inne kluczowe działy, jest fundamentem dla spójnego podejścia do zarządzania bezpieczeństwem. Dodatkowo, zarządzanie zmianą powinno być prowadzone w sposób, który minimalizuje wprowadzenie nowych zagrożeń podczas aktualizacji systemów czy wprowadzania nowych technologii. Wdrożenie tych zmian wymaga zaangażowania na najwyższych szczeblach zarządzania oraz ciągłej gotowości organizacji do adaptacji i doskonalenia praktyk bezpieczeństwa w odpowiedzi na dynamicznie zmieniające się zagrożenia.

Ekspert 5.

W odpowiedzi na rosnące zagrożenia dla bezpieczeństwa informacji, przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych stają przed koniecznością dokonania strategicznych zmian w swoich strukturach organizacyjnych, mających na celu zwiększenie skuteczności działań zabezpieczających oraz promowanie kultury organizacyjnej, w której cyberbezpieczeństwo jest traktowane jako priorytet. Niezbędne jest wzmocnienie roli bezpieczeństwa informacji poprzez utworzenie lub rozbudowę odpowiednich działów, z jasno określoną rolą, odpowiedzialnościami i uprawnieniami. Istotne staje się również powołanie wysokiego rangą oficera ds. bezpieczeństwa informacji, który będzie miał bezpośrednie połączenie z najwyższym kierownictwem. Bezpieczeństwo musi być integralną częścią wszystkich procesów biznesowych, co wymaga ścisłej współpracy między działami IT, bezpieczeństwa i resztą organizacji. Ważne jest także wdrożenie zintegrowanych systemów zarządzania bezpieczeństwem, takich jak ISO 27001, oraz rozwijanie organizacyjnej kultury bezpieczeństwa poprzez regularne szkolenia i kampanie informacyjne. Kluczowe jest również

wprowadzenie wyraźnych procedur reagowania na incydenty oraz zwiększenie zdolności do szybkiego reagowania na zagrożenia. Ponadto, niezbędna jest współpraca z innymi przedsiębiorstwami, instytucjami i organami ścigania, a także rygorystyczna ocena bezpieczeństwa dostawców i partnerów biznesowych. Takie podejście, wymagające zaangażowania na najwyższych szczeblach zarządzania i ścisłej współpracy między działami, jest kluczowe dla skutecznego zarządzania bezpieczeństwem informacji, które jest procesem ciągłym i musi być ciągle dostosowywane do zmieniającego się środowiska zagrożeń.

Ekspert 6.

W odpowiedzi na pytanie dotyczące zmian organizacyjnych w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych, które mogłyby poprawić zarządzanie bezpieczeństwem i efektywność operacyjną, należy zwrócić uwagę na kilka kluczowych obszarów. Po pierwsze, ważne jest wdrożenie bardziej zaawansowanych systemów SIEM (Security Information and Event Management), które umożliwiają efektywniejszą korelację danych z różnych źródeł. Systemy te, analizujące duże ilości danych w czasie rzeczywistym, mogą znacząco skrócić czas reakcji na incydenty bezpieczeństwa. Implementacja zautomatyzowanych protokołów odpowiedzi, które mogą wykrywać, izolować i neutralizować zagrożenia bez konieczności interwencji człowieka, również pomoże w jeszcze szybszym reagowaniu na potencjalne ataki. Wzmocnienie polityki kadrowej poprzez wprowadzenie bardziej rygorystycznych procedur weryfikacji kandydatów, w tym sprawdzeń tła oraz ocen kompetencji technicznych i zrozumienia najlepszych praktyk bezpieczeństwa, jest równie kluczowe. Organizacja regularnych szkoleń z zakresu bezpieczeństwa cyfrowego, prawnych aspektów ochrony danych i reagowania na incydenty dla wszystkich pracowników, dostosowanych do różnych poziomów odpowiedzialności i ryzyka związanego z danym stanowiskiem, również przyczyni się do podniesienia świadomości bezpieczeństwa. Ponadto, utworzenie lub rozbudowa Centrum Operacyjnego Bezpieczeństwa (SOC), które będzie nie tylko monitorować bezpieczeństwo na bieżąco, ale również analizować trendy, raportować i zarządzać wiedzą na temat zagrożeń, pomoże w lepszym zarządzaniu wiedzą i informacją. Zapewnienie, że wszystkie informacje dotyczące bezpieczeństwa są łatwo dostępne dla odpowiednich osób i że istnieją jasne procedury raportowania wszelkich zagrożeń czy incydentów, również jest istotne. Budowanie kultury bezpieczeństwa na wszystkich poziomach organizacji, poprzez kampanie wewnętrzne, regularne przypomnienia, eventy edukacyjne i treningi, zwiększy świadomość i odpowiedzialność za bezpieczeństwo. Regularne audyty i oceny ryzyka, systematyczne przeglądy i aktualizacje polityk bezpieczeństwa oraz oceny skuteczności wprowadzonych środków, upewnią, że przedsiębiorstwo nadąża za szybko zmieniającym się krajobrazem zagrożeń cybernetycznych.

