Załącznik 3

Do wniosku w sprawie nadania stopnia doktora habilitowanego

AUTOREFERAT

Przedstawiający opis dorobku naukowego, osiągnięć naukowych, dydaktycznych, organizacyjnych i zawodowych

dr Joanna Antczak

Wydział Bezpieczeństwa, Logistyki i Zarządzania

Wojskowa Akademia Techniczna w Warszawie

Warszawa, 2025

Spis treści

1. Imię i nazwisko

Joanna Antczak

Nazwisko rodowe: Kisiel
ORCID: https://orcid.org/0000-0001-5691-2525
Web of Science Researcher ID: NTQ-5378-2025

2. Posiadane dyplomy, stopnie naukowe lub artystyczne

2010 - **stopień doktora nauk ekonomicznych w dyscyplinie ekonomia**

- Akademia Finansów w Warszawie obecnie Akademia Finansów i Biznesu Vistula w Warszawie
- Tytuł rozprawy doktorskiej: *Wpływ controllingu na wyniki ekonomiczne przedsiębiorstw*
- Promotor: prof. dr hab. Aldon Zalewski
- Recenzenci:
  - prof. dr hab. Tadeusz Kamiński
  - prof. dr hab. Lech Kościelecki

2012 – Akademia Finansów w Warszawie obecnie Akademia Finansów i Biznesu Vistula w Warszawie

- Dwusemestralne Studia Podyplomowe w zakresie Rachunkowości

2007 –Wyższa Szkoła Pedagogiczna Związku Nauczycielstwa Polskiego w Warszawie

- Trzysemestralne Studia Podyplomowe w zakresie Pedagogiki dla nauczycieli bez przygotowania pedagogicznego

1999-2001 - **tytuł zawodowy magister**

- Wyższa Szkoła Ubezpieczeń i Bankowości w Warszawie Wydział Uzupełniających Studiów Magisterskich obecnie Akademia Finansów i Biznesu Vistula w Warszawie
- Kierunek: Finanse i Bankowość, Specjalność: Bankowość
- Temat pracy: *Sprawozdawczość finansowa jako element efektywnościowego badania funkcjonowania banku komercyjnego*
- promotor: dr Ireneusz Badowski

3. Informacja o dotychczasowym zatrudnieniu w jednostkach naukowych lub artystycznych

Podstawowe miejsce pracy w jednostce naukowej:

Od 10.2021 r. **Wojskowa Akademia Techniczna** w Warszawie, adiunkt badawczo-dydaktyczny Instytutu Zarządzania, Wydziału Bezpieczeństwa, Logistyki i Zarządzania

- od 05.2025 r. Członek zespołu do opracowania zasad wdrożenia AI na Wydziale Bezpieczeństwa, Logistyki i Zarządzania w obszarze działalności naukowej

- od 12.2024 r. Zastępca Dyrektora Instytutu Zarządzania ds. naukowych
- od 11.2024 r. Członek zespołu do opracowania III kryterium ewaluacji działalności naukowej za lata 2022-2025

02.2018 r. - 09.2021 r. **Akademia Sztuki Wojennej** w Warszawie, adiunkt badawczo-dydaktyczny Wydziału Zarządzania i Dowodzenia

- w roku akademickim: 2018/2019 Opiekun Koła Naukowego Studentów Logistyki ASzWoj

10.2015 r. - 01.2018 r. **Wojskowa Akademia Techniczna** w Warszawie, adiunkt Instytutu Organizacji i Zarządzania Wydziału Cybernetyki

10.2006 r. – 09.2015 r. **Akademia Finansów i Biznesu Vistula** w Warszawie, adiunkt Wydziału Biznesu i Stosunków Międzynarodowych

- 02.2014 – 09.2015 Prodziekan Wydziału Biznesu i Stosunków Międzynarodowych
- 02.2013 – 01.2014 Prodziekan Wydziału Biznesu
- 10.2010 – 01.2013 Prodziekan Wydziału Ekonomicznego
- 02.2013 – 01.2014 Kierownik Katedry Finansów i Rachunkowości
- 10.2010 – 01.2013 Opiekun specjalności Rachunkowość
- 10.2010 – 09.2015 Opiekun merytoryczny studiów podyplomowych w zakresie rachunkowości oraz audytu i kontroli wewnętrznej
- 10.2006 – 10.2010 asystent w Katedrze Rachunkowości

Dodatkowe miejsca pracy w jednostkach naukowych:

Od 10.2019	Pracownik dydaktyczny Akademii WIT w Warszawie
Od 05.2024	Pracownik dydaktyczny w Akademii Finansów i Biznesu Vistula Oddział w Olsztynie (dawniej Europejska Akademia Medycznych i Społecznych Nauk Stosowanych, Olsztyńska Szkoła Wyższa)
10.2021 – 02.2022	Pracownik dydaktyczny Uczelni Techniczno-Handlowej im. Heleny Chodkowskiej w Warszawie
10.2019 – 09.2020	Pracownik dydaktyczny Olsztyńskiej Szkoły Wyższej
02.2015 –10.2016	Pracownik dydaktyczny Wyższej Szkoły Biznesu i Zarządzania w Ciechanowie
02.2009 – 10.2010	Pracownik dydaktyczny Wyższej Szkoły Społeczno-Ekonomicznej w Warszawie
03.2008 – 12.2009	Pracownik dydaktyczny Instytutu Nauk Ekonomicznych Polskiej Akademii Nauk w Warszawie

11.2007 – 06.2009	Pracownik dydaktyczny Społecznej Wyższej Szkoły Przedsiębiorczości i Zarządzania Oddział w Warszawie

Doświadczenie praktyczne (zawodowe) uzyskane poza szkolnictwem wyższym (poza uczelnią):

03.2011 – 09.2013	Biuro Rachunkowe Rafał Koc Usługi Księgowe - Księgowa
09.2008 – 08.2009	Powiatowy Zespół Szkół Ponadgimnazjalnych w Legionowie – nauczyciel przedmiotów zawodowych
05.2001 – 06.2003	PBK Ochrona S.A. w Warszawie – Wydział Promocji i Marketingu
11.1999 – 04.2001	Dom Kredytowy Spółka z o.o., należąca do grupy kapitałowej Powszechnego Banku Kredytowego S.A. w Warszawie – Dział Księgowości
02.1998 – 10.1999	Bank Pekao S.A. Departament Ryzyka Kredytowego - Zespół Ryzyka Podmiotów
02.1996 – 02.1998	Bank Pekao S.A. Departament Bankowości Międzynarodowej - Zespół Współpracy z Bankami Krajowymi
07.1994 – 02.1996	Bank Pekao S.A. Filia I-go Oddziału w Warszawie - Wydział Obsługi Ludności

4. Omówienie osiągnięć, o których mowa w art. 219 ust. 1 pkt 2 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2021 r. poz. 478 z późn. zm.)

4.1. Wskazanie i omówienie osiągnięcia

Główne osiągnięcie naukowe, o którym mowa w art. 219 ust. 1 pkt 2 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2021 r. poz. 478 z późn. zm.) zawarte jest w **autorskiej monografii naukowej:**

- *[e_I.1_monografia]* [1]**Antczak J.** (2024), *Zarządzanie cyberbezpieczeństwem w przedsiębiorstwie - doświadczenia wybranych państw Unii Europejskiej*, Wydawnictwo Difin, SBN 978-83-8270-364-1, s. 334.

Recenzje wydawnicze monografii sporządzili:

- prof. dr hab. Dorota Jelonek – Politechnika Częstochowska
- prof. dr hab. Witold Chmielarz – Uniwersytet Warszawski

Główne ramy teoretyczno-badawcze

Podstawą ubiegania się o stopień doktora habilitowanego w dziedzinie nauk społecznych, w dyscyplinie nauki o zarządzaniu i jakości jest osiągnięcie zawarte w monografii pt. *Zarządzanie*

[1] W nawiasach kwadratowych przedstawiłam oznaczenia załączników potwierdzających omawiane zagadnienie. Oznaczenia zawierające literę "e_" wskazują na numerację załączników w wersji elektronicznej.

cyberbezpieczeństwem w przedsiębiorstwie - doświadczenia wybranych państw Unii Europejskiej. Monografia jest rezultatem mojego kilkuletniego zainteresowania i badań nad aspektami zarządzania cyberbezpieczeństwem zarówno na poziomie przedsiębiorstwa jak i państwa. Punktem wyjścia badań jest konceptualizacja cyberbezpieczeństwa jako integralnego elementu współczesnego paradygmatu zarządzania, wykraczającego poza jego techniczną lub peryferyjną rolę oraz uznanie cyberbezpieczeństwa za strategiczne zadanie przypisane kadrze kierowniczej, w tym także menedżerom średniego szczebla.

Zarządzanie cyberbezpieczeństwem stanowi interdyscyplinarne wyzwanie, wymagające współpracy sektorowej, a skuteczne zapewnienie bezpieczeństwa cyfrowego państwu, instytucjom i obywatelom obliguje do dialogu i partnerstwa między różnymi podmiotami. Kooperacja ta obejmuje zarówno sferę strategiczną, gdzie administracja publiczna, odpowiedzialna za tworzenie planów, powinna współpracować z sektorem prywatnym, dysponującym doświadczeniem i sprawdzonymi procesami zarządzania zagrożeniami cyfrowymi, jak i obszar operacyjny. W tym drugim przypadku, działania podejmowane przez administratorów sieci w administracji publicznej muszą być skoordynowane z ich odpowiednikami w sektorze prywatnym, pozarządowym oraz w środowisku naukowym. Kluczowe jest, aby ten dialog był autentyczny i efektywny. Unia Europejska i jej państwa członkowskie potrzebują spójnego systemu ochrony cyberprzestrzeni, opartego na jednolitych standardach, obejmujących wszystkie podmioty zaangażowane w cyberbezpieczeństwo, gdyż ochrona w cyberprzestrzeni jest niemożliwa do osiągnięcia w izolacji.

Zarządzanie współczesnymi organizacjami[2] cechuje się wysoką złożonością oraz zmiennością warunków. Zarządzający na co dzień muszą mierzyć się z takimi wyzwaniami, jak: globalizacja, dynamiczny rozwój teleinformatyczny, różnorodność kulturowa, zmienność regulacji prawno-systemowych, coraz wyższa dynamika procesów biznesowych i rosnące oczekiwania klientów. W tych warunkach profesjonalizacja zarządzania, polegająca na tworzeniu rozwiązań systemowych oraz zarządzaniu nimi z wykorzystaniem określonych narzędzi staje się koniecznością. Podejście intuicyjne, zmienność reguł działania, brak wizji oraz niska sprawność procesów organizacyjnych to główne czynniki niepowodzenia we współczesnym zarządzaniu (Czekaj, Ziębicki, 2021, s. 9).

Koncepcja zarządzania jest to idea, pomysł, sposób na prowadzenie instytucji, przedsiębiorstwa, który powinien określać jej miejsce w otoczeniu oraz pozwolić na stworzenie odpowiednich warunków wewnątrz przedsiębiorstwa do tego, aby móc dopasować pozycję zajmowaną przez przedsiębiorstwo do oczekiwań pracowników. Istnieje wiele różnorodnych koncepcji i metod zarządzania. Wybór jednej, najlepiej dopasowanej do specyfiki przedsiębiorstwa jest zależny od kierownictwa (Teczke, 1996, s. 6). Powstające w praktyce gospodarczej nowe koncepcje, odpowiadające na turbulentne otoczenie stanowią rezultat poszukiwania coraz bardziej skutecznych sposobów zarządzania.

[2] Stosuję zamiennie pojęcia: przedsiębiorstwo/organizacja/firma

Na podstawie analizy literatury można zaproponować następujący podział koncepcji zarządzania zorientowanych na:

1) jakość: kompleksowe zarządzanie jakością (*total quality management* – TQM), zarządzanie wartością (*value based management* – VBM), Sześć Sigma (*six sigma*);
2) wdrażanie zmian w przedsiębiorstwie: *reengineering*, *benchmarking*, *kaizen* (od japońskiego *kai* – zmiana, *zen* – dobrze), zarządzanie czasem (*time based management* – TBM);
3) współdziałanie: wirtualność, zarządzanie sieciowe;
4) wyszczuplanie organizacji: *outsourcing*, *offsharing*, *lean management,*
5) wiedzę: zarządzanie wiedzą (*knowledge management* – KM), zarządzanie przez kompetencje (*competency based management* – CBM);
6) całościowe podejście do zarządzania przedsiębiorstwem: zarządzanie procesowe, zarządzanie przez cele (*management by objectives* – MBO), zarządzanie zmianą, *controlling*.

Koncepcje zarządzania mogą stanowić podstawę do opracowania modelu zarządzania cyberbezpieczeństwem w przedsiębiorstwie, dostosowanego do jego indywidualnych potrzeb i uwarunkowań. Analizę poszczególnych koncepcji zarządzania oraz ich zastosowanie w systemie zarządzania cyberbezpieczeństwem w przedsiębiorstwie ilustruje tabela 1.

Tabela 1. Zastosowanie koncepcji zarządzania w systemie zarządzania cyberbezpieczeństwem w przedsiębiorstwie

Determinanty koncepcji zarządzania	**Zastosowanie w systemie zarządzania cyberbezpieczeństwem**
KOMPLEKSOWE ZARZĄDZANIE JAKOŚCIĄ (*TOTAL QUALITY MANAGEMENT* -TQM)	
– ciągłe doskonalenie procesów – zaangażowanie wszystkich pracowników w procesy jakościowe – skupienie na klientach i ich potrzebach – systematyczne podejście do zarządzania jakością – kontrola jakości danych i systemów	– regularne przeglądy i aktualizacje polityk cyberbezpieczeństwa – zaangażowanie wszystkich pracowników w utrzymanie i poprawę cyberbezpieczeństwa – systematyczna ocena ryzyk i wdrażanie działań prewencyjnych – regularne audyty cyberbezpieczeństwa – proaktywne podejście do wykrywania i eliminacji zagrożeń – ciągłe doskonalenie procesów cyberbezpieczeństwa
ZARZĄDZANIE WARTOŚCIĄ (*VALUE BASED MANAGEMENT* - VBM)	
– skupienie na tworzeniu wartości dla interesariuszy – podejmowanie decyzji na podstawie wartości dodanej – zrównoważone podejście do ryzyk i korzyści	– inwestowanie w technologie i rozwiązania zwiększające cyberbezpieczeństwo – ocena i zarządzanie ryzykiem z perspektywy wartości dla przedsiębiorstwa – wdrażanie strategii cyberbezpieczeństwa zgodnie z celami biznesowymi – ocena wpływu ryzyk cybernetycznych na wartość firmy
SZEŚĆ SIGMA *(SIX SIGMA)*	
– redukcja błędów i wad – skupienie na danych i analizie statystycznej – zwiększenie wydajności procesów – analiza i redukcja błędów – oparte na danych podejście do zarządzania ryzykiem	– identyfikacja i eliminacja luk w zabezpieczeniach – regularne audyty i analizy cyberincydentów – ciągłe doskonalenie strategii cyberzabezpieczeń – monitorowanie i analiza cyberincydentów – optymalizacja procesów zabezpieczeń

Źródło: opracowanie własne.

Tabela 1. Zastosowanie koncepcji zarządzania w systemie zarządzania cyberbezpieczeństwem w przedsiębiorstwie

Determinanty koncepcji zarządzania	Zastosowanie w systemie zarządzania cyberbezpieczeństwem
REENGINEERING	
– radykalne przekształcenie procesów – skupienie na efektywności i wydajności – przeprojektowanie procesów – radykalne zmiany	– przeprojektowanie systemów zabezpieczeń w celu ich optymalizacji – wprowadzenie nowych technologii i metod ochrony danych – kompleksowa analiza i restrukturyzacja systemów cyberbezpieczeństwa
BENCHMARKING	
– porównanie procesów z najlepszymi praktykami – adaptacja sprawdzonych rozwiązań – uczenie się od liderów branży	– analiza i implementacja najlepszych praktyk z zakresu cyberbezpieczeństwa – ciągłe porównywanie polityk i procedur z liderami branży – współpraca z innymi organizacjami w zakresie wymiany informacji o cyberzagrożeniach
KAIZEN	
– ciągłe doskonalenie – małe, stopniowe zmiany – zaangażowanie pracowników	– regularne aktualizacje systemów i procedur cyberbezpieczeństwa – ulepszanie procesów na podstawie feedbacku i audytów – regularne aktualizacje polityk cyberbezpieczeństwa – edukacja i trening pracowników w zakresie cyberbezpieczeństwa
ZARZĄDZANIE CZASEM (TIME BASED MANAGEMENT – TBM)	
– skracanie czasu realizacji procesów – poprawa reaktywności na zmiany – szybka reakcja na zmiany – zwinność operacyjna	– szybka reakcja na cyberincydenty – efektywne zarządzanie aktualizacjami i patchami – dynamiczne dostosowywanie strategii cyberbezpieczeństwa – szybkie wdrażanie nowych technologii ochronnych
WIRTUALNOŚĆ	
– wykorzystanie technologii informacyjnych – zarządzanie rozproszonymi zespołami – praca zdalna i rozproszona – wirtualne zespoły	– zdalne monitorowanie i zarządzanie systemami cyberbezpieczeństwa – wykorzystanie wirtualnych zespołów do analizy i reakcji na cyberincydenty – zabezpieczenia dla pracy zdalnej – zarządzanie ryzykiem w środowisku rozproszonym
ORGANIZACJE SIECIOWE	
– elastyczność i zdolność do szybkiego reagowania – współpraca między różnymi podmiotami – współpraca z partnerami zewnętrznymi – elastyczność i adaptacja	– tworzenie partnerstw z innymi organizacjami w celu wymiany informacji o cyberzagrożeniach – szybkie reagowanie na nowe zagrożenia poprzez współpracę sieciową – koordynacja działań z dostawcami usług cyberbezpieczeństwa – utrzymanie elastycznych i skalowalnych systemów cyberzabezpieczeń
OUTSOURCING	
– przekazywanie niektórych funkcji zewnętrznym dostawcom – wykorzystanie zewnętrznych usług	– zlecanie monitorowania i zarządzania cyberbezpieczeństwem wyspecjalizowanym firmom – korzystanie z usług ekspertów zewnętrznych do audytów i ocen cyberbezpieczeństwa – współpraca z firmami specjalizującymi się w cyberbezpieczeństwie – skupienie na strategicznych aspektach cyberbezpieczeństwa
OFFSHORING	
– dostęp do globalnych zasobów – przenoszenie działań do innych krajów – globalne zarządzanie	– użycie zagranicznych centrów operacyjnych do monitorowania cyberzagrożeń 24 godziny przez siedem dni w tygodniu – wykorzystanie międzynarodowych ekspertów do analizy i reagowania na cyberzagrożenia – zarządzanie cyberbezpieczeństwem w kontekście globalnym

Źródło: opracowanie własne.

Tabela 1. Zastosowanie koncepcji zarządzania w systemie zarządzania cyberbezpieczeństwem w przedsiębiorstwie

Determinanty koncepcji zarządzania	Zastosowanie w systemie zarządzania cyberbezpieczeństwem
LEAN MANAGEMENT	
– eliminacja marnotrawstwa – skupienie na wartości dodanej dla klienta – optymalizacja procesów	– optymalizacja procesów cyberbezpieczeństwa, aby były bardziej efektywne – redukcja zbędnych procedur, które mogą opóźniać reakcje na cyberincydenty – usprawnienie procesów zarządzania cyberincydentami – zwiększenie efektywności działań ochronnych
ZARZĄDZANIE WIEDZĄ (KNOWLEDGE MANAGEMENT – KM)	
– gromadzenie, udostępnianie i zarządzanie wiedzą – tworzenie baz wiedzy – utrzymanie zasobów intelektualnych	– budowanie i utrzymanie bazy wiedzy o cyberzagrożeniach i metodach obrony – szkolenie pracowników i podnoszenie ich świadomości w zakresie cyberbezpieczeństwa – tworzenie bazy wiedzy o cyberzagrożeniach
ZARZĄDZANIE PRZEZ KOMPETENCJE (COMPETENCY BASED MANAGEMENT – CBM)	
– rozwój i zarządzanie kompetencjami pracowników – identyfikacja kluczowych umiejętności – rozwój umiejętności pracowników – dopasowanie kompetencji do ról	– szkolenie specjalistów ds. cyberbezpieczeństwa w nowych technologiach i metodach obrony – certyfikacja i regularne testowanie umiejętności pracowników – rekrutacja i szkolenie specjalistów ds. cyberbezpieczeństwa – regularne oceny kompetencji zespołów cyberbezpieczeństwa
ZARZĄDZANIE PROCESOWE	
– identyfikacja i optymalizacja procesów – skupienie na efektywności procesów – definiowanie i optymalizacja procesów – zarządzanie przepływem pracy	– optymalizacja procesów związanych z zarządzaniem cyberincydentami – standaryzacja procedur i polityk cyberbezpieczeństwa – standaryzacja procesów cyberbezpieczeństwa – monitorowanie i kontrola działań zabezpieczających
ZARZĄDZANIE PRZEZ CELE (*MANAGEMENT BY OBJECTIVES* – MBO)	
– ustalanie jasnych, mierzalnych celów – monitorowanie postępów i osiągnięć – określanie i realizacja celów – motywowanie pracowników	– ustalanie celów w zakresie osiągnięcia określonych poziomów cyberbezpieczeństwa – regularne przeglądy i raportowanie wyników w zakresie cyberbezpieczeństwa – ustalanie celów cyberbezpieczeństwa zgodnych z celami biznesowymi – motywowanie zespołów do osiągania wyznaczonych standardów cyberbezpieczeństwa
ZARZĄDZANIE ZMIANĄ	
– planowanie i wdrażanie zmian – skuteczna komunikacja i zarządzanie oporem wobec zmian – adaptacja do zmieniających się warunków – proaktywne podejście do zmian	– wdrażanie nowych systemów zabezpieczeń i technologii – zarządzanie zmianami w politykach cyberbezpieczeństwa i procesach – planowanie i wdrażanie zmian w strategiach cyberbezpieczeństwa – zarządzanie ryzykiem związanym ze zmianami technologicznymi
CONTROLLING	
– monitorowanie i kontrola procesów – analiza i raportowanie wyników – wspomaganie decyzji	– regularne audyty i przeglądy systemów cyberbezpieczeństwa – monitorowanie zgodności z politykami i procedurami cyberbezpieczeństwa – regularne audyty i kontrole cyberbezpieczeństwa – wsparcie decyzji zarządu w kwestiach cyberbezpieczeństwa

Źródło: opracowanie własne.