Ekspert 7.

Istnieje przekonanie, że w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych powinna obowiązywać jednolita regulacja dotycząca przetwarzania informacji niejawnych. Obowiązujące obecnie przepisy wymagają od firm posiadania określonych certyfikatów bezpieczeństwa i innych uprawnień, które regulują dostęp do takich danych. Ustawodawcy jednak nie zawsze zdają sobie sprawę, że informacje uznawane za niejawne, takie jak dane informacyjno-komunikacyjne wykorzystywane przez personel obsługujący klientów czy pracowników działów CRM i rozliczeniowych, są de facto dostępne

dla osób posiadających odpowiednie uprawnienia wewnątrz organizacji. Z tego względu korzystne byłoby, gdyby wprowadzono regulacje precyzyjnie określające, że za informacje niejawne uważa się wnioski, cele i kontekst przetwarzania tych informacji, a nie same dane przekazywane w ramach zapytań autoryzowanych podmiotów. Takie podejście nie tylko uprościłoby wewnętrzne procedury i procesy w przedsiębiorstwach, ale również przyczyniłoby się do ich efektywniejszego funkcjonowania. Prostsza definicja informacji niejawnych, skoncentrowana na celach i kontekście ich przetwarzania, a nie na samych danych, umożliwiłaby lepsze zarządzanie tymi informacjami bez negatywnego wpływu na współpracę z organami państwowymi.

Ekspert 8.

Wprowadzenie zmian w obszarze organizacyjnym przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych powinno koncentrować się na lepszej integracji działów IT z innymi segmentami przedsiębiorstwa. Wzmocnienie współpracy między tymi działami może prowadzić do bardziej efektywnego zarządzania ryzykiem i szybszego reagowania na incydenty bezpieczeństwa. Istotne byłoby również formalne ustanowienie ról odpowiedzialnych za cyberbezpieczeństwo na wszystkich szczeblach zarządzania, co pozwoli na lepszą komunikację i zrozumienie priorytetów bezpieczeństwa w całej organizacji.

Ekspert 9.

Reorganizacja struktur zarządzania bezpieczeństwem wewnątrz przedsiębiorstwa może przyczynić się do lepszej ochrony przed zagrożeniami wewnętrznymi i zewnętrznymi. Należy wprowadzić regularne szkolenia dotyczące bezpieczeństwa dla wszystkich poziomów zarządzania oraz pracowników, zwiększając ich świadomość i zaangażowanie w procesy bezpieczeństwa. Ponadto, stworzenie jasnych procedur zgłaszania i reagowania na incydenty bezpieczeństwa jest kluczowe dla szybkiego i skutecznego adresowania problemów.

Ekspert 10.

Zmiany organizacyjne powinny również obejmować rozwój i wdrożenie zintegrowanych systemów zarządzania bezpieczeństwem fizycznym, które połączą technologie monitoringu, kontroli dostępu i reagowania na incydenty. Wzmocnienie współpracy między działami technicznymi a operacyjnymi pozwoli na lepsze zrozumienie potrzeb i zagrożeń specyficznych dla różnych obszarów przedsiębiorstwa, co jest kluczowe dla zapewnienia ciągłości operacyjnej i minimalizacji skutków ewentualnych naruszeń bezpieczeństwa.

Ekspert 11.