TQM, Six Sigma i Kaizen kładą nacisk na systematyczne, ciągłe doskonalenie i redukcję błędów. W zarządzaniu cyberbezpieczeństwem przekłada się to na ciągłe przeglądy i aktualizacje polityk,

regularne audyty oraz analizę incydentów w celu eliminacji luk w zabezpieczeniach. Podejście to wymaga zaangażowania wszystkich pracowników w utrzymanie i poprawę bezpieczeństwa.

VBM i Lean Management skupiają się na tworzeniu wartości i eliminacji marnotrawstwa. W zarządzaniu cyberbezpieczeństwem oznacza to, że decyzje inwestycyjne dotyczące technologii i rozwiązań ochronnych powinny być podejmowane z perspektywy wartości dla przedsiębiorstwa. Ma to na celu usprawnienie procesów zarządzania incydentami i zwiększenie efektywności działań, redukując zbędne procedury.

Reengineering, Benchmarking i Organizacje sieciowe podkreślają znaczenie radykalnych zmian, adaptacji do najlepszych praktyk i współpracy. W obszarze zarządzania cyberbezpieczeństwem przekłada się to na przeprojektowywanie systemów zabezpieczeń, wdrażanie sprawdzonych rozwiązań od liderów branży oraz tworzenie partnerstw z innymi podmiotami w celu wymiany informacji o zagrożeniach.

Zarządzanie procesowe oraz Zarządzanie wiedzą i kompetencjami są kluczowe dla standaryzacji procedur i podnoszenia kwalifikacji zespołów. Umożliwiają one optymalizację procesów związanych z cyberincydentami, a także systematyczne szkolenie specjalistów i pracowników w zakresie nowych technologii i metod obrony.

Cyberbezpieczeństwo przeszło transformację, stając się kluczowym elementem nowej jakości w zarządzaniu przedsiębiorstwem. Już nie jest to wyłącznie kwestia techniczna, ale strategiczny wymiar zarządzania, wymagający proaktywnego podejścia menedżerów. Kadra zarządcza staje dziś przed kilkoma wyzwaniami, które zmuszają do przemyślenia dotychczasowych modeli zarządzania. Odejście od postrzegania cyberbezpieczeństwa jako kwestii IT i włączenie go w procesy strategiczne przedsiębiorstwa.

Skuteczne zarządzanie cyberbezpieczeństwem wymaga zrozumienia kluczowych pojęć związanych z funkcjonowaniem w cyberprzestrzeni, takich jak: bezpieczeństwo, cyberprzestrzeń, cyberbezpieczeństwo, bezpieczeństwo informacji, informacja oraz walka informacyjna. Punktem wyjścia jest identyfikacja zasobów wymagających ochrony oraz potencjalnych obszarów zagrożeń, co stanowi podstawę do opracowania efektywnej strategii obronnej.

Pojęcie bezpieczeństwa ma charakter wielowymiarowy i w opinii wielu ekspertów jest zarówno stanem, jak i też procesem. Stan ujmuje kategoria, gdy można określić jego wymiar, skalę trwałości czy zasięg terytorialny. Pojęcie procesu jest natomiast adekwatne, kiedy mowa o jego kształtowaniu i umacnianiu, gdy można określić jego dynamikę oraz w sytuacji, kiedy można wskazać jego zakres podmiotowy, przedmiotowy czy przestrzenny (Malak, 2007, s. 91 – 95). Pojęcie cyberprzestrzeni należy do kategorii pojęć niedookreślonych. Od strony semantycznej cyberprzestrzeń jest hybrydą pojęciową będącą skrótem od sformułowania ang. *cybernetics space*, czyli przestrzeni cybernetycznej (Banasiński, 2023, s. 27). Cyberprzestrzeń można określić jako przestrzeń przetwarzania i zarazem wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami między nimi relacjami z użytkownikami. F. Schreier definiuje cyberprzestrzeń jako, nowy, piąty teatr wojny, po lądzie, wodzie,

powietrzu i kosmosie, jest ze wszystkich sieci komputerowych na świecie oraz wszystkiego, co łączą i kontrolują poprzez kable, światłowody czy bezprzewodowo. To nie tylko Internet - to otwarta sieć sieci (Schreier, 2009, s. 10-11). Cyberbezpieczeństwo oraz cyberprzestrzeń są ściśle ze sobą powiązane i zarazem nieodłącznie związane z rewolucją ostatnich lat jaką jest dostęp do informacji, będący skutkiem rewolucji informatycznej. J. Czekaj na gruncie teorii zarządzania zaproponował wąską i szeroką definicję informacji. Zgodnie z wąską definicją informacji obejmuje ona wyłącznie wiadomości uzyskiwane w układzie nadawca (człowiek) – odbiorca (człowiek) w drodze czynności umysłowej. Szeroka definicja informacji dotyczy nie tylko wiadomości o czymś, ale także każdej decyzji, zakazu, sugestii. Takie ujęcie zakłada, że może ona być przekazywana nie tylko w układzie człowiek - człowiek, ale także w innych systemach, w których funkcjonuje. Rolę nadawcy mogą spełniać istoty żywe, maszyny lub inne obiekty (Czekaj, 2000, s. 178).

Najczęściej cyberbezpieczeństwo definiuje się z punktu widzenia zapobiegania uszkodzeniom, ochronie oraz w perspektywie przywracania zdolności do poprawnego funkcjonowania komputerów, systemów łączności elektronicznej czy też usług komunikacji odbywających się w cyberprzestrzeni. Cyberbezpieczeństwo to również ochrona informacji zawartych w przestrzeni komunikacji elektronicznej, w celu zapewnienia poufności z jednoczesnym uwierzytelnieniem osób do tego upoważnionych (Dunn, 2008, s. 19-23). Z kolei walka informacyjna to działania kooperacji negatywnej wzajemnej, w których cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych sobie stron (Ciborowski, 1999, s. 68). D. L. Pipkin, uważa, że bezpieczeństwo informacji to coś więcej niż bezpieczeństwo danych komputerowych. Oznacza ochronę własności intelektualnej wypracowanej w danej instytucji. Ta wartość intelektualna ma podstawowe znaczenie dla przeżycia instytucji. Działania firm opierają się na informacjach do nich należących, na ich tajemnicach (Pipkin, 2002, s. XV). Ochrona danych osobowych klientów, pracowników oraz kontrahentów stanowi fundamentalny element cyberbezpieczeństwa, ponieważ bezpośrednio wpływa na poziom bezpieczeństwa informacji, reputację przedsiębiorstwa oraz jego perspektywy rozwoju. Skuteczna ochrona danych buduje zaufanie interesariuszy, podczas gdy jej zaniedbanie może to zaufanie poważnie naruszyć.

Cyberbezpieczeństwo jest największym i najważniejszym obszarem bezpieczeństwa informacji, które stanowi zbiór działań, metod, procedur podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczanie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem (Potejko, 2009, s. 194).

Głównym celem zarządzania cyberbezpieczeństwem i zarazem zadaniem dla kadry zarządczej ds. cyberbezpieczeństwa, jest stworzenie systemu cyberbezpieczeństwa, zdefiniowanie, zaplanowanie i wdrożenie struktur organizacyjnych, zwiększających odporność organizacji i zarazem umożliwiających sprawniejsze działania w zakresie radzenia sobie z różnymi formami cyberataków. System nazywany jest jako zbiór wielu elementów które są od siebie zależne. W zarządzaniu wykorzystywane jest prawo

Ackoffa, którego zdaniem sprawność żadnego systemu, a więc i przedsiębiorstwa nigdy nie równa się sumie sprawności jego części składowych. Jest ona wynikiem wzajemnych oddziaływań (Ackoff, 1993, s. 103).

Na podstawie analizy literatury przedmiotu oraz materiałów źródłowych zaproponowałam definicję zarządzania cyberbezpieczeństwem, uwzględniającą aktualne wyzwania oraz dominujące podejścia teoretyczne i praktyczne: *Zarządzanie cyberbezpieczeństwem to kompleksowy proces strategiczny i operacyjny, obejmujący identyfikację, ocenę i mitygację ryzyk związanych z cyberzagrożeniami. Zarządzanie cyberbezpieczeństwem integruje technologie, polityki, procedury oraz zasoby ludzkie w celu ochrony integralności, poufności i dostępności danych oraz systemów informatycznych. Efektywne zarządzanie cyberbezpieczeństwem polega na ciągłym monitorowaniu i analizowaniu zagrożeń, proaktywnym wdrażaniu środków ochronnych, edukacji i szkoleniu pracowników, a także współpracy z zewnętrznymi podmiotami w zakresie wymiany informacji i najlepszych praktyk. Fundamentem zarządzania cyberbezpieczeństwem jest adaptacja do dynamicznie zmieniającego się otoczenia technologicznego oraz regulacyjnego, z uwzględnieniem specyfiki działalności organizacji oraz jej strategicznych celów biznesowych.*

Zarządzanie cyberbezpieczeństwem obejmuje wszystkie kluczowe elementy zarządzania według Griffina (tabela 2): planowanie, decydowanie, organizowanie, przewodzenie i kontrolowanie. W obu przypadkach ważne jest efektywne zarządzanie zasobami, zarówno ludzkimi, finansowymi, rzeczowymi, jak i informacyjnymi w celu osiągnięcia strategicznych celów oraz zapewnienia długoterminowego funkcjonowania przedsiębiorstwa w zmieniającym się otoczeniu.

Tabela 2. Porównanie zarządzania cyberbezpieczeństwem z definicją zarządzania według Griffina

Zarządzanie wg Griffina	**Zarządzanie cyberbezpieczeństwem**
PLANOWANIE	
Kluczowy element procesu zarządzania, obejmujący określenie celów i strategii organizacji	Obejmuje identyfikację cyberzagrożeń i ocenę ryzyk, co prowadzi do opracowania strategii zarządzania cyberbezpieczeństwem
DECYDOWANIE	
Decyzje zarządcze są niezbędne do realizacji celów organizacji	Obejmuje decyzje dotyczące wyboru środków ochronnych, polityk cyberbezpieczeństwa i reakcji na cyberincydenty są kluczowe dla funkcjonowania przedsiębiorstwa
ORGANIZOWANIE	
Organizowanie zasobów w sposób umożliwiający realizację celów przedsiębiorstwa	Obejmuje alokację zasobów technologicznych, ludzkich i proceduralnych w celu zapewnienia skutecznej ochrony danych i systemów
PRZEWODZENIE (kierowanie ludźmi)	
Kierowanie ludźmi, motywowanie i prowadzenie zespołów	Obejmuje szkolenie i edukację pracowników w zakresie cyberbezpieczeństwa oraz budowanie kultury cyberbezpieczeństwa w przedsiębiorstwie
KONTROLOWANIE	
Kontrola procesów i wyników w celu zapewnienia zgodności z planami	Obejmuje ciągłe monitorowanie systemów pod kątem cyberzagrożeń, przeprowadzanie audytów cyberbezpieczeństwa i ocenę skuteczności środków ochronnych

Źródło: opracowanie własne.

Zarządzanie wg Griffina obejmuje funkcje planowania, organizowania, przewodzenia i kontrolowania w celu osiągania celów organizacji. Elementy te znajdują odzwierciedlenie w zarządzaniu cyberbezpieczeństwem poprzez:

- planowanie jako strategiczne i operacyjne planowanie zabezpieczeń, określanie polityk i procedur cyberbezpieczeństwa;
- organizowanie jako strukturalne zarządzanie zasobami technologicznymi i ludzkimi, definiowanie ról i odpowiedzialności w zakresie cyberbezpieczeństwa;
- przewodzenie jako kierowanie zespołami bezpieczeństwa, motywowanie i edukacja pracowników;
- kontrolowanie jako monitorowanie systemów i procesów bezpieczeństwa, audyty i oceny ryzyka, wprowadzanie działań korygujących.

Metodyka badań

Procedura badawcza została rozpoczęta od pogłębionej analizy literatury przedmiotu oraz źródeł normatywnych, obejmujących zarówno klasyczne koncepcje zarządzania, jak i współczesne podejścia do cyberbezpieczeństwa, co umożliwiło ugruntowanie podstaw teoretycznych, identyfikację luki badawczej oraz wskazanie aktualnych trendów w dyskursie naukowym.

W kolejnym etapie zdefiniowałam problem badawczy (PB) w postaci pytania, sformułowałam hipotezę główną (HG) oraz sześć hipotez szczegółowych (H1 – H6).

PB: Jakie determinanty mają wpływ na zarzadzanie cyberbezpieczeństwem w przedsiębiorstwie?

HG: *Zmieniające się cyberzagrożenia powodują określenie kluczowych determinant zarządzania cyberbezpieczeństwem w przedsiębiorstwie.*

H1: *Zarządzanie cyberbezpieczeństwem w przedsiębiorstwie integruje kluczowe sekwencje zarządzania: planowanie, organizowanie, przewodzenie i kontrolowanie dostosowując je do potrzeb ochrony informacji w cyberprzestrzeni.*

H2: *Determinanty koncepcji zarządzania można wykorzystać do stworzenia modelu zarządzania cyberbezpieczeństwem w przedsiębiorstwie.*

H3: *Regularne szkolenia wraz z budowaniem świadomości pracowników w zakresie cyberzagrożeń istotnie wpływają na zarządzenie cyberbezpieczeństwem w przedsiębiorstwie.*

H4: *Wyodrębniony budżet cyberbezpieczeństwa to czynnik determinujący ogólny poziom procesów zarządzania cyberbezpieczeństwem w przedsiębiorstwie.*

H5: *Występują różnice w podejściu do cyberbezpieczeństwa biorąc pod uwagę rodzaj przedsiębiorstwa.*

H6: *Sztuczna Inteligencja stanowi wyzwanie dla przedsiębiorstwa w zakresie zarządzania cyberbezpieczeństwem.*

W nawiązaniu do postawionych hipotez badawczych sformułowałam cel główny (CG) oraz sześć celów szczegółowych podzielonych na: poznawcze (C1-C2), metodyczne (C3-C4) i utylitarne (C6 – C7).

CG: *Identyfikacja kluczowych determinant zarządzania cyberbezpieczeństwem w przedsiębiorstwie.*

C1: *Ustalenie relacji kluczowych etapów zarządzania z zarządzaniem cyberbezpieczeństwem w przedsiębiorstwie.*

C2: *Identyfikacja praktyk koncepcji zarządzania mogących być wykorzystywane w tworzeniu modelu zarządzania cyberbezpieczeństwem w przedsiębiorstwie.*

C3: *Określenie czynności skierowanych do pracowników kluczowych dla zarządzenia cyberbezpieczeństwem w przedsiębiorstwie*

C4: *Identyfikacja barier determinujący ogólny poziom procesów zarządzania cyberbezpieczeństwem w przedsiębiorstwie.*

C5: *Identyfikacja praktyk stosowanych w obszarze zarządzania cyberbezpieczeństwem w przedsiębiorstwie.*

C6: *Identyfikacja najważniejszych wyzwań w obszarze zarządzania cyberbezpieczeństwem w przedsiębiorstwie.*

Istotne było przyjęcie założenia, że cyberbezpieczeństwo to nie odizolowany proces technologiczny, lecz złożona kategoria zarządcza wymagająca integracji z podstawowymi funkcjami organizacji. Na tym etapie powstał również wstępny projekt koncepcji badań empirycznych, obejmujący zarówno dobór metod, jak i określenie próby badawczej.

W kolejnym etapie procesu badawczego opracowałam narzędzia empiryczne, w tym autorski kwestionariusz ankiety wykorzystany w badaniach ilościowych. W badaniach jakościowych zastosowałam wywiady z przedstawicielami kadry zarządzającej, specjalistami ds. bezpieczeństwa informacji oraz analitykami ryzyka w przedsiębiorstwach.

Na kolejnym etapie procesu badawczego dokonałam doboru próby, uwzględniając w badaniach ilościowych przedsiębiorstwa z sektora IT. Zastosowałam metodę doboru celowego, biorąc pod uwagę wielkość organizacji, profil działalności oraz kraj pochodzenia. W badaniu ankietowym udział wzięło 150 respondentów, natomiast w badaniach jakościowych uczestniczyło siedmiu ekspertów reprezentujących sektor prywatny i instytucje publiczne.

W dalszej części procesu badawczego zrealizowałam badania empiryczne w formie studiów przypadków, koncentrując się na dwóch incydentach z obszaru cyberbezpieczeństwa: ataku NotPetya z 2017 r. oraz kryzysie zaufania i wycieku danych w firmie CD Projekt w 2021 r. Analizę przypadków przeprowadziłam z wykorzystaniem metody desk research, uwzględniając raporty wewnętrzne, komunikaty giełdowe oraz doniesienia medialne. Celem tego etapu była identyfikacja mechanizmów reagowania organizacji na zagrożenia, ocena skuteczności działań prewencyjnych oraz analiza kosztów i strat.

W kolejnym etapie procesu badawczego przeprowadzone zostały badania ankietowe, z wykorzystaniem techniki CATI (skrót od angielskiego *computer-assisted telephone interviewing*, czyli wspomagany komputerowo wywiad telefoniczny), co umożliwiło dotarcie do szerokiego grona respondentów z państw Trójkąta Weimarskiego. Analiza komparatywna państw Trójkąta Weimarskiego umożliwiła zestawienie Polski z Francją i Niemcami – kluczowymi, wiodącymi gospodarkami Unii Europejskiej. Procedura ta stanowiła podstawę empiryczną do opracowania szczegółowych rekomendacji w zakresie zarządzania cyberbezpieczeństwem, przedstawionych w ostatniej części pracy.

W kolejnym etapie procesu badawczego przeprowadziłam analizę danych ankietowych, wykorzystując narzędzia statystyczne, takie jak analiza częstości i korelacje. Dodatkowo zrealizowałam analizy porównawcze między przedsiębiorstwami z Polski, Niemiec i Francji, co umożliwiło identyfikację różnic kulturowych i strukturalnych w podejściu do zarządzania cyberbezpieczeństwem.

W kolejnym etapie procesu badawczego zrealizowałam wywiady eksperckie, prowadzone zgodnie z wcześniej opracowanym scenariuszem. Pozwoliły one na pogłębienie zagadnień poruszanych w ankietach oraz uzyskanie interpretacji, opinii i rekomendacji od osób mających realny wpływ na zarządzanie cyberbezpieczeństwem w swoich organizacjach.

Uzyskane wyniki pozwoliły mi na potwierdzenie postawionych hipotez. Następnie opracowałam narzędzia wizualizacji danych oraz integracji wyników ilościowych i jakościowych. Stworzyłam wykresy, tabele, macierz SWOT, które obrazowały zależności między zmiennymi. Umożliwiło to nie tylko przejrzystą prezentację wyników, lecz także sformułowanie podstaw dla konstrukcji modelu zarządzania cyberbezpieczeństwem.

Na zakończenie procesu badawczego sformułowałam końcowe wnioski i rekomendacje, odnoszące się zarówno do teorii zarządzania, jak i praktyki menedżerskiej. Przedstawiłam również propozycję autorskiego modelu zarządzania cyberbezpieczeństwem.

W pracy zastosowałam komplementarne podejście metodologiczne, integrujące zarówno metody ilościowe, jak i jakościowe. W celu zwiększenia wiarygodności i rzetelności uzyskanych wyników, wykorzystałam triangulację metod badawczych. Podejście to, polegające na łączeniu co najmniej dwóch odmiennych metod, umożliwiło poszerzenie perspektywy oraz dogłębne zrozumienie analizowanego zjawiska (Dźwigoł, 2015, s. 106). Integracja różnych metod zwiększa trafność poznawczą oraz umożliwia wieloaspektową analizę złożonych zjawisk organizacyjnych (Czakon 2011). Zastosowałam następujące metody badawcze: przegląd literatury i dokumentów zastanych, studium przypadku, badanie ankietowe oraz wywiad.

Przegląd literatury jako krytyczna analiza dostępnej literatury, badań i publikacji naukowych, istotnych dla badanego tematu, która pozwoliła mi na zidentyfikowanie odpowiednich teorii, metodologii oraz podejścia stosowanego w opublikowanych badaniach co umożliwiło zidentyfikowanie luki badawczej oraz pomogło ukształtować badania.

Analizę danych zastanych (badaniem wtórnym, *desk research*) jako metodę badawczą polegającą na kompilacji, analizowaniu oraz przetwarzaniu danych i informacji pochodzących z istniejących źródeł,

a następnie formułowaniu na ich podstawie wniosków dotyczących badanego problemu (Bednarowska, 2015, s. 20). Desk research realizowany był przez wszystkie etapy procesu badawczego poprzez ciągłe uzupełnianie dokumentów oraz zestawianie ich z już pozyskanymi materiałami.

Analizę przypadku (studium przypadku, case study) jako metodę badawczą zawierającą szeroki opis danego zjawiska, mającą na celu jego pogłębioną analizę i ocenę. Poprzez wykorzystanie wielu technik gromadzenia oraz analizy danych pozwala na rozwiązywanie problemu naukowego i praktycznego (Grzegorczyk, 2015, s. 9-10). W celu lepszego zrozumienia omawianego problemu badawczego do analizy przypadku wybrałam atak NotPetya który był bardzo istotny dla rozwoju myślenia o cyberbezpieczeństwie i zarazem pokazał zagrożenia dla funkcjonowania przedsiębiorstw – ponadpaństwowe i zagrażające łańcuchom dostaw. Drugie studium przypadku dotyczy ataku na spółkę CD Projekt S.A. Analiza ta koncentruje się na ocenie reakcji kierownictwa na incydent oraz sposobie dostosowania polityki zarządzania ryzykiem do wymogów zapewnienia ciągłości cyberbezpieczeństwa przedsiębiorstwa. Analiza przypadku posłużyły zrozumieniu okoliczności decyzyjnych konkretnych decydentów w określonych warunkach (Czakon, 2020, s. 192) w analizowanym przypadku były to skutki po cyberataku.

Badania ankietowe zaprezentowane w monografii miały charakter sondażowy i zostały zrealizowane na przestrzeni dwóch lat (listopad 2022 r. - listopad 2023 r.) wśród przedsiębiorstw z branży IT działających na terytorium Francji, Niemiec i Polski. Badanie metodą ilościową z wykorzystaniem techniki CATI, przeprowadził wśród osób odpowiedzialnych za cyberbezpieczeństwo w firmach - Instytut Badawczy IPC Sp. z o.o. z siedzibą we Wrocławiu. Podstawą ich realizacji był kwestionariusz ankiety mojego autorstwa, składający się z 29 pytań jednokrotnego i wielokrotnego wyboru, podzielonych na dwa bloki tematyczne: ogólne zagadnienia związane z cyberbezpieczeństwem oraz nakłady finansowe na jego zapewnienie. Badanie przeprowadzono na próbie 150 przedsiębiorstw z branży IT. Próba miała charakter probabilistyczny (zwany losowym). Dobór jednostek do próby przeprowadzono z zastosowaniem metody prostego losowania. Losowy dobór próby charakteryzuje się wysokim stopniem standaryzacji i jest elementem badań ilościowych, a jej podstawową zaletą jest fakt, że wyniki można uogólnić na całą populację (Gerring, 2001).

Na podstawie przeprowadzonych badań (studium literatury, dokumentów zastanych, studium przypadku, badań ankietowych) wyodrębniłam trzy obszary tematyczne do dalszej analizy: trudności przedsiębiorców w obszarze zarządzania bezpieczeństwem informacji, prawdopodobieństwo wystąpienia cyberataków w ciągu roku do pięciu lat oraz sztuczna inteligencja w odniesieniu do cyberbezpieczeństwa. W celu uzyskania szczegółowych opinii w wyszczególnionym zakresie przeprowadziłam badania jakościowe techniką wywiadu eksperckiego jako specyficzną formę rozmowy, w trakcie, której wiedzę tworzy się w toku interakcji między osobą prowadzącą wywiad a respondentem (Kvale, 2010, s. 19). Wywiady przeprowadziłam na przełomie maja i czerwca 2024 r. Przeprowadzone wywiady można zakwalifikować jako: indywidualne, jawne, ustne, częściowo ustrukturyzowane. Zostały przeprowadzone w celu uzyskania szczegółowych opinii w trzech obszarach

tematycznych: kłopoty przedsiębiorców w obszarze zarządzania bezpieczeństwem informacji, prawdopodobieństwo wystąpienia cyberataków w ciągu roku do pięciu lat oraz sztuczna inteligencja w odniesieniu do cyberbezpieczeństwa. Ekspertami byli: dr inż. Andrzej Bartosiewicz, Prezes CISO #Poland, Młodszy Redaktor CyberDefence 24, Właściciel firmy, Audytor ISO 27001, Menedżer ds. Systemu zarządzania ryzykiem, Specjalista IT, oraz Pan Adam Marczyński Zastępca Dyrektora NASK ds. Cyberbezpieczeństwa i Innowacji (część respondentów nie zgodziła się na opublikowanie ich danych osobowych).

Charakterystyka układu pracy

Struktura monografii (tabela 3) została zaprojektowana w sposób sekwencyjny, mający na celu stopniowe rozwijanie zrozumienia złożoności zarządzania cyberbezpieczeństwem w kontekście przedsiębiorstwa. Każdy rozdział kończy się podsumowaniem i wnioskami. Taka struktura zapewnia holistyczne podejście do zarządzania cyberbezpieczeństwem, łącząc podstawy teoretyczne z praktycznymi studiami przypadków i aktualnymi trendami.

Rozdział pierwszy zatytułowany *„Wprowadzenie do zarządzania cyberbezpieczeństwem w przedsiębiorstwie”,* który podzieliłam na pięć podrozdziałów, jest rozdziałem wprowadzającym w problematykę monografii. Omówiłam w nim koncepcje zarządzania przedsiębiorstwem w kontekście cyberbezpieczeństwa. Ponieważ zarządzanie współczesnymi organizacjami wymaga profesjonalizacji, systemowych rozwiązań oraz narzędzi wspierających, a jego kluczowe elementy obejmują planowanie, podejmowanie decyzji, organizowanie, przewodzenie i kontrolowanie zasobów organizacyjnych, wskazałam, że podejście do zarządzania cyberbezpieczeństwem musi być integralne i obejmować wszystkie aspekty działalności organizacji. Zwróciłam uwagę na zalety i wady klasycznych koncepcji zarządzania. Wskazałam, które determinanty poszczególnych koncepcji mogą być wykorzystane w tworzeniu modelu zarządzaniu cyberbezpieczeństwem w przedsiębiorstwie. Następnie zdefiniowałam zarządzanie cyberbezpieczeństwem zwracając uwagę na elementy definicji zarządzania wg Grifina. Opisałam także wymagania w obszarze cyberbezpieczeństwa jakim muszą sprostać przedsiębiorstwa.

W rozdziale pierwszym scharakteryzowałam środowisko, w którym działają i zarazem są narażone na niebezpieczeństwo systemy informatyczne przedsiębiorstwa, to w rozdziale drugim pt. „*Zagrożenia w cyberprzestrzeni i przeciwdziałania nim”* przedstawiłam zarówno rodzaje zagrożeń jak i aktorów występujących w cyberprzestrzeni. Cyberzagrożenia przyjmują różną formę, dlatego istotne jest zrozumienie struktury kosztów i korzyści związanych z cyberprzestępstwami oraz mechanizmów działania cyberprzestępców. Organizacje powinny implementować dojrzałe praktyki cyberbezpieczeństwa i systematycznie monitorować swoje zasoby informacyjne w tym obszarze pomocne jest wdrożenie norm i standardów, m.in. takich jak ISO/IEC 27001 i tą tematykę poruszam w dalszej części rozdziału. Przybliżyłam również tematykę kosztów związanych z zarządzaniem cyberbezpieczeństwem.

Tabela 3. Syntetyczne zestawienie treści poszczególnych rozdziałów pracy, zastosowane metody badawcze, realizacja celów, weryfikacja hipotez

Tematyka rozdziału		**Treści/zakres rozdziału**	**Metoda badawcza, realizacja celu, weryfikacja hipotez**
Rozdział 1	Wprowadzenie do zarządzania cyberbezpieczeństwem w przedsiębiorstwie	1. Koncepcje zarządzania jednostką gospodarczą 2. Definicje i kluczowe pojęcia w zakresie cyberbezpieczeństwa 3. Zarządzanie cyberbezpieczeństwem 4. Wymagania w zakresie cyberbezpieczeństwa	Analiza: literatury, dokumentów zastanych (aktów prawnych) **realizacja celu: C1, C2** **weryfikacja hipotez: H1, H2**
Rozdział 2	Zagrożenia w cyberprzestrzeni i przeciwdziałanie nim	1. Rodzaje zagrożeń i aktorów w cyberprzestrzeni 2. Wybrane modele zarządzania bezpieczeństwem IT 3. Zarządzanie kosztami cyberbezpieczeństwa przedsiębiorstwa	Analiza: literatury, dokumentów zastanych (norm, danych statystycznych w zakresie ISO) **realizacja celu: C3, C4** **weryfikacja hipotez: H2, H4**
Rozdział 3	Cyberbezpieczeństwo państw Trójkąta Weimarskiego	1. Charakterystyka państw Trójkąta Weimarskiego 2. Nakłady na cyberbezpieczeństwo w państwach Trójkąta Weimarskiego 3. Ramy prawne w zakresie cyberbezpieczeństwa w UE 4. Analiza strategii cyberbezpieczeństwa państw Trójkąta Weimarskiego	Analiza: literatury, dokumentów zastanych (aktów prawnych, raportów firm audytorsko-doradczych, danych Eurostat, EDA) **realizacja celu: C4, C6**
Rozdział 4	Wpływ cyberataków na zarządzanie przedsiębiorstwem	1. Wprowadzenie do krajobrazu zagrożeń według analiz raportów firm audytorsko-doradczych 2. Przegląd ataków hackerskich w Europie i na świecie 3. Wpływ cyberataku typu ransomware na zarządzanie przedsiębiorstwem 4. Wpływ cyberataku typu wyciek danych na zarządzanie przedsiębiorstwem	Analiza: literatury, dokumentów zastanych (raporty firm audytorsko-doradczych), Studium przypadku (NotPetya CD Projekt S. A.) **realizacja celu: C3, C4, C5** **weryfikacja hipotez: H3, H4**
Rozdział 5	Praktyczne aspekty zarządzania cyberbezpieczeństwem w przedsiębiorstwie – wyniki badań	1. Wyniki badań ankietowych i ich analiza 1.1. Charakterystyka próby badawczej 1.2. Zagadnienia dotyczące zarządzania cyberbezpieczeństwem w przedsiębiorstwie 1.3. Zagadnienia dotyczące zarządzania nakładami finansowymi na cyberbezpieczeństwo 2. Trudności i wyzwania w zakresie zarządzania cyberbezpieczeństwem w przedsiębiorstwie 2.1. Zagadnienia dotyczące kłopotów przedsiębiorców w obszarze zarządzania bezpieczeństwem informacji 2.2. Zagadnienia w zakresie wystąpienia cyberataków w ciągu roku do pięciu lat 2.3. Zagadnienia dotyczące sztucznej inteligencji w odniesieniu do cyberbezpieczeństwa 3. Determinanty i model zarządzania cyberbezpieczeństwem w przedsiębiorstwie	Badania ankietowe Wywiady eksperckie **realizacja celu: C3, C4, C5, C6, CG** **weryfikacja hipotez: H2, H3, H4, H5, H6, HG**

Źródło: opracowanie własne.

W rozdziale trzecim pt. „*Cyberbezpieczeństwo państw Trójkąta Weimarskiego"* scharakteryzowałam kluczowe aspekty zarządzania cyberbezpieczeństwem państw Trójkąta Weimarskiego. Francja, Niemcy, Polska, podobnie jak inne kraje na świecie, stoją w obliczu wyzwań związanych z zapewnieniem cyberbezpieczeństwa w szybko zmieniającym się, globalnym otoczeniu. W odpowiedzi na te wyzwania, poszczególne państwa opracowały i zarazem wdrożyły omówione w niniejszym rozdziale strategie mające na celu wzmocnienie cyberbezpieczeństwa kraju, chroniąc infrastrukturę krytyczną,

przedsiębiorstwa i obywateli przed cyberzagrożeniami. Przedstawiłam również ramy prawne w zakresie cyberbezpieczeństwa obowiązujące w Unii Europejskiej. Analiza państw Trójkąta Weimarskiego pozwoliła porównać Polskę z Niemcami i Francją, a więc wiodącymi dużymi gospodarkami UE, co umożliwiło mi lepiej wypracować rekomendacje w zakresie zarządzania cyberbezpieczeństwem zaprezentowane w ostatniej części pracy.

W rozdziale czwartym pt. „*Wpływ cyberataków na zarządzanie przedsiębiorstwem"* analizuję wpływ cyberataków na działalność przedsiębiorstwa, wskazując na różnorodne zagrożenia, m.in. takie jak ransomware, phishing, wycieki danych i zaawansowane ataki. Cyberprzestępcy coraz częściej wykorzystują zaawansowane technologie, w tym sztuczną inteligencję, do przeprowadzania ataków. Przedsiębiorstwa muszą zatem przyjmować zaawansowane środki obronne i inwestować w cyberbezpieczeństwo. W pierwszej kolejności na podstawie raportów firm audytorsko-doradczych przedstawiłam krajobraz zagrożeń na jakie są narażone przedsiębiorstwa w tym zwróciłam szczególną uwagę na cyberzagrożenia państw Trójkąta Weimarskiego. Następnie w celu zobrazowania szerszej perspektywy analizowanego zagadnienia zaprezentowałam ataki hackerskie w Europie i na świecie. W celu lepszego zrozumienia analizowanego zjawiska omówiłam dwa przypadki cyberataku i ich wpływ na zarządzanie cyberbezpieczeństwem w przedsiębiorstwie. Pierwszy przypadek dotyczył ataku NotPetya, który był bardzo ważny dla rozwoju myślenia o cyberbezpieczeństwie oraz pokazał zagrożenia dla funkcjonowania przedsiębiorstw. Drugi przypadek z jednej strony przedstawia podejście właścicieli CD Project S. A. do cyberataku z drugiej wskazuje jak wdrażana jest polityka zarządzania ryzykiem dostosowywana do zapewnienia cyberbezpieczeństwa przedsiębiorstwa.

W rozdziale piątym p.t. „*Praktyczne aspekty zarządzania cyberbezpieczeństwem w przedsiębiorstwie – wyniki badań"* zaprezentowałam wyniki badań ilościowych oraz jakościowych. W pierwszej części przedstawiłam wyniki badań ankietowych przeprowadzonych na próbie 150 przedsiębiorstw z branży informatycznej państw Trójkąta Weimarskiego. Badania ankietowe dotyczyły praktyk stosowanych w przedsiębiorstwach w zakresie zarządzania cyberbezpieczeństwem w dwóch obszarach: cyberbezpieczeństwem (ogólnie) i nakładach finansowych na cyberbezpieczeństwem. Następnie omówiłam wyniki przeprowadzonych wywiadów eksperckich, które zostały zrealizowane w celu uzyskania szczegółowych opinii w trzech obszarach tematycznych: zagrożeniach przedsiębiorców w obszarze zarządzania bezpieczeństwem informacji, prawdopodobieństwo wystąpienia cyberataków w ciągu roku do pięciu lat oraz sztuczna inteligencja w odniesieniu do cyberbezpieczeństwa. Po przedstawieniu wyników badań ilościowy i jakościowych wskazałam determinanty oraz zaproponowałam model zarządzania cyberbezpieczeństwem w przedsiębiorstwie.

Na podstawie przeprowadzonych badań w ostatniej części monografii przedstawiłam wnioski końcowe, rekomendacje i zweryfikowałam przyjęte hipotezy oraz cele pracy. Na koniec wskazałam kierunki dalszych prac badawczych.

Omówienie osiągnięć

Badania przeprowadzone w ramach monografii pozwoliły mi na zgromadzenie materiału empirycznego, który stanowił podstawę pogłębionej analizy zjawiska zarządzania cyberbezpieczeństwem w przedsiębiorstwie. Skoncentrowałam się zarówno na ogólnych trendach i uwarunkowaniach, jak i na konkretnych praktykach organizacyjnych, co umożliwiło wielopoziomowe ujęcie problemu.

Zrozumienie kluczowych pojęć i definicji w zarządzaniu cyberbezpieczeństwem jest fundamentem skutecznej ochrony przed rosnącą liczbą cyberzagrożeń. Wiedza ta pozwala na lepsze zrozumienie złożoności środowiska cyfrowego, w którym funkcjonują współczesne przedsiębiorstwa, oraz na opracowanie skutecznych strategii, polityk ochrony danych i infrastruktury IT. Stałe kształcenie i aktualizacja wiedzy w dziedzinie cyberbezpieczeństwa są niezbędne, aby nadążyć za szybkimi zmianami w technologiach i metodach ataków, zapewniając tym samym bezpieczeństwo i stabilność operacyjną organizacji.

Zarządzanie cyberbezpieczeństwem jest niezbędnym elementem współczesnej strategii organizacyjnej, mającym na celu ochronę przed rosnącą różnorodnością cyberzagrożeń. Wymaga ono nie tylko stosowania zaawansowanych technologii, ale również ciągłej edukacji, świadomości oraz adaptacji do zmieniającego się środowiska. Poprzez zrozumienie podstaw, wyzwań oraz kluczowych elementów zarządzania cyberbezpieczeństwem, organizacje mogą lepiej przygotować się na przyszłe wyzwania, zapewniając bezpieczeństwo swoich cyfrowych zasobów.

Wdrażanie polityk cyberbezpieczeństwa w przedsiębiorstwie jest złożonym procesem, wymagającym zaangażowania zasobów materialnych i niematerialnych oraz ciągłego doskonalenia. Poprzez definiowanie jasnych polityk w zakresie cyberbezpieczeństwa, zaangażowanie kadry zarządzającej, edukację pracowników, skuteczne wdrażanie, monitorowanie oraz regularne aktualizacje procedur, przedsiębiorstwa mogą skutecznie zarządzać cyberbezpieczeństwem i chronić swoje zasoby cyfrowe przed rosnącymi zagrożeniami. Ważne jest, aby zarządzanie cyberbezpieczeństwem było integralną częścią kultury przedsiębiorstwa, promując otwartość na zgłaszanie potencjalnych słabości i incydentów oraz wspierając ciągłe doskonalenie procesów bezpieczeństwa.

Na kanwie pierwszego rozdziału sformułowałam następujące wnioski:

1) Organizacje winny wdrażać systemowe podejście do zarządzania z wykorzystaniem narzędzi wspierających procesy decyzyjne i operacyjne.
2) Szkolenie i rozwijanie kompetencji pracowników w zakresie cyberbezpieczeństwa, w tym rozpoznawania zagrożeń i reagowania na incydenty stanowi kluczowe znaczenie w zarządzaniu cyberbezpieczeństwem.
3) Stworzenie jasnych procedur i polityk dotyczących zarządzania cyberbezpieczeństwem, które będą obejmować planowanie, organizowanie, przewodzenie i kontrolowanie stanowi drogowskaz dla przedsiębiorstwa działającego w cyberprzestrzeni.

Zrozumienie cyberzagrożeń i ich potencjalnego wpływu na działalność organizacji stanowi pierwszy krok do budowania skutecznej cyberobrony. Poprzez połączenie edukacji, regularnych aktualizacji, odpowiednich zabezpieczeń technicznych i zarządzania dostępem, można zredukować ryzyko i minimalizować potencjalne szkody wynikające z cyberataków. Cyberbezpieczeństwo wymaga ciągłej uwagi i adaptacji do zmieniającego się krajobrazu zagrożeń.

Na kanwie drugiego rozdziału sformułowałam następujące wnioski:

1) Niezależnie od wielkości przedsiębiorstwa winny być wdrażane rygorystyczne praktyki w zakresie cyberbezpieczeństwa.
2) W organizacjach należy przeprowadzać regularne analizy zagrożeń i testy penetracyjne, aby identyfikować i eliminować wąskie gardła w zakresie cyberbezpieczeństwa.
3) Świadomość pracowników na temat cyberzagrożeń powinna być zwiększana poprzez regularne szkolenia i kampanie informacyjne.

Normatywne ramy Unii Europejskiej służą ochronie kontynentu przed cyfrowymi zagrożeniami. System ten narzuca państwom członkowskim obowiązek opracowania krajowych strategii, a także wymaga zgłaszania incydentów oraz wspiera mechanizmy certyfikacji. Działania te są ukierunkowane na zapewnienie zaawansowanego poziomu cyberbezpieczeństwa, co ma krytyczne znaczenie dla stabilności społeczeństwa, gospodarki i procesów demokratycznych. Skuteczna implementacja regulacji jest uwarunkowana ciągłą synergistyczną współpracą instytucji publicznych, podmiotów gospodarczych oraz społeczeństwa.