W obszarze organizacyjnym przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych należy wprowadzić kilka kluczowych zmian, które mogą znacząco poprawić zarządzanie bezpieczeństwem informacji. Przede wszystkim, istotne jest stworzenie dedykowanego zespołu ds. bezpieczeństwa, który będzie odpowiedzialny za monitorowanie i analizowanie zagrożeń w czasie rzeczywistym. Taki zespół powinien korzystać z zaawansowanych narzędzi analitycznych i systemów SIEM (Security Information and Event Management) do korelacji danych gromadzonych na urządzeniach końcowych z regułami

bezpieczeństwa oraz polityką bezpieczeństwa przedsiębiorstwa. Regularne przeglądy i aktualizacje polityk bezpieczeństwa powinny być przeprowadzane w oparciu o nowe zagrożenia i zmieniające się technologie. Wdrożenie bardziej zaawansowanych systemów automatyzacji reakcji na incydenty, które mogą skrócić czas reakcji na incydent bezpieczeństwa i dostarczyć szerokie informacje na temat jego charakteru, źródła i ewentualnego celu, jest również kluczowe.

Ekspert 12.

W obszarze organizacyjnym przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych ważne jest wprowadzenie zmian, które wzmocnią politykę kadrową i procesy zarządzania personelem. Budowanie świadomości pracowników na temat bezpieczeństwa informacji powinno zaczynać się już na etapie rekrutacji, dlatego istotne jest wprowadzenie bardziej rygorystycznych procedur selekcji kandydatów, które uwzględniają oceny ryzyka i bezpieczeństwa. Wprowadzenie szerokiego spektrum szkoleń dotyczących bezpieczeństwa i zagrożeń przedsiębiorstwa jest kluczowe. Ponadto, powinno się zwiększyć nacisk na monitorowanie zachowań pracowników oraz wprowadzenie procedur, które pozwalają na szybkie wykrywanie i raportowanie podejrzanych działań. Regularne przeglądy uprawnień dostępowych oraz systematyczne audyty bezpieczeństwa pomogą w identyfikacji i eliminacji potencjalnych luk w zabezpieczeniach. Warto również rozważyć wdrożenie polityk rotacji stanowisk i obowiązków, co może pomóc w ograniczeniu ryzyka związanego z długoterminowym dostępem pracowników do krytycznych informacji. Wreszcie, integracja technologii takich jak systemy DLP (Data Loss Prevention) i zaawansowane monitorowanie sieci może znacząco zwiększyć poziom ochrony danych i zapobiegać nieautoryzowanemu dostępowi oraz wyciekom informacji.

Załącznik nr 2

KWESTIONARIUSZ ANKIETY NA TEMAT:

„PROBLEMATYKA SZPIEGOSTWA KORPORACYJNEGO W PRZEDSIĘBIORSTWIE SEKTORA TECHNOLOGII INFORMACYJNO-KOMUNIKACYJNYCH”

Szanowni Państwo,

zwracam się z prośbą o uzupełnienie kwestionariusza ankiety nt. „Problematyka szpiegostwa korporacyjnego w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych”.

Uzyskane odpowiedzi w formie zbiorczej zostaną wykorzystane do opracowania wniosków w ramach pracy doktorskiej dotyczącej zarządzania bezpieczeństwem przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych w kontekście zagrożenia szpiegostwem korporacyjnym.

Ankieta skierowana jest do osób zatrudnionych w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych, które działają na terenie Polski. Udział w badaniu jest dobrowolny i anonimowy. Uzyskane odpowiedzi będą traktowane w pełni poufnie.

Proszę o zaznaczenie Państwa odpowiedzi bądź wpisanie odpowiedzi w wyznaczonym do tego celu miejscu.

Dziękuję za uzupełnienie kwestionariusza ankiety.

1. Proszę o wskazanie organizacji, w której jest Pani/Pan zatrudniona/y.

(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Netia.
2) Orange.
3) Play.
4) Plus.
5) T-Mobile.
6) Vectra.
7) Inny – jaki? ……..

2. Proszę o wskazanie swojego wieku.

(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) do 30 lat.
2) 31-40 lat.
3) 41-50 lat.
4) 51-60 lat.
5) powyżej 60 lat.

3. Proszę o wskazanie swojego stażu pracy.

(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) do 5 lat.
2) 6-10 lat.
3) 11-15 lat.
4) 16-20 lat.
5) powyżej 20 lat.