Występuje konieczność koordynacji systemowej w skali państwa, tak aby skutecznie analizować konieczność wydatków, minimalizować koszty. Niezbędna jest wiedza dla rządzących w zakresie ponoszonych kosztów przez sektor prywatny. Wnioski z przeprowadzonej analizy prowadzą do rekomendacji, że skuteczne budowanie własnego, narodowego potencjału naukowo-techniczno-przemysłowego w zakresie cyberbezpieczeństwa jest kluczowe.

Strategie państw Trójkąta Weimarskiego łącznie podkreślają znaczenie cyberbezpieczeństwa w ochronie wzajemnie połączonych systemów cyfrowych oraz proaktywne środki niezbędne do przeciwdziałania potencjalnym cyberzagrożeniom i łagodzenia ich skutków poprzez inicjatywy krajowe i współpracę międzynarodową.

Na kanwie trzeciego rozdziału sformułowałam następujące wnioski:

1) Państwa powinny promować międzynarodową współpracę i wymianę informacji w zakresie cyberbezpieczeństwa między sobą.
2) W celu poprawy zdolności reagowania na zagrożenia państwa winny inwestować w rozwój technologii zabezpieczeń oraz w szkolenia personelu.
3) Poszczególne państwa powinny implementować strategiczne ramy i mierzalne wskaźniki efektywności w zakresie wdrażania polityk cyberbezpieczeństwa.

Każdy cyberatak stanowi poważne przypomnienie o zagrożeniach, jakie niosą ze sobą cyberataki oraz o konieczności ciągłego rozwijania i wzmacniania systemów bezpieczeństwa informacyjnego.

Reakcja zarządzających na incydent może stanowić przykład, jak transparentność i odpowiedzialne podejście do zarządzania kryzysowego mogą pomóc w minimalizowaniu negatywnych skutków ataku oraz w odbudowie zaufania wśród użytkowników i inwestorów czego przykładem jest CD Projekt.

Poprzez analizę cyberataków podkreśliłam znaczenie inwestycji w zaawansowane systemy cyberbezpieczeństwa oraz ciągłej edukacji pracowników w zakresie najlepszych praktyk związanych z cyberbezpieczeństwem. Analizowane cyberataki ilustrują też potrzebę posiadania skutecznych planów reagowania na incydenty i strategii komunikacji kryzysowej, aby szybko i skutecznie odpowiadać na zagrożenia. Cyberprzestępczość stanowi rosnące ryzyko dla przedsiębiorstw, zagrażając ich ciągłości działania i reputacji. Z tego powodu, wdrożenie procedur zarządzania cyberbezpieczeństwem staje się coraz ważniejsze dla uzyskania przewagi konkurencyjnej na rynku.

Na kanwie czwartego rozdziału sformułowałam następujące wnioski:

1) Organizacje powinny opracować i wdrożyć procedury szybkiego reagowania na cyberincydenty, uwzględniając komunikację z interesariuszami.
2) W organizacjach powinny być regularnie audytowane i aktualizowane systemy zabezpieczeń, w celu dostosowania ich do nowych i istniejących cyberzagrożeń.
3) Inwestycje w zaawansowane technologie zabezpieczeń oraz w programy szkoleniowe dla pracowników powinny się zwiększać tak aby podnieść ogólny poziom cyberodporności organizacji.

W mojej opinii, funkcjonowanie jednostki gospodarczej w cyberprzestrzeni, która oferuje liczne ułatwienia, ale również generuje poważne zagrożenia, wymusza na kadrze zarządczej podjęcie strategicznych decyzji. Dlatego też, w celu zapewnienia stabilności i możliwości rozwoju, rekomenduję priorytetowe wzmacnianie działań w obszarze cyberbezpieczeństwa.

Na podstawie przeprowadzonych badań ankietowych ustaliłam, że znaczna część badanych przedsiębiorstw wdrożyła polityki i procedury ochrony danych, jednak ich stopień implementacji był zróżnicowany. W dużych i międzynarodowych podmiotach rozwiązania te miały charakter sformalizowany i były zintegrowane z systemem zarządzania, natomiast w mniejszych firmach często opierały się na intuicji kadry kierowniczej lub miały charakter incydentalny.

Na podstawie przeprowadzonych badań ankietowych sformułowałam kluczowe wnioski:

1) Wszystkie trzy kraje podejmują znaczące kroki w zakresie zarządzania cyberbezpieczeństwem, jednak różnią się pod względem stopnia zaawansowania i podejścia do szkoleń oraz budżetowania.
2) Niemcy przodują w tworzeniu oddzielnych budżetów i regularnych audytach, natomiast Polska wykazuje wysoką skłonność do korzystania z zewnętrznych firm szkoleniowych.
3) We Francji i Niemczech częstym motywem powstawania działów cyberbezpieczeństwa są wzrastające liczby cyberataków oraz wymogi prawne.

Występujące różnice w badanych przedsiębiorstwach wskazują na zróżnicowane podejście do cyberbezpieczeństwa.

Na podstawie przeprowadzonych wywiadów:

1) określiłam z jakimi trudnościami spotykają się przedsiębiorcy w obszarze zarządzania bezpieczeństwem informacji (tabela 4);
2) wskazałam jakiego rodzaju cyberataki będą się nasilały w najbliższym czasie: roku - pięciu lat (tabela 5);
3) sporządziłam analizę oceny potencjału sztucznej inteligencji w obszarze cyberbezpieczeństwa (tabela 6).

Tabela 4. Trudności w obszarze zarządzania bezpieczeństwem informacji w przedsiębiorstwie

Kłopoty	**Charakterystyka**
Braki kadrowe	– niedobór wykwalifikowanych specjalistów ds. bezpieczeństwa informacji stanowi poważne wyzwanie – brak zasobów ludzkich utrudnia firmom skuteczne wdrażanie polityk i procedur bezpieczeństwa oraz reagowanie na incydenty
Brak zrozumienia zagrożeń i wymagań legislacyjnych	– zarządy często nie rozumieją zagrożeń ani wymagań prawnych związanych z ochroną danych, co prowadzi do niedostatecznego finansowania i wsparcia dla działań związanych z cyberbezpieczeństwem
Niska świadomość i edukacja pracowników	– nawet najlepsze systemy ochrony są nieskuteczne, jeśli pracownicy nie przestrzegają podstawowych zasad bezpieczeństwa – edukacja i budowanie świadomości wśród pracowników są kluczowe
Koszty i inwestycje	– wdrażanie skutecznych systemów bezpieczeństwa informacji jest kosztowne, co stanowi obciążenie finansowe dla wielu małych i średnich przedsiębiorstw
Niedostateczne planowanie i integracja procesów	– przedsiębiorstwa często nie planują odpowiednich funduszy na cyberbezpieczeństwo, a także nie integrują procesów bezpieczeństwa informacji z innymi procesami biznesowymi

Źródło: opracowanie własne na podstawie wywiadów.

Przedsiębiorcy borykają się z wieloma problemami w zarządzaniu bezpieczeństwem informacji. Zarządy często nie rozumieją specyfiki cyberzagrożeń ani przepisów prawnych. Brakuje wykwalifikowanych specjalistów, a finansowanie jest niewystarczające. Procedury bezpieczeństwa nie są w pełni wdrażane w codzienne działania przedsiębiorstwa, często są też tworzone przez firmy zewnętrzne bez uwzględnienia specyfiki danego podmiotu, przez co nie są w ogóle stosowane. Problemem jest również brak regularnych szkoleń i świadomości wśród pracowników. Małe i średnie przedsiębiorstwa często nie mogą pozwolić sobie na wysokie koszty wdrożenia i utrzymania systemów bezpieczeństwa.

Tabela 5. Rodzaje cyberataków najbliższym czasie – roku – do pięciu lat

Rodzaj cyberataku	**Charakterystyka**
Phishing	– rodzaj ataku, który ewoluował i staje się coraz bardziej złożony, wykorzystując różne kanały komunikacji, takie jak e-mail, SMS oraz nowsze BLIK (wyłudzenie kodu BLIK)
Ataki DDoS	– rodzaj ataku obecnie mniej aktywne, mogące się nasilić, wykorzystując większe botnety oraz nowe technologie, takie jak IoT
Ataki na infrastrukturę IoT	– zwiększająca się liczba urządzeń IoT wpływa, że stają się one celem ataków, a przestępcy będą wykorzystywać luki w ich zabezpieczeniach
Ataki z użyciem sztucznej inteligencji	– wykorzystanie AI do przeprowadzania ataków będzie rosło – przestępcy mogą używać AI m.in.: do automatyzacji działań, tworzenia trudniejszych do wykrycia złośliwych programów, do wykorzystania deepfake'ów
Ransomware	– rodzaj ataki popularny z uwagi na jego skuteczność i widowiskowość – oprogramowanie wymuszające okup będzie coraz bardziej wyspecjalizowane i ukierunkowane na konkretne cele
Kradzież danych osobowych	– coraz bardziej zaawansowane metody kradzieży danych osobowych przechowywanych w chmurze

Źródło: opracowanie własne na podstawie wywiadów.

W najbliższych latach można spodziewać się nasilenia różnych rodzajów cyberataków m.in.: ataki wspierane przez Sztuczną Inteligencję (SI), ataki socjotechniczne, Ransomware, Phishing, ataki DDoS czy ataki na dostawców oprogramowania, które są podobne do ataku na SolarWinds, gdzie zainfekowane aktualizacje oprogramowania są rozsyłane do wielu klientów.

Tabela 6. Analiza SWOT: sztuczna inteligencja a cyberbezpieczeństwo

Mocne strony (*Strengths*) 1. **Szybkość i efektywność wykrywania zagrożeń**: Sztuczna inteligencja (SI) może analizować ogromne ilości danych w czasie rzeczywistym, co pozwala na szybsze wykrywanie zagrożeń, takich jak ataki DDoS czy próby nieautoryzowanego dostępu. 2. **Automatyzacja reakcji na incydenty**: SI może podejmować automatyczne działania, takie jak blokowanie podejrzanych adresów IP czy izolowanie zainfekowanych urządzeń, co skraca czas reakcji i zmniejsza obciążenie zespołów ds. bezpieczeństwa. 3. **Wykrywanie nowych zagrożeń**: Algorytmy uczenia nienadzorowanego pozwalają na identyfikację nowych typów ataków na podstawie wzorców i anomalii, co jest kluczowe w obronie przed nowymi i nieznanymi zagrożeniami. 4. **Wsparcie dla analityków**: SI może dostarczać analitykom szczegółowe raporty i analizy dotyczące incydentów, co wspomaga podejmowanie szybkich i skutecznych decyzji.	**Słabe strony (*Weaknesses*)** 1. **Zależność od jakości danych**: Skuteczność działania SI zależy od jakości i ilości danych treningowych. Niedostateczna ilość lub niska jakość danych może prowadzić do błędnych wyników. 2. **Potencjalne błędy w danych**: Błędy w danych wejściowych mogą prowadzić do fałszywych wyników, takich jak wykrywanie nieistniejących zagrożeń lub niewykrywanie prawdziwych ataków. 3. **Stronniczość algorytmów**: SI może wykazywać uprzedzenia, które są obecne w danych treningowych, co może wpływać na decyzje podejmowane przez systemy ochrony.
Szanse (*Opportunities*) 1. **Rozpoznawanie nietypowych zachowań**: Analiza behawioralna użytkowników systemów IT, np. w bankowości elektronicznej, pozwala na identyfikację podejrzanych działań i szybkie reagowanie na zagrożenia. 2. **Wsparcie dla Security Operations Centers (SOC)**: SI może wspierać pracę SOCów, umożliwiając bardziej efektywne zarządzanie zagrożeniami i incydentami bezpieczeństwa. 3. **Prognozowanie ryzyka**: Analiza danych historycznych i trendów przez SI pozwala na przewidywanie przyszłych zagrożeń i proaktywne podejście do cyberbezpieczeństwa	**Zagrożenia (*Threats*)** 1. **Wykorzystanie SI przez cyberprzestępców**: Cyberprzestępcy mogą używać SI do automatyzacji swoich działań, co pozwala na przeprowadzanie bardziej zaawansowanych i skutecznych ataków, takich jak spersonalizowane ataki phishingowe. 2. **Zaawansowane złośliwe oprogramowanie**: Złośliwe oprogramowanie oparte na SI może być trudniejsze do wykrycia i bardziej skuteczne, adaptując się do środowiska w celu uniknięcia detekcji. 3. **Dezinformacja i manipulacja informacjami**: Technologia deepfake oraz boty zarządzane przez SI mogą być wykorzystywane do szerzenia fałszywych informacji i manipulacji opinią publiczną, co stanowi poważne zagrożenie dla społeczeństwa i instytucji demokratycznych.

Źródło: opracowanie własne na podstawie wywiadów.

SI jest dynamicznym narzędziem, które może służyć zarówno obronie, jak i atakowi, w zależności od tego, kto i jak je wykorzystuje. SI ma potencjał, aby znacząco poprawić cyberbezpieczeństwo poprzez szybsze i bardziej efektywne wykrywanie oraz reagowanie na zagrożenia. Jednocześnie istnieją wyzwania związane z jakością danych oraz ryzyko wykorzystania SI przez cyberprzestępców. Kluczowe jest zatem ciągłe monitorowanie i doskonalenie systemów SI, aby maksymalizować ich pozytywny wpływ i minimalizować potencjalne zagrożenia.

Jednym z najbardziej istotnych rezultatów badania była identyfikacja dziesięciu kluczowych determinant zarządzania cyberbezpieczeństwem:

1) świadomość i edukacja pracowników,
2) wsparcie zarządu i integracja z procesami organizacji,
3) wyspecjalizowana kadra,

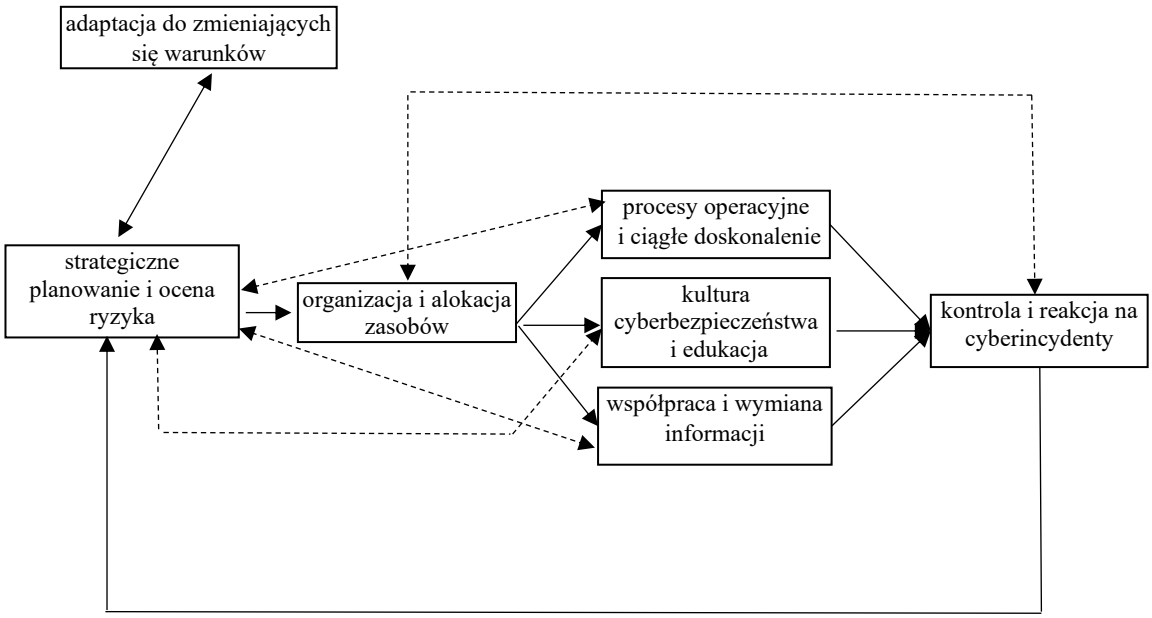
4) budżet i finansowanie,
5) wymagania prawne i regulacyjne,
6) technologie i narzędzia,
7) planowanie i zarządzanie ryzykiem,
8) reakcja na incydenty i zarządzanie kryzysowe,
9) adaptacja do zmieniających się cyberzagrożeń,
10) współpraca między działami i zewnętrznymi podmiotami.

Budowanie świadomości na wszystkich szczeblach organizacyjnych jest kluczowe dla utrzymania wysokiego poziomu cyberochrony. Pracownicy muszą być w pełni świadomi polityk bezpieczeństwa oraz aktualnych cyberzagrożeń. Wymaga to regularnych szkoleń, zarówno teoretycznych, jak i praktycznych, uwzględniających np. symulacje ataków phishingowych. Wsparcie ze strony kadry zarządczej oraz integracja procesów bezpieczeństwa z całością procesów firmowych są fundamentalne. Kadra zarządcza musi rozumieć istniejące cyberzagrożenia i aktywnie wspierać inicjatywy w zakresie cyberbezpieczeństwa. W obliczu braku kadrowego, wyspecjalizowani specjaliści ds. cyberbezpieczeństwa są niezbędni do skutecznego zarządzania systemami ochrony. Przedsiębiorstwa często napotykają trudności w rekrutacji i utrzymaniu odpowiednio wykwalifikowanego personelu. Adekwatne planowanie funduszy jest kluczowe i musi obejmować inwestycje w nowoczesne systemy ochrony, aktualizacje oprogramowania oraz regularne audyty. Wydatki na cyberbezpieczeństwo muszą być uzasadnione pod kątem ryzyka i efektywne kosztowo. Przestrzeganie wymagań prawnych, takich jak RODO czy NIS2 oraz dostosowanie się do krajowych i międzynarodowych regulacji, jest istotnym aspektem zarządzania cyberbezpieczeństwem, wpływającym na compliance organizacji. Stosowanie zaawansowanych technologii i narzędzi, które mogą być stale rozwijane i aktualizowane przez pracowników, może zwiększyć poziom cyberbezpieczeństwa często bez znaczących, jednorazowych nakładów finansowych. Wdrożenie metodyk zarządzania ryzykiem oraz tworzenie i testowanie planów ciągłości działania są obligatoryjne. Regularne aktualizacje polityk i procedur cyberbezpieczeństwa stanowią klucz do utrzymania skuteczności systemu cyberochrony. Szybkie i skuteczne reagowanie na cyberincydenty jest niezbędne. Wymaga to posiadania i regularnego testowania procedur na wypadek naruszeń bezpieczeństwa. Automatyzacja procesów reakcji może skrócić czas odpowiedzi i zmniejszyć obciążenie zespołów bezpieczeństwa. Konieczna jest ciągła adaptacja i elastyczne podejście do nowych rodzajów zagrożeń (np. ataki wspierane przez SI, oprogramowanie ransomware), co wymaga stałego monitorowania i ewaluacji środowiska zagrożeń. Kluczowa jest synergia działu cyberbezpieczeństwa z działami takimi jak IT, HR, administracja i finanse, niezbędna do holistycznego reagowania na zagrożenia. Wskazana jest również kooperacja z podmiotami zewnętrznymi (dostawcy usług, organy regulacyjne) w celu wymiany informacji i wdrażania najlepszych praktyk.

Przeprowadzona analiza wykazała, że największy wpływ na poziom odporności organizacji mają: zaangażowanie najwyższego kierownictwa, istnienie formalnych polityk i procedur bezpieczeństwa,

regularność szkoleń, przejrzystość komunikacji wewnętrznej oraz integracja zarządzania bezpieczeństwem z innymi procesami organizacyjnymi, takimi jak zarządzanie jakością, zarządzanie projektami czy zarządzanie ciągłością działania.

Na podstawie zidentyfikowanych determinant zarządzania cyberbezpieczeństwem w przedsiębiorstwie, opracowałam model zarządzania cyberbezpieczeństwem (Rysunek 1), który integruje najlepsze praktyki zarządcze z kluczowymi elementami bezpieczeństwa informacji. Model strukturyzuje zarządzanie cyberbezpieczeństwem w przedsiębiorstwie w ramach siedmiu głównych obszarów: strategiczne planowanie i ocena ryzyka, organizacja i alokacja zasobów, procesy operacyjne i ciągłe doskonalenie, kultura cyberbezpieczeństwa i edukacja, współpraca i wymiana informacji, kontrola i reakcja na incydenty, adaptacja do zmieniających się warunków.



Linie ciągłe oznaczają stałe, bezpośrednie i silne zależności, oznaczające, że dane obszary są ze sobą trwale zintegrowane i ich wzajemne oddziaływanie jest fundamentalne dla funkcjonowania modelu. `
Linie przerywane oznaczają relacje o charakterze dynamicznym, mniej bezpośrednim, wskazujące na procesy, które nie są ciągłe w tym samym stopniu co te symbolizowane przez linie ciągłe, ale są równie ważne dla skuteczności modelu.

Rysunek 1. Model zarządzania cyberbezpieczeństwem w przedsiębiorstwie
Źródło: opracowanie własne.