4. Proszę o wskazanie swojego wykształcenia.

(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Podstawowe.
2) Zawodowe.
3) Średnie.
4) Studia I stopnia.
5) Studia II stopnia.
6) Studia III stopnia.

5. Proszę o wskazanie swojego stanowiska.

(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Pracownik biurowy.
2) Asystent.
3) Specjalista.
4) Kierownictwo średniego szczebla (manager).
5) Kierownictwo wyższego szczebla (dyrektor).

6. Czy uważa Pani/Pan, że szpiegostwo korporacyjne stanowi zagrożenie dla przedsiębiorstwa, w którym jest Pani/Pan zatrudniona/y?
(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Zdecydowanie się nie zgadzam.
2) Nie zgadzam się.
3) Nie mam zdania.
4) Zgadzam się.
5) Zdecydowanie się zgadzam.

7. Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y podjęła odpowiednie środki w celu ochrony przed szpiegostwem korporacyjnym?
(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Zdecydowanie się nie zgadzam.
2) Nie zgadzam się.
3) Nie mam zdania.
4) Zgadzam się.
5) Zdecydowanie się zgadzam.

8. Czy uważa Pani/Pan, że regulacje i procedury w organizacji, w której jest Pani/Pan zatrudniona/y są skuteczne w wykrywaniu i zapobieganiu zjawisku szpiegostwa korporacyjnego?
(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Zdecydowanie się nie zgadzam.
2) Nie zgadzam się.
3) Nie mam zdania.
4) Zgadzam się.
5) Zdecydowanie się zgadzam.

9. Czy uważa Pani/Pan, że przeprowadzanie kontroli przeszłości pracowników i dostawców może pomóc zmniejszyć ryzyko zjawiska szpiegostwa korporacyjnego?
(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Zdecydowanie się nie zgadzam.
2) Nie zgadzam się.
3) Nie mam zdania.
4) Zgadzam się.
5) Zdecydowanie się zgadzam.

10. Czy uważa Pani/Pan, że organizacja, w której jest Pani/Pan zatrudniona/y, jest przygotowana do reagowania na podejrzewany lub potwierdzony incydent szpiegostwa korporacyjnego?
(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Zdecydowanie się nie zgadzam.
2) Nie zgadzam się.
3) Nie mam zdania.
4) Zgadzam się.
5) Zdecydowanie się zgadzam.

11. Czy uważa Pani/Pan, że szkolenia i edukacja na temat szpiegostwa korporacyjnego są istotnym elementem dla pracowników i kontrahentów?
(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Zdecydowanie się nie zgadzam.
2) Nie zgadzam się..
3) Nie mam zdania.
4) Zgadzam się.
5) Zdecydowanie się zgadzam.

12. Czy uważa Pani/Pan, że działania prawne są skutecznym środkiem odstraszającym w kontekście zjawiska szpiegostwa korporacyjnego?
(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

6) Zdecydowanie się nie zgadzam.
7) Nie zgadzam się.
8) Nie mam zdania.
9) Zgadzam się.
10) Zdecydowanie się zgadzam.

13. Czy uważa Pani/Pan, że szpiegostwo korporacyjne jest rosnącym problemem w branży sektora technologii informacyjno-komunikacyjnych?
(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Zdecydowanie się nie zgadzam.

2) Nie zgadzam się.
3) Nie mam zdania.
4) Zgadzam się.
5) Zdecydowanie się zgadzam.

14. Czy uważa Pani/Pan, że środki bezpieczeństwa w organizacji, w której jest Pani/Pan zatrudniona/y, są wystarczające, aby chronić zarówno przed fizycznymi, jak i cyfrowymi zagrożeniami zjawiska szpiegostwa korporacyjnego?
(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Zdecydowanie się nie zgadzam.
2) Nie zgadzam się.
3) Nie mam zdania.
4) Zgadzam się.
5) Zdecydowanie się zgadzam.

15. Czy uważa Pani/Pan, że pracownicy i kontrahenci organizacji, w której jest Pani/Pan zatrudniona/y, są świadomi oznak i ryzyka związanego ze szpiegostwem korporacyjnym?
(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Zdecydowanie się nie zgadzam.
2) Nie zgadzam się.
3) Nie mam zdania.
4) Zgadzam się.
5) Zdecydowanie się zgadzam.