Pierwszy obszar, **strategiczne planowanie i ocena ryzyka**, koncentruje się na integracji cyberbezpieczeństwa z celami biznesowymi i wymogami regulacyjnymi. Zgodnie z koncepcją zarządzania Griffina, zarządzanie cyberbezpieczeństwem rozpoczyna się od strategicznego planowania, opartego na szczegółowej analizie ryzyka i długoterminowych celach przedsiębiorstwa. Kluczowe jest opracowanie kompleksowej strategii, obejmującej identyfikację zagrożeń i ocenę ryzyka, co prowadzi do stworzenia planów prewencyjnych i awaryjnych. Cyberbezpieczeństwo musi być integralną częścią strategii biznesowej, a inwestycje w ochronę powinny być postrzegane jako inwestycja w stabilność

i rozwój firmy, a nie tylko koszt. Ponadto, strategiczne planowanie musi uwzględniać obowiązujące regulacje prawne (np. RODO, NIS2), co jest kluczowe dla uniknięcia sankcji i budowania zaufania.

Kolejnym obszarem jest **organizacja i alokacja zasobów**, obejmująca wyspecjalizowaną kadrę, budżetowanie i inwestycje oraz strukturę organizacyjną. Skuteczne zarządzanie cyberbezpieczeństwem wymaga dostępu do wykwalifikowanych specjalistów, a organizacje powinny inwestować w rozwój ich kompetencji lub rozważyć outsourcing. Niezbędne są również odpowiednie środki finansowe na technologie ochronne, audyty i szkolenia, a budżet na cyberbezpieczeństwo powinien być elastyczny, by reagować na nowe zagrożenia. Kluczowa jest także właściwa struktura organizacyjna z jasno określonymi rolami i odpowiedzialnościami, od zarządzania ryzykiem po reagowanie na incydenty.

Następny obszar związany jest z **procesem operacyjnym i ciągłym doskonaleniem**, obejmującym koncepcje takie jak TQM, Kaizen, Six Sigma, Lean Management oraz Reengineering. Procesy zarządzania cyberbezpieczeństwem muszą być regularnie oceniane i doskonalone. Wykorzystanie metod ciągłego doskonalenia, takich jak cykl PDCA w ramach TQM czy podejście Kaizen, pozwala na adaptację do zmieniających się cyberzagrożeń. Zarządzanie cyberbezpieczeństwem wymaga również optymalizacji procesów pod kątem efektywności. Metody takie jak Lean Management (eliminacja marnotrawstwa) i Six Sigma (redukcja błędów) mogą usprawnić działania ochronne. Regularne audyty i analizy incydentów, oparte na Six Sigma, pomagają eliminować luki w zabezpieczeniach. W dynamicznym środowisku cyberzagrożeń organizacje muszą być gotowe na radykalne przekształcenia procesów bezpieczeństwa poprzez reengineering, co może obejmować wprowadzanie nowych technologii, zmiany strukturalne czy innowacyjne metody ochrony.

Kolejny obszar to **kultura cyberbezpieczeństwa i edukacja**, obejmująca świadomość, edukację, przewodzenie i motywację. Kluczowe jest budowanie świadomości na wszystkich poziomach organizacji. Pracownicy muszą znać politykę cyberbezpieczeństwa i być regularnie szkoleni z najlepszych praktyk, włączając w to symulacje incydentów, takie jak phishing. Systematyczna edukacja minimalizuje ryzyko cyberincydentów wynikających z błędów ludzkich. Skuteczne zarządzanie zespołami cyberbezpieczeństwa wymaga silnego przywództwa, które motywuje do osiągania celów i promuje kulturę, gdzie bezpieczeństwo informacji jest priorytetem. Liderzy powinni również inspirować innowacje i wspierać inicjatywy edukacyjne.

Kolejny obszar dotyczący **współpracy i wymiany informacji** obejmuje współpracę międzyoddziałową i zewnętrzną, a także benchmarking i adaptację najlepszych praktyk. Efektywne zarządzanie cyberbezpieczeństwem wymaga współpracy między działami w organizacji (np. IT, HR, finanse), co umożliwia lepsze zrozumienie zagrożeń i skoordynowane reagowanie. Przedsiębiorstwa powinny również aktywnie współpracować z zewnętrznymi podmiotami, takimi jak dostawcy usług cyberbezpieczeństwa czy organy regulacyjne, w celu wymiany informacji i najlepszych praktyk. Regularny benchmarking z liderami branży pozwala identyfikować luki i wdrażać sprawdzone rozwiązania, poprawiając własne procesy bezpieczeństwa.

Kontrola i reakcja na cyberincydenty stanowi kolejny obszar, obejmujący monitorowanie, audyty, reakcję na incydenty i zarządzanie kryzysowe. Regularne audyty cyberbezpieczeństwa oraz ciągłe monitorowanie systemów są niezbędne do utrzymania wysokiego poziomu ochrony. Benchmarking pomaga porównać polityki i procedury z najlepszymi praktykami rynkowymi. Stałe monitorowanie systemów IT i regularne audyty są kluczowe do wczesnego wykrywania zagrożeń i minimalizowania ryzyka. Firmy powinny wdrażać zaawansowane systemy monitorowania, umożliwiające szybką analizę danych i reagowanie na cyberincydenty. Automatyzacja procesów reakcji, np. izolacji zainfekowanych systemów, znacząco skraca czas reakcji i minimalizuje skutki. Zarządzanie kryzysowe powinno również obejmować komunikację wewnętrzną i zewnętrzną, aby zapewnić spójność działań. Audyty należy przeprowadzać regularnie, by ocenić skuteczność środków ochronnych i zidentyfikować obszary wymagające poprawy.

Ostatni obszar związany jest z **adaptacją do zmieniających się warunków**, obejmującą zarządzanie zmianą i adaptację do nowych cyberzagrożeń. W dynamicznym środowisku technologicznym cyberbezpieczeństwo wymaga elastyczności i gotowości do wdrażania nowych technologii. Zarządzanie zmianą obejmuje planowanie, komunikację i przezwyciężanie oporu, co jest kluczowe dla skutecznego wdrażania zmian technologicznych i proceduralnych. Cyberzagrożenia stale ewoluują (np. ataki SI, ransomware, zagrożenia IoT), dlatego organizacje muszą regularnie aktualizować swoje strategie i systemy ochrony. Ciągłe monitorowanie trendów i adaptacja do nich jest niezbędna dla skutecznej obrony przed nowymi wyzwaniami.

Podsumowanie i rekomendacje

Wyniki badań przedstawione w monografii, umożliwiające identyfikację determinant oraz zaproponowany przeze mnie model zarządzania cyberbezpieczeństwem w przedsiębiorstwie, stanowią oryginalny wkład w rozwój dorobku teoriopoznawczego w dziedzinie nauk o zarządzaniu i jakości. Rozszerzają one dotychczasowy stan wiedzy na temat praktyk zarządzania cyberbezpieczeństwem w organizacjach. Zidentyfikowane determinanty oraz zaproponowany model mogą posłużyć jako fundament do opracowania indywidualnych systemów i procedur ochrony informacji, dostosowanych do specyfiki strategii organizacji oraz dynamicznie zmieniającego się otoczenia.

Zaproponowany przeze mnie model zarządzania cyberbezpieczeństwem to zintegrowane podejście, łączące strategiczne planowanie, efektywność operacyjną, edukację, kontrolę i adaptację do zmieniających się warunków. Jego wdrożenie, dostosowane do specyfiki przedsiębiorstwa, może znacząco poprawić zarządzanie ryzykiem cybernetycznym, zwiększyć odporność na ataki i chronić kluczowe zasoby informacyjne. Skuteczna implementacja wymaga zaangażowania całej organizacji oraz regularnych przeglądów i aktualizacji, by sprostać nowym wyzwaniom w dynamicznym środowisku technologicznym.

Zarówno badania własne, jak i ogólnodostępne wskazują na potrzebę analizy i prezentacji mechanizmów zarządzania cyberbezpieczeństwem w przedsiębiorstwach, szczególnie w kontekście

rosnącej liczby incydentów w cyberprzestrzeni. Ryzyko cybernetyczne stanowi istotne zagrożenie dla ciągłości działania, reputacji i finansów firm, niezależnie od branży. Skuteczne zarządzanie cyberbezpieczeństwem, oparte na integracji działań, edukacji i adaptacji do dynamicznego środowiska zagrożeń, może stanowić źródło przewagi konkurencyjnej. Współcześnie funkcje cyberbezpieczeństwa coraz silniej wpływają na zarządzanie organizacją, wykraczając poza aspekty technologiczne. Przyszłość zarządzania cyberbezpieczeństwem w przedsiębiorstwie wiąże się z rozwojem technologii, takich jak sztuczna inteligencja i uczenie maszynowe, które znacząco zwiększają skuteczność wykrywania i przeciwdziałania cyberatakom

Działania związane z bezpieczeństwem informacyjnym muszą stać się kluczowym elementem działań i strategii współczesnych państw i organizacji. Trend coraz bardziej intensywnego korzystania ze świata cyfrowego będzie się wyłącznie pogłębiał, a co za tym idzie, ewoluować będą same zagrożenia (Barlińska, Małecka, Świątkowska, s. 80)

Dynamiczne zmiany w cyberprzestrzeni, niosące zarówno korzyści, jak i zagrożenia, wymagają od kadry zarządzającej podejmowania świadomych decyzji w zakresie wzmacniania bezpieczeństwa informacyjnego. Kluczowe znaczenie ma wdrażanie odpowiednich procedur, polityk oraz podnoszenie świadomości pracowników, gdyż zarządzanie przedsiębiorstwem w środowisku cyfrowym staje się jednym z największych wyzwań współczesności.

Analiza przeprowadzona w ramach monografii wykazała, że współczesne przedsiębiorstwa stają w obliczu coraz większej liczby i złożoności cyberzagrożeń, wynikających z dynamicznego rozwoju technologii informatycznych oraz zmieniającego się charakteru ataków. Kluczowym wnioskiem jest konieczność zintegrowanego podejścia do zarządzania cyberbezpieczeństwem, obejmującego nie tylko aspekty technologiczne, ale także organizacyjne, proceduralne oraz ludzkie.

Na podstawie zgromadzonego materiału badawczego oraz przeprowadzonej analizy ustaliłam, że założone cele monografii zostały spełnione. Dokonałam pozytywnej weryfikacji zarówno hipotezy głównej (HG), jak i hipotez szczegółowych (H1-H6), co umożliwiło mi sformułowanie następujących kluczowych konkluzji naukowych:

- Weryfikacja hipotezy głównej (HG)*: Zmieniające się cyberzagrożenia powodują określenie kluczowych determinant zarządzania cyberbezpieczeństwem w przedsiębiorstwie.* Hipotezę potwierdziłam poprzez definiowanie kluczowych determinant zarządzania cyberbezpieczeństwem. Na ich podstawie zaproponowałam autorski model zarządzania dedykowany przedsiębiorstwom. Ponadto wskazałam główne trudności w obszarze zarządzania bezpieczeństwem informacji, z którymi zmaga się kadra menedżerska, oraz dokonałam projekcji rodzajów cyberataków mogących wystąpić w horyzoncie czasowym od jednego do pięciu lat.
- Weryfikacja hipotezy szczegółowej (H1): *Zarządzanie cyberbezpieczeństwem w przedsiębiorstwie integruje kluczowe sekwencje zarządzania: planowanie, organizowanie,*

przewodzenie i kontrolowanie dostosowując je do potrzeb ochrony informacji w cyberprzestrzeni.

Hipotezę potwierdziłam poprzez wykazanie korelacji między definicją zarządzania cyberbezpieczeństwem a klasyczną definicją zarządzania w ujęciu Griffina (tabela 2).

- Weryfikacja hipotezy szczegółowej (H2): *Determinanty koncepcji zarządzania można wykorzystać do stworzenia modelu zarządzania cyberbezpieczeństwem w przedsiębiorstwie*.
  Hipotezę potwierdziłam poprzez wskazanie determinant ogólnych koncepcji zarządzania, które implementowałam w procesie tworzenia zintegrowanego systemu zarządzania cyberbezpieczeństwem (przedstawione w omówieniu osiągniętych wyników).
- Weryfikacja hipotezy szczegółowej (H3): *Regularne szkolenia wraz z budowaniem świadomości pracowników w zakresie cyberzagrożeń istotnie wpływają na zarządzenie cyberbezpieczeństwem w przedsiębiorstwie*.
  Hipotezę potwierdziłam empirycznie na podstawie rezultatów przeprowadzonych badań ilościowych i jakościowych, które udowodniły istotność wpływu świadomości i edukacji na efektywność zarządzania.
- Weryfikacja hipotezy szczegółowej (H4): *Wyodrębniony budżet cyberbezpieczeństwa to czynnik determinujący ogólny poziom procesów zarządzania cyberbezpieczeństwem w przedsiębiorstwie.*
  Hipotezę potwierdziłam na podstawie wyników badań ilościowych i jakościowych, które uzasadniły, że alokacja dedykowanych środków finansowych stanowi kluczowy czynnik determinujący dojrzałość procesów zarządzania cyberbezpieczeństwem.
- Weryfikacja hipotezy szczegółowej (H5): *Występują różnice w podejściu do cyberbezpieczeństwa biorąc pod uwagę rodzaj przedsiębiorstwa.*
  Hipotezę potwierdziłam na podstawie danych uzyskanych w badaniach ilościowych, które wykazały zróżnicowane podejścia i priorytety w zarządzaniu cyberbezpieczeństwem w zależności od typu (rodzaju) działalności przedsiębiorstwa.
- Weryfikacja hipotezy szczegółowej (H6): *Sztuczna Inteligencja stanowi wyzwanie dla przedsiębiorstwa w zakresie zarządzania cyberbezpieczeństwem.*
  Hipotezę potwierdziłam poprzez analizę wpływu Sztucznej Inteligencji na domenę cyberbezpieczeństwa, obejmującą identyfikację jej mocnych i słabych stron oraz określenie wynikających szans i zagrożeń (tabela 6).

Wnioski końcowe wskazują, że cyberbezpieczeństwo powinno być integralnym elementem misji i strategii organizacyjnej, a nie jedynie formalnym czy technicznym obowiązkiem. Podkreśliłam, że odporność organizacyjna kształtowana jest poprzez aktywne zaangażowanie liderów, inwestycje w rozwój kompetencji, zarządzanie procesowe oraz świadome budowanie kultury cyfrowej. W warunkach permanentnych zagrożeń nie wystarcza reakcja — konieczne jest podejście proaktywne, oparte na przewidywaniu, planowaniu i współpracy.

Wnioski uzyskane w ramach pracy mają wartość zarówno poznawczą, jak i aplikacyjną. Mogą stanowić podstawę do projektowania programów szkoleniowych, audytów bezpieczeństwa, benchmarkingu organizacyjnego oraz wspierać rozwój strategii cyfrowej transformacji w przedsiębiorstwach o zróżnicowanej wielkości i profilu działalności.

Przeprowadzone analizy i badania pozwoliły mi na sformułowanie następujących rekomendacji, mających na celu wsparcie kadry zarządczej w efektywniejszym zarządzaniu cyberbezpieczeństwem oraz ochronie przed narastającymi zagrożeniami w cyberprzestrzeni:

1. Aby lepiej wykrywać i reagować na cyberzagrożenia, przedsiębiorstwa niezależnie od wielkości, powinny zwiększyć częstotliwość audytów bezpieczeństwa IT.
2. Aby zwiększyć konkurencyjność, przedsiębiorstwa powinny regularnie aktualizować i przeglądać swoje polityki cyberbezpieczeństwa, zapewniając ich zgodność z najnowszymi standardami i praktykami w branży.
3. Kluczowa jest kontynuacja i intensyfikacja programów edukacyjnych i szkoleń dotyczących cyberbezpieczeństwa, aby pracownicy na wszystkich szczeblach byli świadomi zagrożeń i potrafili na nie odpowiednio reagować.
4. Aby skutecznie chronić się przed cyberzagrożeniami i korzystać z najnowszej wiedzy oraz technologii, przedsiębiorstwa powinny współpracować z zewnętrznymi firmami szkoleniowymi i ekspertami ds. cyberbezpieczeństwa.
5. Aby zminimalizować skutki potencjalnych cyberataków i szybko przywrócić normalne funkcjonowanie, przedsiębiorstwa powinny opracować i wdrożyć kompleksowe plany reakcji na cyberincydenty.

Wkład pracy do rozwoju nauk o zarządzaniu i jakości

Analiza zagadnień związanych z zarządzaniem cyberbezpieczeństwem w przedsiębiorstwie pozwoliła mi wykazać, że problematyka ta mieści się w obszarze nauk o zarządzaniu i jakości. Zgodnie z klasyfikacją przyjętą przez American Academy of Management (AOM, 2024), zagadnienie to wpisuje się w jedną z 26 dyscyplin zarządzania, określaną jako „komunikacja, technologia cyfrowa i organizacja”. Dyscyplina ta obejmuje interdyscyplinarne podejście do analizy procesów behawioralnych, społecznych i ekonomicznych zachodzących na styku komunikacji, technologii i organizacji. Szczególny nacisk kładzie się tu na zagadnienia komunikacyjne, które odzwierciedlają transformacje współczesnego środowiska pracy, możliwe dzięki wykorzystaniu zarówno istniejących, jak i nowo powstających technologii oraz systemów. Główne obszary badawcze koncentrują się na integracji elementów komunikacji, technologii i organizacji.

Osiągnięcie zawarte w monografii, stanowiące syntetyczne połączenie rozważań teoretycznych i ustaleń empirycznych, wprowadza istotny i oryginalny wkład poznawczy do dyscypliny nauk o zarządzaniu i jakości, jednocześnie znacząco poszerzając zakres wiedzy zarówno w ujęciu teoretycznym, jak i aplikacyjnym, w obszarze zarządzania cyberbezpieczeństwem w strukturach

organizacyjnych. Podjęta problematyka zarządzania cyberbezpieczeństwem w przedsiębiorstwie, mimo swojej aktualności i istotności praktycznej, pozostaje niedostatecznie zbadana w polskiej literaturze zarządzania, a niniejsza praca stanowi jedno z pierwszych tak kompleksowych badań w Polsce, integrujące aspekty techniczne, prawne, zarządcze, strategiczne, organizacyjne i kulturowe.

Osiągnięcie zawarte w monografii wnosi istotną wartość do dyscypliny nauk o zarządzaniu i jakości, co przejawia się w trzech wzajemnie uzupełniających się płaszczyznach:

1) wkład teoretyczny:
   - w pracy opracowałam autorską definicję zarządzania cyberbezpieczeństwem, która wykracza poza ujęcia inżynieryjne, definiując je jako *kompleksowy proces strategiczny i operacyjny, obejmujący identyfikację, ocenę i mitygację ryzyk związanych z cyberzagrożeniami. Zarządzanie cyberbezpieczeństwem integruje technologie, polityki, procedury oraz zasoby ludzkie w celu ochrony integralności, poufności i dostępności danych oraz systemów informatycznych. Efektywne zarządzanie cyberbezpieczeństwem polega na ciągłym monitorowaniu i analizowaniu zagrożeń, proaktywnym wdrażaniu środków ochronnych, edukacji i szkoleniu pracowników, a także współpracy z zewnętrznymi podmiotami w zakresie wymiany informacji i najlepszych praktyk. Fundamentem zarządzania cyberbezpieczeństwem jest adaptacja do dynamicznie zmieniającego się otoczenia technologicznego oraz regulacyjnego, z uwzględnieniem specyfiki działalności organizacji oraz jej strategicznych celów biznesowych.*
   - jako zintegrowany proces zarządczy obejmujący planowanie, organizowanie, motywowanie i kontrolowanie działań ukierunkowanych na ochronę zasobów informacyjnych, tym samym osadzając cyberbezpieczeństwo w rdzeniu teorii organizacji i zarządzania;
   - stworzony przeze mnie model zarządzania cyberbezpieczeństwem stanowi oryginalny konstrukt teoretyczny. Zintegrowałam w nim elementy zarządzania strategicznego, jakością, ryzykiem, wiedzą i projektami. Model ten pełni jednocześnie funkcje opisowe i normatywne w kontekście diagnozowania dojrzałości organizacyjnej oraz identyfikacji obszarów do doskonalenia.
2) Wkład empiryczny:
   - dostarczyłam unikalny zbiór danych dotyczących stanu i uwarunkowań zarządzania cyberbezpieczeństwem w państwach Trójkąta Weimarskiego (Polska, Niemcy, Francja). Umożliwiło mi to przeprowadzenie międzykulturowych badań porównawczych, skutkujących identyfikacją dobrych praktyk oraz oceną efektywności zastosowanych rozwiązań instytucjonalnych i regulacyjnych;
   - uzyskałam wyniki charakteryzujące się wysoką wartością poznawczą, które stanowią podstawę metodologiczną i informacyjną do dalszych, w tym międzynarodowych, badań porównawczych.,

3) Wkład praktyczny:
   - opracowałam zestaw rekomendacji aplikacyjnych skierowanych do kluczowych interesariuszy, w tym menedżerów, audytorów oraz doradców organizacyjnych. Rekomendacje te obejmują krytyczne aspekty zarządzania, takie jak metody planowania budżetu bezpieczeństwa, zasady wdrażania polityk informacyjnych, metody szkolenia personelu oraz zasady modelowania relacji między jednostkami odpowiedzialnymi za bezpieczeństwo;
   - poprzez moją pracę wpisałam się w misję nauk o zarządzaniu i jakości, aktywnie kształtując rzeczywistość organizacyjną w duchu efektywności, odpowiedzialności i innowacyjności, tym samym komplementarnie uzupełniając tradycyjną funkcję wyjaśniającą tej dyscypliny.

W odróżnieniu od licznych prac o charakterze teoretycznym, ogólnym lub skupiających się na pojedynczych aspektach, moja monografia łączy w sobie perspektywy zarządzania, prawa i technologii informacyjnych, opierając się na badaniach empirycznych przeprowadzonych w trzech krajach Unii Europejskiej. Prace I. C. Popa, M. Nastase i R. G. (CHIVU) Popa (Popa et. al., 2022) oraz N. Kshetri (Kshetri, 2021) podkreślają strategiczne znaczenie cyberbezpieczeństwa. R. Rajan, N. Rana, N. Parameswar, S. Dhir, S. Sushil, Y. K. Dwivedi (Rajan et. al., 2021) czy M. Frayssinet, D. Esenarro, F. F. Juárez, M. Díaz (Frayssinet et. al., 2021), przedstawiają ramy teoretyczne oparte na standardach, takich jak NIST. W literaturze można znaleźć prace koncentrujące się na elementach prawnych lub organizacyjnych. D. R. Jaworski i P. Opitek (Jaworski, Opitek, 2025) poruszają tematykę cyberprzestępczości w prawie karnym i kryminalistyce, a K. Chałubińska-Jentkiewicz i M. Nowikowska (Nowikowska, Chałubińska-Jentkiewicz. 2024) zajmują się ochroną danych osobowych w cyberprzestrzeni. C. Banasiński i M. Rojszczak (Banasiński, Rojszczak, 2020; Banasiński 2023) systematyzują polski i unijny krajobraz prawny. Z kolei Z. Zadorozhnyi, V. Muravskyi, O. Shevchuk (Zadorozhnyi et. al. 2021) analizują wpływ outsourcingu na bezpieczeństwo. A. Althonayan i A. Andronache (Althonayan, Andronache, 2019) badają związek zarządzania cyberbezpieczeństwem z zarządzaniem ryzykiem korporacyjnym. B. Payne (Payne, 2023), J. DiMaggio (DiMaggio , 2023) czy S. Enoka (Enoka, 2024) koncentrują się na obronie przed cyberatakami, strategiach blue teamów czy bezpieczeństwie w małych sieciach. Ich celem jest dostarczenie praktycznej wiedzy technicznej. Z kolei O. Negulescu, E. Doval i A. Stefanescu (Negulescu et. al., 2022) skupia się na aktualnych i przyszłych zagrożeniach cyfrowych. K. Sehgala i N. Thymianisa (Sehgal, Thymianis, 2024), omawiają operacyjne działania zespołów obronnych w organizacjach. J. M. Boyensa (Boyens, 2024) omawia zarządzanie ryzykiem w łańcuchu dostaw. Z kolei publikacje o charakterze filozoficznym i społecznym, Ł. Olejnika i A. Kurasińskiego (Olejnik, Kurasiński, 2022), podejmują refleksję nad etycznymi i ontologicznymi aspektami technologii cyfrowych.

Różnica jakościowa osiągnięcia zawartego w mojej monografii polega na tym, że te rozproszone elementy zostają scalone w spójną ścieżkę decyzyjno-wdrożeniową, zweryfikowaną empirycznie na gruncie UE i przełożoną na role, mierniki i praktyki zarządcze, które można wdrożyć „tu i teraz”

w polskim przedsiębiorstwie. Przedstawione osiągnięcia w monografii stanowią brakujący pomost między teorią i ramami koncepcyjnymi a rzeczywistością organizacji, w której cyberbezpieczeństwo ma stać się integralnym elementem strategii, zarządzania ryzykiem i codziennych procesów operacyjnych.

Ograniczenia badań

Zrealizowane postępowanie badawcze nie jest wolne od klasycznych ograniczeń dotyczących zaprojektowania badań, próby badawczej (Dyduch, 2015). Niektóre z nich wynikają z przyjętych założeń, metod oraz możliwości organizacyjnych i czasowych. Świadomie i transparentnie identyfikuję te ograniczenia, wskazując jednocześnie na możliwe kierunki ich wyeliminowania w przyszłości.

Po pierwsze, ograniczenia badania dotyczą jego zakresu podmiotowego. Choć próba badawcza była zróżnicowana i obejmowała głównie prywatne przedsiębiorstwa (zwłaszcza z sektora ICT narażonego na zagrożenia cyfrowe), sektor publiczny i administracja nie zostały uwzględnione w równym stopniu. To może ograniczać możliwość generalizacji wyników na inne typy organizacji.

Po drugie, ograniczeniem jest czasowy charakter badania. Zarówno technologie, jak i zagrożenia ewoluują bardzo szybko. Skuteczne dziś praktyki mogą okazać się niewystarczające w przyszłości, w obliczu wyzwań takich jak rozwój kryptografii kwantowej, autonomicznych systemów cyberwojennych czy nowych form manipulacji informacją (np. deepfake). Oznacza to, że uzyskane wnioski należy interpretować w kontekście dynamicznego otoczenia.

Kolejnym ograniczeniem jest złożoność badanych zjawisk i ryzyko ich uproszczenia. Mimo starań, nie wszystkie aspekty zarządzania cyberbezpieczeństwem łatwo zmierzyć czy uchwycić standaryzowanymi narzędziami badawczymi. Szczególnie trudne okazało się ujęcie elementów kultury organizacyjnej, nieformalnych relacji, poziomu zaufania czy osobistych motywacji menedżerów, które mają kluczowe znaczenie dla skuteczności działań w obszarze bezpieczeństwa.

W toku przeprowadzonej analizy bibliometrycznej dostrzegam pewne ograniczenia wynikające z przyjętych założeń metodologicznych, takich jak: wybór konkretnych baz danych, określenie ram czasowych, kryteria selekcji dokumentów, zastosowane słowa kluczowe, a także fragmentaryczność pozyskanych danych. Czynniki te mogą wpływać na trudność w pełnym uchwyceniu całokształtu literatury istotnej dla badanego zagadnienia. Pomimo tych ograniczeń, przeprowadzona przeze mnie analiza treści w ramach systematycznego przeglądu literatury umożliwiła wieloaspektowe ujęcie problematyki zarządzania cyberbezpieczeństwem.

Mimo wskazanych ograniczeń, procedura badawcza pozwoliła na zrealizowanie założonych celów. Przeprowadzone badania wnoszą wkład w dotychczasową wiedzę, jednocześnie stanowiąc podstawę do dalszych analiz.

Kierunki dalszych badań

Ograniczenia pracy, ale również jej wyniki i wnioski, stanowią inspirację dla prowadzenia badań m.in. w następujących obszarach:

1) pogłębienie badań sektorowych, np. w administracji publicznej, służbie zdrowia, edukacji czy małych i średnich przedsiębiorstwach, jest kluczowe ze względu na odmienną kulturę organizacyjną, strukturę decyzyjną i poziom zasobów każdego z nich, co znacząco wpływa na zarządzanie cyberbezpieczeństwem;
2) przeprowadzenie porównawczych badań międzynarodowych, obejmujących wszystkie kraje członkowskie Unii Europejskiej, państwa spoza UE (w tym kraje azjatyckie, amerykańskie i afrykańskie), pozwoliłby na identyfikację globalnych trendów, różnic kulturowych oraz skutecznych wzorców działania, które można adaptować do lokalnych warunków;
3) pogłębienie badań nad przywództwem cyfrowym, rolą liderów w kształtowaniu kultury bezpieczeństwa oraz procesami edukacyjnymi i rozwojem kompetencji pracowników, ze szczególnym uwzględnieniem analizy zachowań organizacyjnych w warunkach zagrożenia, stresu i presji czasowej, które często towarzyszą cyberincydentom;
4) badanie i analiza narzędzi oceny dojrzałości organizacyjnej w zakresie zarządzania bezpieczeństwem informacji, zarówno w formie audytów wewnętrznych, jak i certyfikacji zewnętrznych, co wspierałoby rozwój praktyk audytorskich, doradczych i szkoleniowych w obszarze bezpieczeństwa cyfrowego;
5) analiza skuteczności różnych strategii zarządzania w kontekście zmieniającego się krajobrazu cyberzagrożeń;
6) badanie wpływu regulacji i norm dotyczących cyberbezpieczeństwa na praktyki zarządzania w przedsiębiorstwach;
7) badanie roli czynnika ludzkiego w efektywnym zarządzaniu cyberbezpieczeństwem, w tym zagadnień związanych z zachowaniami pracowników oraz procesami szkoleniowymi.

Podsumowując, przedstawione w monografii badania nie wyczerpują w pełni potencjału problematyki zarządzania cyberbezpieczeństwem w przedsiębiorstwie. Mam jednak nadzieję, że posłużą one jako punkt wyjścia do dalszych rozważań i dyskusji naukowych, pozwalając na zwiększenie złożoności zaproponowanego modelu zarządzania cyberbezpieczeństwem i przyczyniając się do pogłębienia badań.

Literatura wykorzystana w podrozdziale 4.1 autoreferatu

1. Althonayan A., Andronache A. (2019), *Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management Alignment*, International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), IEE, DOI: 10.1109/CyberSA.2019.8899445.
2. AOM, *Changing your Division or Interest Group Selection* (2024), https://aom.org/network/divisions-interest-groups-(digs) (dostęp: 01.02.2025).
3. Banasiński C. (2023), *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, [w:] C. Banasinski (red.) *Cyberbezpieczeństwo Zarys wykładu*, Wolters Kluwer, Warszawa.
4. Banasiński C., Rojszczak M. (red.) (2020), *Cyberbezpieczeństwo*, Wolters Kluwer Polska, Warszawa.
5. Barlińska J., Małecka A., Świątkowska J. (2018), *Cyberbezpieczeństwo Charakterystyka, mechanizmy i strategie zaradcze w makro i mikro skali*, Texter, Warszawa.
6. Bednarowska Z. (2015), *Desk research - wykorzystanie potencjału danych zastanych w prowadzeniu badań marketingowych i społecznych*, Marketing i rynek, nr 7.

7. Boyens J., Smith A., Bartol N. (2024), Winkler K., Holbrook A., Fallon M., *Cybersecurity Supply Chain Risk Management for Systems and Organizations*, NIST Special Publication, NIST SP 800-161r1.
8. Czakon W. (2011), *Paradygmat sieciowy w naukach o zarządzaniu*, Przegląd Organizacji nr 11.
9. Czakon, W. (2020), *Podstawy metodologii badań w naukach o zarządzaniu*, Wyd. III rozszerzone, Wydawnictwo Nieoczywiste, Warszawa.
10. Czekaj J. (2000), *Zarządzanie informacją jako funkcja przedsiębiorstwa*, [w:] T. Borkowski, A. Marcinkowski, A. Oherow-Urbaniec (red.), W kręgu zarządzania. Spojrzenie multidyscyplinarne, Kraków.
11. Czekaj J. (2021), Ziębicki B. (red.), *Współczesne zarządzanie Koncepcje, metody, systemy*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków.
12. DiMaggio J. (2023), *Sztuka wojny cyfrowej. Przewodnik dla śledczego po szpiegostwie, oprogramowaniu ransomware i cyberprzestępczości zorganizowanej*, Helion, Gliwice.
13. Dunn M. C. (2008), *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*, Londyn Routledge.
14. Dyduch, W. (2015), *Cel i przebieg badań z wykorzystaniem metod ilościowych,* [w:] Czakon W. (red.), *Podstawy metodologii badań w naukach o zarządzaniu*, Wolters Kluwer Business, Warszawa.
15. Dyduch, W. (2015), *Ilościowe badanie i operacjonalizacja zjawiska w naukach o zarządzaniu,* [w:] Czakon W. (red.), *Podstawy metodologii badań w naukach o zarządzaniu*, Oficyna a Wolters Kluwer Business, Warszawa.
16. Dźwigoł H. (2015), *Założenia do budowy metodyki badawczej*, Zeszyty Naukowe Politechniki Śląskiej, Wydawnictwo Politechniki Śląskiej, tom 78, Gliwice.
17. Enoka S. (2024), *Cyberbezpieczeństwo w małych sieciach, Praktyczny przewodnik dla umiarkowanych paranoików*, Helion, Gliwice.
18. Frayssinet M., Esenarro D., Juárez F. F., Díaz M. (2021), *Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations*, 3C TIC. Cuadernos de desarrollo aplicados a las TIC, 10(2), September 2021, p. 123-141. https://doi.org/10.17993/3ctic.2021.102.123-141.
19. Gerring J. (2001), *Social science methodology: A criterial framework.* Cambridge University Press.
20. Grzegorczyk W. (red.) (2015), Wybrane problemy zarządzania i finansów, Wydawnictwo Uniwersytetu Łódzkiego, Łódź.
21. Jaworski D. R., Opitek P. (2025), *Cyberprzestępczość w prawie karnym i kryminalistyce. Kompendium wiedzy*, Difin.Warszawa.
22. Kshetri N. (2021), *Cybersecurity Management: An Organizational and Strategic Approach*, Toronto: University of Toronto Press.
23. Kvale S. (2010), *Prowadzenie wywiadów*, Wydawnictwo Naukowe PWN, Warszawa.
24. Malak K. (2007), *Bezpieczeństwo jako kategoria i zjawisko społeczne*, „Piotrkowskie Zeszyty Międzynarodowe", nr 2, Piotrków Trybunalski.
25. Negulescu O., Doval E. (2022), Stefanescu A., *Actual and future digital threats and their impact on civil and military cybersecurity management*, Defence Science Review No. 15, DOI: https://doi.org/10.37055/pno/158811.
26. Nowikowska M., Chałubińska-Jentkiewicz K. (2024), *Ochrona informacji w cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa.
27. Olejnik Ł., Kurasiński A. (2022), *Filozofia cyberbezpieczeństwa*, Wydawnictwo Naukowe PWN, Warszawa.
28. Payne B. (2023), Go H*ck Yourself. Proste wprowadzenie do obrony przed cyberatakami, Helion, Gliwice.
29. Pipkin D. L. (2002), *Bezpieczeństwo informacji Ochrona globalna przedsiębiorstwa*, Wydawnictwo Naukowo-Techniczne, Warszawa.
30. Pop I. C., Nastase M., Pop R. G. (2022), *Strategic cybersecurity management*, Proceedings of The 16th International management conference "Management and resilience strategies for a post-pandemic future" 3rd– 4th November 2022, Bucharest, Romania p. 557-564 https://conferinta.management.ase.ro/archives/2022/pdf_IMC_2022/3_15.pdf
31. Potejko P. (2009), *Bezpieczeństwo informacyjne*, [w:] K. A. Wojtaszczyk, A. Martesrska – Sosnowska (red.), Bezpieczeństwo państwa, Oficyna Wydawnicza ASPRA-JR, Warszawa.
32. Rajan R., Rana N., Parameswar N., Dhir S., Sushil S., Dwivedi Y. K. (2021), *Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management*, Technological Forecasting and Social Change, Volume 170, September 2021, https://doi.org/10.1016/j.techfore.2021.120872.
33. Schreier F. (2009), *On Cyberwarfare. „DCAF Horizon 2015 Working Paper"*. Vol. 7. Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center. Office of the Press Secretary. Department of Homeland Security. Washington.

34. Sehgal K., Thymianis N. (2024), *Cyberbezpieczeństwo i strategie blue teamów. Walka z cyberzagrożeniami w Twojej organizacji*, Helion, Gliwice.
35. Teczke J. (1996), *Metody i techniki zarządzania*, Akademia Ekonomiczna w Krakowie, Kraków.
36. Zadorozhnyi Z., Muravskyi V., Shevchuk O. (2021), *Influence of Organizational Factors and Forms of Accounting Outsourcing on Enterprise Cybersecurity*, 11th International Conference on Advanced Computer Information Technologies (ACIT), IEE, DOI: 10.1109/ACIT52158.2021.9548370.

4.2. Pozostałe osiągnięcia naukowo-badawcze

Pozostałe osiągnięcia naukowe obejmują okres po uzyskaniu stopnia naukowego doktora, czyli lata 2011-2025.

4.2.1. Osiągnięcia naukowe po uzyskaniu stopnia doktora

Od ponad dekady konsekwentnie rozwijam swoją działalność naukową, koncentrując się na problemach współczesnego zarządzania w kontekście transformacji cyfrowej, rosnącej niepewności oraz odpowiedzialności organizacji wobec otoczenia społecznego i państwowego. Moje badania wyróżniają się spójnością tematyczną i metodologiczną, a jednocześnie cechują się wieloaspektowością oraz interdyscyplinarnym podejściem do podejmowanych zagadnień. W ramach dyscypliny nauk o zarządzaniu i jakości moje badania koncentrują się wokół dwóch głównych nurtów, które wzajemnie się dopełniają, tworząc spójną wizję nowoczesnego zarządzania w warunkach zmiennego, cyfrowego i zglobalizowanego otoczenia. Dwa główne nurty tematyczne (zarządzanie organizacją w środowisku cyfrowym i niepewnym oraz strategiczne zarządzanie odpowiedzialnością i bezpieczeństwem narodowym), charakteryzują się szerokim zakresem problemowym. W ich obrębie wyodrębniam bardziej szczegółowe obszary badawcze, stanowiące podstawę pogłębionej analizy teoretycznej i empirycznej:

1. Zarządzanie organizacją w środowisku cyfrowym i niepewnym (cyfrowo-strategiczne zarządzanie ryzykiem):
    1) zarządzanie cyberbezpieczeństwem w przedsiębiorstwie;
    2) zarządzanie informacją, wiedzą i technologią w organizacjach;
    3) zarządzanie organizacją w warunkach niepewności i zmienności otoczenia;
2. Strategiczne zarządzanie odpowiedzialnością i bezpieczeństwem narodowym:
    1) zarządzenie w kontekście zrównoważonego rozwoju (ESG, CSR);
    2) zarządzania w sektorze zbrojeniowym oraz w obszarze szeroko pojętego bezpieczeństwa narodowego.

W nurcie pierwszym z*arządzanie organizacją w środowisku cyfrowym i niepewnym*, trzy obszary badań (*zarządzanie cyberbezpieczeństwem w przedsiębiorstwie, zarządzanie informacją, wiedzą i technologią w organizacjach, zarządzanie w warunkach niepewności i turbulentnego otoczenia*) łączy wspólny mianownik konieczność adaptacyjnego i systemowego zarządzania organizacją w warunkach ryzyka cyfrowego informacyjnego i strategicznego. W tym ujęciu cyberbezpieczeństwo, zarządzanie wiedzą i reagowanie na zmienność są nie tyle odrębnymi problemami co różnymi wymiarami jednego złożonego wyzwania jak zorganizować firmę by była odporna elastyczna i świadoma cyfrowo. W tym

nurcie rozwijam spójne podejście integrujące technologie kompetencje i strukturę organizacyjną tworząc model zarządzania oparty na przewidywaniu zagrożeń i zdolności do.

Jednym z najbardziej rozwiniętych i konsekwentnie prowadzonych kierunków badawczych w moim dorobku jest **zarządzanie cyberbezpieczeństwem w organizacjach**, szczególnie w sektorze przedsiębiorstw działających w otoczeniu cyfrowym. Obszar tych badań został ukształtowany jako odpowiedź na rosnące zapotrzebowanie praktyki gospodarczej oraz administracyjnej na skuteczne modele i strategie zarządzania bezpieczeństwem informacji i procesów cyfrowych, przy uwzględnieniu dynamicznego otoczenia technologicznego i prawnego. Badania prowadzone w tym zakresie cechują się interdyscyplinarnością, łącząc zarządzanie strategiczne, informatykę gospodarczą, zarządzanie ryzykiem oraz psychologię organizacji.

Podstawowe założenie teoretyczne niniejszego kierunku badań koncentruje się na redefinicji cyberbezpieczeństwa z wyłącznie technicznego aspektu funkcjonowania organizacji do rangi kluczowego komponentu strategii zarządzania. W ramach tego podejścia bezpieczeństwo cyfrowe jest traktowane jako integralny element klasycznych funkcji zarządzania, obejmujących planowanie, organizowanie, motywowanie i kontrolowanie.

Najważniejszym rezultatem moich badań w tym obszarze jest publikacja: *Zarządzanie cyberbezpieczeństwem w przedsiębiorstwie - doświadczenia wybranych państw Unii Europejskiej*" (Difin, 2024), w której zawarte jest główne osiągnięcie naukowe, o którym mowa w art. 219 ust. 1 pkt 2 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2021 r. poz. 478 z późn. zm.). Osiągnięcie zawarte w monografi szczegółowo omówiłam w podrozdziale 4.1 autoreferatu.