16. Czy uważa Pani/Pan, że system szkolenia i profilaktyka prowadzona przez organizację, w której jest Pani/Pan zatrudniona/y, są wystarczające w kontekście edukowania i profilaktyki na temat zjawiska szpiegostwa korporacyjnego?
(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Zdecydowanie się nie zgadzam.
2) Nie zgadzam się.
3) Nie mam zdania.
4) Zgadzam się.
5) Zdecydowanie się zgadzam.

17. Czy uważa Pani/Pan, że szkolenia prowadzone przez instytucje państwowe (np. Agencję Bezpieczeństwa Wewnętrznego, Policję lub inne podmioty odpowiedzialne za bezpieczeństwo) byłyby istotnym czynnikiem zwiększającym świadomość

pracowników i kontrahentów organizacji, w której jest Pani/Pan zatrudniona/y, na temat zjawiska szpiegostwa korporacyjnego?

(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Zdecydowanie się nie zgadzam.
2) Nie zgadzam się.
3) Nie mam zdania.
4) Zgadzam się.
5) Zdecydowanie się zgadzam.

18. Czy uważa Pani/Pan, że zjawisko szpiegostwa korporacyjnego powinno zostać zdefiniowane i uregulowane prawnie w celu skutecznego przeciwdziałania mu przez organy państwowe?

(proszę o zakreślenie numeru wybranej jednej odpowiedzi)

1) Zdecydowanie się nie zgadzam.
2) Nie zgadzam się.
3) Nie mam zdania.
4) Zgadzam się.
5) Zdecydowanie się zgadzam.

ABSTRACT

MANAGING ENTERPRISE SECURITY IN THE INFORMATION AND COMMUNICATION TECHNOLOGY SECTOR AND CORPORATE ESPIONAGE

Globalisation and the rapid advancement of technology have profoundly transformed the operational and competitive landscape for contemporary enterprises. These changes have introduced a wide range of risks that threaten organisational stability, performance, and competitive positioning. Among these, corporate espionage emerges as a particularly critical yet frequently underestimated challenge. Defined as the illegal acquisition of confidential information to gain a competitive advantage, corporate espionage encompasses deliberate actions targeting sensitive data such as strategies, technologies, production processes, financial records, and other critical corporate assets. Despite being historically recognised in forms such as industrial and economic espionage, the concept has gained unprecedented prominence in the digital era, where information is a cornerstone of organisational value and operational success.

The increasing reliance on digital technologies and the interconnectedness of global markets have magnified the risks associated with corporate espionage. This phenomenon has become a pressing issue for organisations across all industries, particularly those within the Information and Communication Technology (ICT) sector. Characterised by rapid innovation, high-value intellectual property, and unique technological solutions, ICT enterprises face significant exposure to espionage-related risks. Consequently, corporate espionage represents a multifaceted threat that undermines not only financial stability but also competitive advantage and organisational reputation. This research critically examines corporate espionage within the ICT sector in Poland, offering insights into its prevalence, methods, and consequences while proposing comprehensive countermeasures.

A central argument advanced in this dissertation is the pivotal role of employees in combating corporate espionage. Although advanced technological solutions are essential in securing organisational assets, human factors—such as awareness, education, and engagement—play an equally critical role. Gaps in employee understanding of espionage risks and insufficient knowledge of countermeasures weaken internal security systems, rendering organisations vulnerable to sophisticated attacks. The study highlights the importance of

integrating technical, organisational, and human-centric approaches in designing effective security management strategies.

The primary objective of this research is to develop a security management model tailored to the unique challenges faced by ICT enterprises, with a specific focus on addressing employees' diverse perceptions of espionage-related threats. The study's overarching aim is to enhance data protection and safeguard organisational secrecy in a manner that accounts for both technological and human factors. To achieve this, the following specific objectives were established:

1. **Identification of Security's Role in Corporate Management:** Recognising the strategic importance of security in maintaining organisational stability and achieving business objectives.
2. **Analysis of Challenges in Implementing Information Security Practices:** Exploring the barriers and prerequisites for adopting robust information security measures.
3. **Examination of Espionage Risks in the ICT Sector:** Investigating how corporate espionage influences security management practices in ICT enterprises.
4. **Assessment of Employee Awareness and its Impact on Security Management:** Evaluating the relationship between employee awareness of espionage risks and the effectiveness of security management systems.

This research defines its main problem as understanding the challenges posed by varying employee perceptions of corporate espionage threats in the management of security within ICT enterprises. To address this, a central hypothesis is proposed: effective security management in ICT enterprises must account for differences in employees' threat perceptions to address espionage risks comprehensively. Supporting hypotheses explore the role of rational decision-making, adherence to international standards, countermeasures against espionage techniques, and the integration of employee perspectives into security strategies.

The methodology adopted for this research involves a multifaceted approach, comprising literature reviews, expert interviews, survey-based research, and computational simulations. The study was conducted in five distinct stages:

1. **Literature Review:** An extensive review of existing scholarly and professional literature on corporate espionage, security management, and the ICT sector. This stage involved critical analysis and identification of key themes for further exploration.
2. **Expert Interviews:** Semi-structured interviews with 12 experts in organisational security, focusing on their insights into espionage threats and security practices within the ICT sector.

3. **Survey Research:** A comprehensive survey of 466 respondents across various organisational levels in selected ICT enterprises operating in Poland. The survey assessed perceptions of corporate espionage, response procedures, training practices, and the role of state institutions in addressing these threats.
4. **Model Development:** Based on empirical findings, a security management model was designed, integrating technical, procedural, and human-centric dimensions to address the identified challenges comprehensively.
5. **Computational Simulations:** Simulation-based validation of the proposed model, examining its effectiveness in real-world scenarios and optimising its implementation through iterative testing.

Key findings from the expert interviews and surveys reveal significant gaps in employees' understanding of espionage risks and their ability to respond effectively to incidents. While technical measures such as advanced firewalls, intrusion detection systems, and encryption protocols are widely adopted, the human element remains a critical vulnerability. Inadequate training, low levels of awareness, and inconsistent communication of security policies weaken the overall efficacy of organisational security measures.

The results underscore the importance of regular training, awareness campaigns, and simulated exercises to prepare employees for potential threats. Additionally, organisations must invest in advanced identity and access management systems, conduct periodic security audits, and adopt a proactive approach to policy updates in response to evolving threats. Collaboration with industry partners, technology providers, and governmental agencies is also essential for sharing threat intelligence and coordinating responses to espionage incidents.

The proposed security management model integrates these insights, offering a structured framework for ICT enterprises to enhance their resilience against espionage threats. The model emphasises the following core elements:

- **Educational Initiatives:** Regular training programmes to increase employee awareness of espionage risks and improve their capacity to identify and respond to threats.
- **Technological Solutions:** Deployment of state-of-the-art security infrastructure, including threat detection systems, encryption tools, and access control mechanisms.
- **Policy and Governance:** Development and enforcement of comprehensive security policies, aligned with international standards and best practices.
- **Monitoring and Evaluation:** Implementation of key performance indicators (KPIs) to assess the effectiveness of security measures and identify areas for improvement.

Computational simulations conducted during the research validate the model's effectiveness, demonstrating significant improvements in organisational resilience when its

components are applied holistically. Nine implementation scenarios were tested, each highlighting the importance of adapting the model to the specific needs and risk profiles of individual enterprises. The simulations also reveal the critical role of dynamic adaptation, enabling organisations to respond effectively to emerging threats in the rapidly evolving ICT environment.

This dissertation contributes to the field by presenting a comprehensive and empirically validated framework for managing security in ICT enterprises. It emphasises the need for an interdisciplinary approach, integrating technological, procedural, and human-centric elements to address the complex challenges posed by corporate espionage. The findings have practical implications for policymakers, business leaders, and security professionals, offering actionable insights for enhancing organisational resilience in an increasingly competitive and innovation-driven market.

The research concludes by emphasising the importance of fostering a culture of security within organisations. This involves not only investing in advanced technologies but also prioritising employee education, promoting cross-departmental collaboration, and maintaining alignment with international regulations and standards. Future research directions include exploring the role of artificial intelligence and machine learning in enhancing security management practices and examining the broader implications of corporate espionage in other high-risk sectors.

This study underscores that effective security management is a cornerstone of organisational stability and success in the ICT sector, providing a robust foundation for safeguarding valuable assets and ensuring long-term competitiveness in a rapidly changing global marketplace.