Obok monografii, poszczególne etapy realizowanych przeze mnie badań zostały również udokumentowane w innych publikacjach, które stanowią istotne uzupełnienie głównego opracowania, które wykazałam w podrozdziałach 1.1, 2.1 i 4.2 załącznika 4, m.in.:

- *[e_II.1.1_1]* **Antczak J.** (2021), *Zarządzanie przedsiębiorstwem w cyberprzestrzeni*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa, ISBN: 978-83-7523-914-0 2021 (s. 136).
- *[e_II.2.1_3]* **Antczak J.** (2022), *Zarządzanie cyberbezpieczeństwem w przedsiębiorstwach branży logistycznej* [w:] Woźniak J., Tarapata J. (red.), Odporność organizacji. Cyfryzacja, bezpieczeństwo, innowacje Difin, Warszawa s. 256-268, ISBN 978-83-8270-094-7.
- *[e_II.2.1_4]* **Antczak. J.** (2021), *Zarządzanie nakładami na cyberbezpieczeństwo w jednostce gospodarczej*, [w:] Kiełtyka L., Smoląg K. (red.), Wybrane uwarunkowania i determinanty rozwoju współczesnych przedsiębiorstw, DOM ORGANIZATORA, Towarzystwo Naukowe Organizacji i Kierownictwa, Toruń, s. 85-102, ISBN 978-83-7285-981-5.
- *[e_II.4.2_10]* **Antczak J.** (2020), C*osts of cybersecurity in an business enity*, Education of Economists and Managers *55*(1), s. 81–93, https://doi.org/10.33119/EEiM.2020.55.6.

Wyniki moich badań znalazły również odzwierciedlenie w referatach wygłoszonych na krajowych i międzynarodowych konferencjach naukowych które wykazałam w podrozdziale 5.1 załącznika 4, m.in.:

- XII Międzynarodowa Konferencja Naukowa *Wiedza i technologie informacyjne w kreowaniu przedsiębiorczości*, Olsztyn k/Częstochowy, 09-10.10.2025 r.
  - udział z wystąpieniem *Wpływ cyberataków na zarządzanie przedsiębiorstwem;*
- KM Conference 2024, Warszawa, 03-06.07.2024 r.
  - udział z wystąpieniem **Antczak J.** (współwystępująca Sołek-Borowska C.), *The impact of Petya'2027 cyberattack on business continuity;*
- Międzynarodowa konferencja naukowa *Jednostka i państwo w cyberprzestrzeni szanse i zagrożenia*, Bydgoszcz, 20-21.05.2024 r.
  - udział z wystąpieniem *Cyberbezpieczeństwo państw Trójkąta Weimarskiego;*
- XIV Konferencja Naukowa *Multimedia w Biznesie i Administracji, Technologie ICT we współczesnym zarządzaniu*, Częstochowa, 25.03.2021 r.
  - udział z wystąpieniem *Zarządzanie nakładami na cyberbezpieczeństwo w jednostce gospodarczej;*

W dynamicznie zmieniającym się otoczeniu społeczno-gospodarczym rośnie znaczenie badań nad odpornością organizacyjną, adaptacyjnością i zarządzaniem w warunkach kryzysowych. Dostrzegając ten problem, rozwijam od kilku lat obszar badawczy skupiający się na **zarządzaniu organizacją w warunkach niepewności i zmienności otoczenia.** Jest to obszar szczególnie aktualny w kontekście postępującej globalizacji, pandemii COVID-19, wojny na Ukrainie, zakłóceń łańcuchów dostaw, kryzysów energetycznych i transformacji cyfrowej, które zmieniają nie tylko uwarunkowania działania organizacji, ale także sposoby ich adaptacji do zmiennego otoczenia.

Podstawą teoretyczną tego obszaru jest przyjęcie założenia, że zdolność organizacji do przetrwania i rozwoju w warunkach niepewności zależy nie tylko od posiadanych zasobów, ale przede wszystkim od zdolności zarządczych do szybkiego diagnozowania zmian, reagowania na zakłócenia oraz wykorzystywania zmian jako szansy na rozwój. W moich pracach koncentruję się zarówno na analizie czynników zewnętrznych – takich jak makrootoczenie, zmienność regulacyjna i sytuacje kryzysowe – jak i na aspektach wewnętrznych, w tym przywództwie, kulturze organizacyjnej oraz zdolności do transformacji cyfrowej.

Wnioski wynikające z prowadzonych rozważań zostały zaprezentowane w formie publikacji naukowych oraz wystąpień konferencyjnych, które wykazałam w podrozdziale 4.1 oraz 5.1 załącznika 4, m.in.:

- *[e_II.4.2_1]* **Antczak J.** (2024), *Determinants of business management in the digital age*, International Journal of Contemporary Management, Management, https://doi.org/10.2478/ijcm-2023-0017.

- *[e_II.4.2_5]* **Antczak J.** (2023), *Finance management in a turbulent environment on the example of a company operating in the video games industry*, Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 2023 Nr. 186 s. 7-24, DOI 10.29119/1641-3466.2023.168.1
- *[e_II.4.2_2]* **Antczak J.**, Nowakowska-Grunt J. (2023), *Zarządzanie cyberbezpieczeństwem podmiotów gospodarczych w kontekście wyzwań pandemii COVID-19*, Przegląd organizacji 4/2023, s. 439-446 DOI: 10.33141/po.2023.04.45.
- *[e_II.4.2_8]* **Antczak. J.**, Horzela I. (2021), *Home office as new approach to smart city idea in pandemic time*, Procedia Computer Science, vol. 192, s. 3832-3847, https://doi.org/10.1016/j.procs.2021.09.158.
- XIII Konferencja naukowa *Nowoczesne koncepcje i metody zarządzania, Innowacyjne zarządzanie w organizacjach komercyjnych, publicznych i społecznych w aspekcie bezpieczeństwa – obszary, szanse, wyzwania, perspektywy*, Stryków k. Łodzi, 23-24.11.2023 r.
    - udział z wystąpieniem Wpływ turbulentnego otoczenia na zarządzanie przedsiębiorstwem działającym w branży intermodalnej;
- X Konferencja Naukowa *Wiedza i technologie informacyjne w kreowaniu przedsiębiorczości,* Olsztyn k/Częstochowy, 05-06.10.2023 r.
    - udział z wystąpieniem *Cyberbezpieczeństwem jednostki gospodarczej w czasie pandemii COVID-19;*
- Konferencja naukowa *Zarządzanie organizacjami w erze cyfrowej Wyzwania, trendy koncepcje*, Zakopane, 14-16.09.2023 r.
    - udział z wystąpieniem *Determinanty zarządzania przedsiębiorstwem w erze cyfrowej;*

W omawianym obszarze ważne znaczenia ma umiejętne łączenie teorii z praktyką, co przejawia się w doborze przypadków badawczych. Korzystam m.in. z analiz konkretnych firm i branż, uwzględniając ich specyfikę, potrzeby adaptacyjne i ograniczenia. W swoich pracach posługuje się podejściem systemowym i kompleksowym.

Wyniki badań prowadzonych w ramach tego obszaru wykazują, że jednym z podstawowych warunków przetrwania i wzrostu organizacji w turbulentnym otoczeniu jest integracja podejścia strategicznego z operacyjnym. Organizacje muszą być w stanie nie tylko szybko reagować na zakłócenia, ale również wykorzystywać je jako okazje do wdrażania innowacji, zmian strukturalnych i transformacji cyfrowej. Takie podejście umożliwia osiąganie przewagi konkurencyjnej opartej na zdolności adaptacyjnej, a nie wyłącznie na optymalizacji kosztów czy przewidywalności.

W dobie cyfrowej transformacji oraz wzrastającej roli zasobów niematerialnych, takich jak dane, wiedza i kompetencje, jednym z istotnych obszarów badawczych jest **zarządzania informacją, wiedzą oraz technologią w organizacjach.** Obszar tych badań rozwija się na pograniczu zarządzania strategicznego, zarządzania zasobami ludzkimi, informatyki ekonomicznej oraz zarządzania bezpieczeństwem informacji, a jego wspólnym mianownikiem jest przekonanie, że wiedza i informacja

stają się kluczowymi aktywami XXI wieku – aktywami, które należy chronić, doskonalić i strategicznie wykorzystywać.

Traktuję informację nie tylko jako przedmiot przetwarzania technologicznego, ale również jako zasób organizacyjny, zarządzany analogicznie do zasobów ludzkich czy finansowych. Szczególne znaczenie przypisuję digitalizacji procesów, bezpieczeństwu informacji, zarządzaniu wiedzą nieformalną oraz roli kultury organizacyjnej w transferze i ochronie wiedzy. Zagadnienia te osadzam w szerszym kontekście przemian społeczno-technologicznych, w tym automatyzacji, robotyzacji i sztucznej inteligencji, które redefiniują role pracowników i menedżerów.

Publikacje w tym zakresie które wykazałam w podrozdziałach 2.1 i 4.1 załącznika 4, to m.in.:

- *[e_II.2.1_2]* **Antczak J.** (2023), *Zarządzanie bezpieczeństwem informacji w jednostce gospodarczej* [w:] Kiełtyka L. (red.) Wykorzystanie technik informacyjnych w zarządzaniu, Wydawnictwo Politechniki Częstochowskiej, Częstochowa, s. 99-114, ISBN 978-83-7193-933-4
- *[e_II.4.2_6]* **Antczak J.**, Dębicka E., Nowakowska-Grunt J. (2023), *Wybrane aspekty zarządzania bezpieczeństwem informacji w organizacjach w świetle współczesnych wyzwań gospodarki. Przykład przedsiębiorstw działających w Polsce*, Studia Wschodnioeuropejskie Nr ekspercki 19-t. 2/2023, s. 311-335, DOI:10.31971/24500267.20.14
- *[e_II.2.1_5]* **Antczak J.** (2019), *Cybersecurity management in the light of ISO standards requirements*, [w:] Soliman K. S. (red.) Proceedings of the 34th International Business Information Management Association Conference (IBIMA), Vision 2025: Education Excellence and Management of Innovations through Sustainable Economic Competitive Advantage, Madrid,s. 12724 – 12737, ISBN: 978-0-9998551-3-3.

Rezultaty prowadzonych analiz znalazły odzwierciedlenie w prezentacjach wygłoszonych podczas konferencji, które wykazałam w podrozdziale 5.1 załącznika 4, m.in.:

- XI Międzynarodowa Konferencja Naukowa *Wiedza i technologie informacyjne w kreowaniu przedsiębiorczości*, Olsztyn k/Częstochowy, 10-11.10.2024 r.
    - udział z wystąpieniem *Sztuczna inteligencja a cyberbezpieczeństwo – analiza SWOT*
- XV Konferencja naukowa *Multimedia w biznesie i administracji*, Koszęcin, 22-24.03.2023 r.
    - udział z wystąpieniem *Zarządzanie bezpieczeństwem informacji w jednostce gospodarczej*;
- V Międzynarodowa Konferencja Naukowa *Dylematy Badań naukowych w różnych dziedzinach nauki*, Katowice, 27.06.2019 r.
    - udział z wystąpieniem *Zarządzanie cyberbezpieczeństwem w świetle wymagań norm ISO*;

Konsekwentnie podkreślam, że informacja nie może być zarządzana w oderwaniu od człowieka – nawet najbardziej zaawansowany system informatyczny nie zapewni pełnego bezpieczeństwa, jeśli

zawiedzie czynnik ludzki. Z tego względu szczególną uwagę poświęcam edukacji pracowników i rozwojowi kompetencji cyfrowych.

Obszar badawczy dotyczący zarządzania informacją, wiedzą i technologią jest odpowiedzią na jedno z najpoważniejszych wyzwań współczesnego zarządzania. W świecie, w którym informacja stała się walutą, bronią i zasobem, moje prace oferują nie tylko diagnozę problemów, ale i konkretne narzędzia do ich rozwiązywania – a tym samym stanowią ważny wkład w rozwój i profesjonalizację polskiej oraz europejskiej szkoły zarządzania.

W nurcie drugim *Strategiczne zarządzanie odpowiedzialnością i bezpieczeństwem narodowym*, dwa obszary badań (*zarządzenie w kontekście zrównoważonego rozwoju, zarządzanie w sektorze obronnym i bezpieczeństwa narodowego*) dotyczą organizacji podwyższonej odpowiedzialności społecznej niezależnie od tego czy chodzi o środowiskową odpowiedzialność firm cywilnej czy o strategiczne funkcjonowanie obronności i bezpieczeństwo publiczne. W obu przypadkach analizuje systemy zarządzania z perspektywy wartości (etyka, odpowiedzialność, ład korporacyjny) oraz instytucjonalnych ram działania.

Obszar badań związany z **zarządzaniem w kontekście zrównoważonego rozwoju** łączy perspektywę etyczną, strategiczną i operacyjną zarządzania, z naciskiem na odpowiedzialność społeczną i środowiskową. Moje badania w tym zakresie są odpowiedzią na wzrastające oczekiwania społeczne, inwestorskie i regulacyjne wobec organizacji, by działały nie tylko efektywnie ekonomicznie, ale również odpowiedzialnie wobec ludzi, środowiska i interesariuszy.

Podstawową przesłanką tego nurtu jest przekonanie, że zarządzanie w XXI wieku nie może być rozumiane wyłącznie jako dążenie do maksymalizacji zysku, ale powinno opierać się na trójwymiarowym podejściu do wartości: ekonomicznych, społecznych i środowiskowych. W swoich publikacjach i wystąpieniach naukowych konsekwentnie pokazuje, że strategia ESG (Environmental, Social, Governance) to nie moda czy wymóg formalny, lecz kluczowy czynnik długofalowego sukcesu i odporności organizacji.

Wnioski wynikające z prowadzonych rozważań zostały zaprezentowane w formie publikacji naukowych oraz wystąpień konferencyjnych, które wykazałam w podrozdziałach 2.1 i 4.1 oraz 5.1 załącznika 4, m.in.:

- *[e_II.2.1_1]* **Antczak J.,** Nowakowska-Grunt J., Ciąder-Jackowiak J. (2025), *Praca przymusowa w standardach odpowiedzialności biznesowej: wdrażanie procedur przeciwdziałania ich wpływ na jakość zarządzania łańcuchem dostaw* [w:] Jasińska J. (red.) Problematyka normalizacji, jakości i kodyfikacji w aspekcie integracji NATO z Unią Europejską, Jakość – problemy i rozwiązania część IX, Wydawnictwo PPH Remigraf Sp. Z o.o., Warszawa s. 5-14, ISBN 978-83-7938-454-9.
- *[e_II.4.2_3]* **Antczak J.,** Nowakowska-Grunt J., Ciąder-Jackowiak J. (2023), *Decent work as an element of organization management in the context of sustainable development*, Zeszyty

Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 2023 Nr. 189 s. 25-43, http://dx.doi.org/10.29119/1641-3466.2023.189.2

- XIX Konferencja Centrum Certyfikacji *Jakości Problematyka normalizacji, jakości i kodyfikacji w aspekcie integracji z NATO i Unią Europejską jakość – problemy i rozwiązania,* Żnin 22-24.09.2025 r.
    - Udział z wystąpieniem *Praca przymusowa w standardach odpowiedzialności biznesowej: wdrażanie procedur przeciwdziałania i ich wpływ na jakość zarządzania łańcuchem dostaw*
- XIV Konferencja Naukowa *Nowoczesne koncepcje i metody zarządzania Zarządzanie organizacją w warunkach niepewności i zmienności otoczenia*, Warszawa, 14-15.11.2024 r.
    - udział z wystąpieniem (współwystępujący Nowkaowska-Grunt J., Ciąder-Jackowiak J.) *Etyczne aspekty godnej pracy w zrównoważonym zarządzaniu łańcuchem dostaw*;
- VIII Międzynarodowa Konferencja naukowa „*SCIENCE 2 BUSINESS*" oraz Forum'24 Kobieta między przestrzenią prywatną a publiczną, Częstochowa, 07-08.03.2024 r.
    - udział z wystąpieniem *Aspect of decent work in norms and law;*
- XVI konferencja Naukowa *Nowoczesne metody zarządzania przedsiębiorstwem, miastem i regionem, Zrównoważony rozwój organizacji*, Karpacz, 19-20.10.2023 r.
    - udział z wystąpieniem *Godna praca jako element zarządzania organizacją w kontekście zrównoważonego rozwoju*;

Badania w zakresie zarządzania w kontekście ESG i zarazem zrównoważonego rozwoju stanowią odpowiedź na potrzeby nauki i praktyki zarządzania, wykraczającą poza tradycyjny model ekonomiczno-instrumentalny. Pokazuje, że w centrum uwagi menedżerów musi znaleźć się człowiek, wspólnota i planeta – nie jako przeszkody, lecz jako fundamenty trwałego sukcesu organizacji.

W zakresie opisywanego obszaru w 2023 r. wraz z dr hab. J. Nowakowską-Grunt rozpoczęłyśmy współpracę z przedsiębiorstwem, Litex Promo Sp. z o.o. (Spółka Grupy Kapitałowa Lubawa) w ramach której przygotowałyśmy i wdrożyłyśmy Procedurę: Przeciwdziałania pracy przymusowej w ramach Procesu: Polityki ochrony praw człowieka**,** co szczegółowo przedstawiłam w podrozdziale 5.3 niniejszego autoreferatu.

Wśród rozwijanych przeze mnie kierunków badawczych istotne miejsce zajmuje problematyka **zarządzania w sektorze zbrojeniowym oraz w obszarze szeroko pojętego bezpieczeństwa narodowego**. Obszar ten jest szczególny z kilku powodów: po pierwsze, dotyczy sektora o kluczowym znaczeniu dla suwerenności i stabilności państwa; po drugie, jest silnie zintegrowany z polityką publiczną, wymogami międzynarodowymi (np. NATO, UE), a także uwarunkowaniami makroekonomicznymi, po trzecie, łączy elementy zarządzania strategicznego, finansowego, jakościowego i technologicznego – w kontekście organizacji o szczególnej odpowiedzialności społecznej i politycznej.

Punktem wyjścia dla tego nurtu badawczego są zagadnienia związane z efektywnością funkcjonowania przedsiębiorstw sektora obronnego oraz instytucji wspierających bezpieczeństwo państwa. Analizuję zarówno aspekty organizacyjne i finansowe tych podmiotów, jak i ich wpływ na gospodarkę, innowacyjność i spójność społeczną. Szczególne znaczenie przypisuję aspektom systemowym, takim jak strategia rozwoju sektora, współpraca międzyorganizacyjna, standardy jakości i bezpieczeństwa, a także integracja koncepcji ESG w sektorze uznawanym dotychczas za „twardy" i odporny na presję społeczną.

Prowadzone przeze mnie badania w tym obszarze doprowadziły do opracowania i publikacji współautorskiej monografii:

- *[e_II.1.1_2]* **Antczak J.**, Błażejczyk T., Kamola J., Korol K., Młynarski Sz. (2021), *Konkurencyjność przedsiębiorstw z branży zbrojeniowej – aspekty finansowe*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa, ISBN: 978-83-8263-102-9 (s. 141).

Książka ma dualny charakter: teoretyczno-praktyczny. W pracy skoncentrowaliśmy się na identyfikacji i analizie czynników wpływających na konkurencyjność przedsiębiorstw sektora zbrojeniowego z perspektywy finansowej. Wskazujemy, że sektor zbrojeniowy mimo strategicznego charakteru, nie jest wolny od ryzyk typowych dla gospodarki rynkowej, takich jak fluktuacje popytu, presja regulacyjna czy zależność od zamówień publicznych. Wnioski płynące z naszych analiz wskazują jednoznacznie, że stabilność oraz efektywność finansowa stanowią kluczowe determinanty pozycji konkurencyjnej przedsiębiorstw z branży zbrojeniowej, zarówno na rynku krajowym, jak i międzynarodowym. Szczególną uwagę poświęciliśmy analizie wskaźników płynności finansowej oraz struktury kapitałowej, które w istotny sposób wpływają na zdolność przedsiębiorstw do realizacji kontraktów, inwestycji oraz długofalowego rozwoju. Analiza finansowa stanowi istotne narzędzie zarządcze, dostarczając kierownictwu rzetelnych i uporządkowanych informacji na temat sytuacji finansowej przedsiębiorstwa. Wspiera proces podejmowania decyzji, pełni funkcję kontrolną i nadzorczą, a także odgrywa kluczową rolę we wspomaganiu zarządzania strategicznego. Zidentyfikowaliśmy również szereg barier ograniczających ekspansję eksportową, w tym czynniki regulacyjne, polityczne i finansowe, które determinują możliwości internacjonalizacji działalności firm z branży obronnej. W oparciu o uzyskane wyniki sformułowaliśmy rekomendacje dotyczące poprawy konkurencyjności, obejmujące m.in. zwiększenie efektywności operacyjnej, dywersyfikację źródeł finansowania oraz podniesienie poziomu przejrzystości finansowej. Nasze opracowanie ma charakter aplikacyjny i może stanowić punkt wyjścia do dalszych badań nad finansowymi aspektami funkcjonowania przedsiębiorstw sektora zbrojeniowego w kontekście ich zdolności konkurowania w dynamicznie zmieniającym się otoczeniu rynkowym.

Wśród publikacji w tym obszarze pragnę wymienić następujące artykuły, które wykazałam w podrozdziale 4.2 załącznika 4:

- *[e_II.4.2_4]* **Antczak J.,** Mitkow S., Roszkiewicz M. (2023), *Zarządzanie innowacjami w przemyśle zbrojeniowym przy współpracy startupu jako istotny element budowy*

bezpieczeństwa w dobie zagrożenia ze Wschodu, Studia Wschodnioeuropejskie Nr 19/2023, s. 222-249, DOI:10.31971/24500267.19.18;

- *[e_II.4.2_7]* **Antczak J.**, Mitkow S., Roszkiewicz M. (2022), *Challenges for the Defense Industry Against the Background of ESG (Environmental, Social, Governance)*, Concepts European Research Studies Journal, Volume XXV, Issue 4, 177-194, DOI: 10.35808/ersj/3074;
- *[e_II.4.2_9]* **Antczak J.**, Horzela I., Nowakowska-Krystamn A. Moskal-Niewczas J. (2021), *Value creation of a defence industry in a new communication and information environment,* Wiedza Obronna 2021, t. 276, nr 3, s. 90-122, https://doi.org/10.34752/2021g276.

Przytoczone publikacje są publikacjami współautorskimi, w których dokonujemy analizy różnych obszarów związanych z przemysłem zbrojeniowym.

Rezultaty analiz empirycznych znalazły odzwierciedlenie w prezentacjach konferencyjnych, stanowiąc podstawę do sformułowania wniosków przedstawionych podczas wystąpień, które wykazałam w podrozdziale 5.1. załącznika 4, jak m.in.:

- VI Krajowa konferencja naukowa z cyklu Społeczeństwo, Gospodarka, Siły Zbrojne *Odporność państwa, społeczeństwa i gospodarki na zagrożenia,* Warszawa, 06.12.2023 r.
    - udział z wystąpieniem (współwystępujący Chmielarczyk K.), *ESG w strategiach rozwoju wybranych grup zbrojeniowych;*
- XVI Konferencja Centrum Certyfikacji i Jakości Problematyka normalizacji, jakości i kodyfikacji w aspekcie integracji z NATO i Unią Europejską, Ryn, 27-30.09 2022 r.
    - udział z wystąpieniem *Przemysł zbrojeniowy a koncepcja ESG*;
- VI Krajowa Konferencja Naukowa-Przemysłowa z cyklu *Przedsiębiorstwa przyszłości polskiego przemysłu obronnego,* Warszawa, 03.06.2022 r.
    - udział z wystąpieniem (współwystępujący Roszkiewicz M.), *Wyzwania dla przemysłu obronnego na tle ESG;*

W analizach swoich czy to współautorskich podkreślam, że skuteczne zarządzanie w sektorze zbrojeniowym wymaga nie tylko zaawansowanej wiedzy technicznej, lecz przede wszystkim rozwiniętych kompetencji menedżerskich – zdolności do przewidywania, podejmowania decyzji w warunkach ryzyka, efektywnego zarządzania zasobami strategicznymi oraz budowania zaufania społecznego.

Ukazuje, że sektor zbrojeniowy nie musi pozostawać na marginesie dyskursu o zrównoważonym rozwoju i etyce w zarządzaniu. Przeciwnie – może on stanowić przykład wdrażania zasad ESG w szczególnie wymagających warunkach operacyjnych. Tym samym proponowane przeze mnie podejście integruje klasyczne badania z zakresu administracji publicznej i ekonomii obronnej z nowoczesnymi koncepcjami zarządzania strategicznego i jakościowego.

Reasumując, moja działalność naukowa jest osadzona w dyscyplinie nauki o zarządzaniu i jakości, charakteryzując się jednocześnie teoretyczną złożonością i interdyscyplinarnością. W moich pracach

łączę różne paradygmaty badawcze, integrując klasyczne ujęcia zarządzania z nowoczesnymi koncepcjami zrównoważonego rozwoju, cyberbezpieczeństwa, odporności organizacyjnej i zarządzania wiedzą. Każdy z omówionych nurtów stanowi mój samodzielny wkład w rozwój nauk o zarządzaniu i jakości, a łącznie tworzą one kompleksową, aktualną i aplikacyjną wizję zarządzania organizacją w warunkach XXI wieku.

W zakresie opisywanego obszaru w 2020 r. realizowałam staż badawczy w Polskiej Grupie Zbrojeniowej. Zakres stażu dotyczył działalności przedsiębiorstw w ramach Grupy kapitałowej, ze szczególnym uwzględnieniem prowadzenia wspólnych prac badawczo-rozwojowych oraz zajęć dydaktycznych w ramach studiów podyplomowych, co szczegółowo przedstawiłam w podrozdziale 5.2. niniejszego autoreferatu.

Zaprezentowane obszary wpisują się w profil Instytutu Zarządzania, Wydziału Bezpieczeństwa, Logistyki i Zarządzania WAT i zakres prowadzonych w niej badań naukowych. Moja dalsza aktywność akademicka będzie w dużej mierze oparta na kontynuacji kierunków badawczych rozwijanych w dotychczasowej działalności naukowo-badawczej.

Moje prace badawcze zostały docenione i w 2024 r. otrzymałam dyplom uznania za aktywność naukową oraz wysoko punktowane publikacje naukowe, przyznany przez płk prof. dr hab. Szymona Mitkowa, Dziekana Wydziału Bezpieczeństwa, Logistyki i Zarządzania. W 2020 r. otrzymałam również jednorazowe stypendium naukowe od gen. bryg. dr inż. Ryszarda Parafianowicza Rektora Akademii Sztuki Wojennej.

W ramach mojej działalności naukowo-badawczej aktywnie uczestniczę w rozwoju dyscypliny poprzez recenzowanie artykułów naukowych i monografii, przyczyniając się tym samym do podnoszenia jakości oraz poziomu merytorycznego publikacji naukowych. Wykaz zrecenzowanych prac stanowi punkt 11 załącznika 4.

Uczestniczę w szkoleniach, które pomagają mi rozwijać mój warsztat naukowo-badawczy, m.in.:

- październik 2025 r. – PREDICTIVE SOLUTIONS Sp. z o. o., szkolenie pt. Szkolenie z zakresu obsługi oprogramowania PS IMAGO PRO;
- grudzień 2024 r. - Centrum Kształcenia IDEA, szkolenie pt. Dowody wpływu działalności naukowej i artystycznej na funkcjonowanie społeczeństwa i gospodarki — Praktyczne rozwiązania;
- październik 2020 r. - Centrum Kształcenia IDEA, szkolenie pt. Pisanie artykułów naukowych – źródło sukcesu naukowego.
- grudzień 2019 r. – StatSoft Polska, szkolenie pt. Automatyczna analiza dokumentów twkstowych.

5. Informacja o wykazywaniu się istotną aktywnością naukową albo artystyczną realizowaną w uczelni, instytucji naukowej lub instytucji kultury, w szczególności zagranicznej oraz współpraca z otoczeniem

5.1. Współpraca z Politechniką Częstochowską

W okresie od 1 marca do 30 września 2023 r. odbyłam staż naukowy na Wydziale Zarządzania Politechniki Częstochowskiej, w Katedrze Logistyki, pod opieką naukową dr hab. inż. Joanny Nowakowskiej-Grunt, który dotyczył:

1. Sprecyzowania wspólnego obszaru badawczego w naukach o zarządzaniu i jakości.
2. Egzemplifikacji kierunku rozwoju zarządzania organizacjami działającymi w turbulentnym otoczeniu.
3. Prowadzenie wspólnych badań z zakresu cyberbezpieczeństwa organizacji.
4. Przygotowanie publikacji do czasopism znajdujących się na liście MNi SW.

Podczas stażu wzięłam udział w konferencjach:

- Konferencja Naukowa *Zarządzanie organizacjami w erze cyfrowej. Wyzwania, trendy, koncepcje* w terminie 14-16.09.2023 Zakopane organizowanej przez Uniwersytet Ekonomiczny w Krakowie, wystąpienie z referatem n. t.: *Determinanty zarządzania przedsiębiorstwem w erze cyfrowej*.
- XV Konferencji Naukowej *Multimedia w biznesie i administracji* w terminie 22-24.03.2023 Koszęcin organizowana przez Politechnikę Częstochowska wystąpienie z referatem n. t.: *Zarządzanie bezpieczeństwem informacji w jednostce gospodarczej*.

W czasie stażu zostały opracowane i opublikowane dwa artykuły i rozdział:

- *[e_II.4.2_6]* **Antczak J.**, Dębicka E., Nowakowska-Grunt J. (2023), *Wybrane aspekty zarządzania bezpieczeństwem informacji w organizacjach w świetle współczesnych wyzwań gospodarki. Przykład przedsiębiorstw działających w Polsce*, Studia Wschodnioeuropejskie, Uniwersytet Warszawski, Nr ekspercki 19-t 2/2023 s. 311-335.
- *[e_II.2.1_2]* **Antczak J.** (2023), *Zarządzanie bezpieczeństwem informacji w jednostce gospodarczej* [w:] Kiełtyka L. (red.) Wykorzystanie technik informacyjnych w zarządzaniu, Wydawnictwo Politechniki Częstochowskiej, Częstochowa, s. 99-114, ISBN 978-83-7193-933-4.
- *[e_II.4.2_2]* **Antczak J.**, Nowakowska-Grunt J. (2023), *Zarządzanie cyberbezpieczeństwem podmiotów gospodarczych w kontekście wyzwań pandemii COVID-19*, Przegląd organizacji 4/2023, s. 439-446 DOI: 10.33141/po.2023.04.45.

Pragnę zwrócić uwagę, że moja współpraca z pracownikami Wydziału Zarządzania Politechniki Częstochowskiej nie ograniczyła się tylko do stażu naukowego. Aktywnie uczestniczę w konferencjach organizowanych przez pracowników Wydziału:

- XII Międzynarodowa Konferencja Naukowa Wiedza i technologie informacyjne w kreowaniu przedsiębiorczości, Olsztyn k/Częstochowy, 09-10.10.2025 r.
  - udział z wystąpieniem *Wpływ cyberataków na zarządzanie przedsiębiorstwem;*
- IX Konferencja Naukowa „*Science 2 Business*" Forum'24 Młodzi rodzice wobec wyzwań przyszłości. Praca, mieszkanie, zdrowie, bezpieczeństwo i ekologia, Częstochowa, 14-15.11.2024 r.
  - udział z wystąpieniem *Praca młodych ludzi w kontekście zrównoważonego zarządzania*;
- XI Międzynarodowa Konferencja Naukowa *Wiedza i technologie informacyjne w kreowaniu przedsiębiorczości*, Olsztyn k/Częstochowy, 10-11.10.2024 r.
  - udział z wystąpieniem *Sztuczna inteligencja a cyberbezpieczeństwo – analiza SWOT*;
- VIII Międzynarodowa Konferencja naukowa „*SCIENCE 2 BUSINESS*" oraz Forum'24 Kobieta między przestrzenią prywatną a publiczną, Częstochowa, 07-08.03.2024 r.
  - udział z wystąpieniem *Aspect of decent work in norms and law;*
- X Konferencja Naukowa *Wiedza i technologie informacyjne w kreowaniu przedsiębiorczości,* Olsztyn k/Częstochowy, 05-06.10.2023 r.
  - udział z wystąpieniem *Cyberbezpieczeństwem jednostki gospodarczej w czasie pandemii COVID-19;*
- XV Konferencja naukowa *Multimedia w biznesie i administracji*, Koszęcin, 22-24.03.2023 r.
  - udział z wystąpieniem Zarządzanie bezpieczeństwem informacji w jednostce gospodarczej;
- XIV Konferencja Naukowa *Multimedia w Biznesie i Administracji, Technologie ICT we współczesnym zarządzaniu*, Częstochowa, 25.03.2021 r.
  - udział z wystąpieniem *Zarządzanie nakładami na cyberbezpieczeństwo w jednostce gospodarczej*

Byłam również członkiem Rady Programowo-Naukowej podczas Forum'24 *Kobieta między przestrzenią prywatną a publiczną*, Częstochowa 07-08.03.2024 r.

Od 03 października 2023 r. jestem członkiem Naukowego Towarzystwa Informatyki Ekonomicznej.

Z dr hab. inż. J. Nowakowską-Grunt (do 30.09.2024 r. profesor PCz.) współpracuję w ramach realizacji projektu Wdrożenia procedury zapobiegania pracy przymusowe w Litex PROMO Sp. z o. o. (Spółka Grupy Kapitałowa Lubawa). Tematyka pracy przymusowej została przedstawiona w publikacjach:

- *[e_II.2.1_1]* **Antczak J.,** Nowakowska-Grunt J., Ciąder-Jackowiak J. (2025), *Praca przymusowa w standardach odpowiedzialności biznesowej: wdrażanie procedur przeciwdziałania ich wpływ na jakość zarządzania łańcuchem dostaw* [w:] Jasińska J. (red.) Problematyka normalizacji,

jakości i kodyfikacji w aspekcie integracji NATO z Unią Europejską, Jakość – problemy i rozwiązania część IX, PPH Remigraf Sp. z o.o., Warszawa s. 5-14, ISBN 978-83-7938-454-9.

- *[e_II.4.2_3]* **Antczak J.**, Nowakowska-Grunt J., Ciąder-Jackowiak J. (2023), *Decent work as an element of organization management in the context of sustainable development*, Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 2023 Nr. 189 s. 25-43, http://dx.doi.org/10.29119/1641-3466.2023.189.2

5.2. Współpraca z Polską Grupą Zbrojeniową S.A.

W okresie od 17 stycznia do 31 maja 2020 r. odbyłam staż naukowy w Departamencie Innowacji i Rozwoju Technologicznego Polskiej Grupy Zbrojeniowej S.A. Celem głównym stażu było prowadzenie badań związanych z realizacją pracy naukowej w zakresie zarządzania grupą kapitałową, prowadzenia prac badawczo-rozwojowych oraz zajęć dydaktycznych, a także pogłębienie wiedzy i umiejętności praktycznych. Cele cząstkowe:

1) Zapoznanie się ze specyfiką krajowych i międzynarodowych projektów naukowo-badawczych/badawczo-rozwojowych realizowanych przez PGZ SA.
2) Udział w pracach zespołu w ramach realizacji projektów naukowo-badawczych/badawczo-rozwojowych.
3) Uczestnictwo w seminariach naukowych, forach przemysłowych organizowanych w PGZ SA.
4) Identyfikacja wspólnych płaszczyzn badań w ramach nauk społecznych w obszarze zarządzania i jakości.
5) Poszerzanie i pogłębianie wiedzy oraz doświadczeń naukowych.

Podczas stażu brałam udział w:

- pracach zespołu, które realizowało jedno z zadań operacyjnych związanych realizacją strategii PGZ S.A.: ZO2.8.4. Opracowanie zasad współpracy ze szkołami średnimi, uczelniami wyższymi w zakresie oferty dla uczniów, studenta i absolwentów, w tym działania: DZ 2.8.4.3. Opracowanie zakresu wsparcia do przygotowania programów nauczania dla uczelni o profilu wojskowo-militarnym oraz DZ 2.8.4.6. znalezienie partnerów i uzgodnienie z partnerami kryteriów naboru do udziału w programie;
- przygotowaniu dokumentu związanego z: analizą kluczowych struktur, grup sektora obronnego za granicą, w których PGZ S.A. powinien uczestniczyć.

Pragnę zwrócić uwagę, że moja współpraca z pracownikami PGZ S.A. nie ograniczyła się tylko do stażu naukowego. Aktywnie współpracuję naukowo pisząc wspólne artykuły oraz występując na konferencjach:

- VI Krajowa *Konferencja Naukowa-Przemysłowa z cyklu Przedsiębiorstwa przyszłości polskiego przemysłu obronnego* 03.06.2022 r. Warszawa

- wystąpienie **Antczak J.**, (współwystępujący Roszkiewicz M.) n. t.: *Wyzwania dla przemysłu obronnego na tle ESG*

- VI Krajowa konferencja naukowa z cyklu *Społeczeństwo, Gospodarka, Siły Zbrojne pt. Odporność państwa, społeczeństwa i gospodarki na zagrożenia* 06.12.2023 r. Warszawa
  - wystąpienie **Antczak J.**, (współwystępujący Chmielarczyk K.) n. t. *ESG w strategiach rozwoju wybranych grup zbrojeniowych*;
- *[e_II.4.2_4]* **Antczak J.,** Mitkow S., Roszkiewicz M. (2023), *Zarządzanie innowacjami w przemyśle zbrojeniowym przy współpracy startupu jako istotny element budowy bezpieczeństwa w dobie zagrożenia ze Wschodu*, Studia Wschodnioeuropejskie Nr 19/2023, s. 222-249, DOI:10.31971/24500267.19.18
- *[e_II.4.2_7]* **Antczak J.**, Mitkow Sz., Roszkiewicz M. (2022), *Challenges for the Defense Industry Against the Background of ESG (Environmental, Social, Governance),* Concepts European Research Studies Journal, Volume XXV, Issue 4, 177-194,, DOI: 10.35808/ersj/3074

Pełnię funkcję promotora pomocniczego u mgr. Mateusza Roszkiewicza, Dyrektora Departamentu Rozwoju w Polskiej Grupie Zbrojeniowej S.A., przygotowującego rozprawę doktorską pt. *Bezpieczeństwo komunikowania się organizacji sektora zbrojeniowego wobec zachodzących zmian technologicznych*, której promotorem jest płk prof. dr hab. Szymon Mitkow.

W ramach zainteresowań przemysłem zbrojeniowym byłam współorganizatorem rocznych studiów podyplomowych pt. Zarządzanie przedsiębiorstwem z branży zbrojeniowej w latach akademickich: 2017/2018; 2018/2019, 2019/2020. Studia uzyskały Certyfikat „Studiów z Przyszłością" w III edycji Konkursu i Programu Akredytacji „Studia z Przyszłością" (2017/2018), którego celem jest wyróżnianie najbardziej innowacyjnych i nowoczesnych kierunków oraz programów studiów oferowanych przez polskie uczelnie. Byłam również konsultant merytoryczny Programu (dwuletnich) studiów podyplomowych MBA Security & Defence, w roku akademicki 2019-2021.

Moje aktywne zaangażowanie w środowisko naukowo-przemysłowe w zakresie przyszłości polskiego przemysłu obronnego odzwierciedlają udziały w krajowych konferencjach naukowych, prezentujące pełnione funkcje organizacyjne i naukowe:

- VI Krajowa Konferencja Naukowa-Przemysłowa z cyklu *Przedsiębiorstwa przyszłości polskiego przemysłu obronnego* Warszawa 03.06.2022 r.
  - Zastępca przewodniczącej Komitetu Organizacyjnego;
  - Członek Komitetu Naukowego;
- IV Krajowa Konferencja Naukowa *Przedsiębiorstwa przyszłości polskiego przemysłu obronnego,* Warszawa, 25-26.10.2019 r.
  - przewodnicząca Komitetu Organizacyjnego;

- III Krajowa Konferencja Naukowa *Przedsiębiorstwa przyszłości polskiego przemysłu obronnego,* Warszawa, 28.06.2019 r.
  - członek Komitetu Organizacyjnego;
- II Krajowa Konferencja Naukowa *Przedsiębiorstwa przyszłości polskiego przemysłu obronnego,* Warszawa, 15.03.2019 r.
  - członek Komitetu Organizacyjnego;

5.3. Współpraca z Litex Promo Sp. z o.o. (Spółką Grupy Kapitałowej Lubawa)

W ramach realizacji projektu w zakresie sporządzenia Procedury: Przeciwdziałania pracy przymusowej w ramach Procesu: Polityki ochrony praw człowieka w przedsiębiorstwie Litex Promo Sp. z o.o. (Spółki Grupy Kapitałowej Lubawa), razem z dr hab. Joanną Nowakowską-Grunt przeprowadziłyśmy następujące prace:

1. Wstępną ocenę ryzyka w obszarze kontekstu organizacyjnego podmiotu oceniającego oraz kontekstu podmiotu ocenianego, wykorzystując m.in.: Kwestionariusz „Wstępna ocena ryzyka".
2. Ocenę ryzyka we współpracy z zewnętrznymi formami zatrudnienia wykorzystując m.in.: Listy kontrolne.
3. Identyfikację warunków i diagnozy stanu występowania pracy przymusowej w łańcuchu dostaw pracy wykorzystując ankiety dla cudzoziemców świadczących pracę, oraz wizytując miejsca zamieszkania.
4. Identyfikację warunków i diagnozy stanu występowania pracy przymusowej wśród zatrudnionych Polaków przy wykorzystaniu wywiadów.

W trakcie przeprowadzenia powyższych prac prowadziłyśmy rozmowy z kadrą zarządczą i pracownikami oraz przedstawicielami agencji zatrudnienia.

Efektem powyższych prac było opracowanie i wdrożenie Procedury: Przeciwdziałania pracy przymusowej w ramach Procesu: Polityki ochrony praw człowieka. Procedura, ma charakter ogólny i obejmuje opis procesu postepowania w celu przeciwdziałania pracy przymusowej.

Kolejnymi etapami realizacji projektu był audyt wdrożeniowy Procedury: Przeciwdziałania pracy przymusowej, który przeprowadziłyśmy 05.03.2024 r. w siedzibie przedsiębiorstwa. W trakcie audytu przeprowadziłyśmy wywiady z Prezesem Zarządu, Pełnomocnikiem Zarządu ds. SZJ, Specjalistą ds. BHP i PPOŻ oraz wśród polskich pracowników oraz cudzoziemców. W trakcie kontroli audytu nie stwierdziłyśmy naruszenia Procedury przeciwdziałania pracy przymusowej. Na podstawie przeprowadzonych wywiadów sformułowałyśmy wnioski, które posłużyły do zaproponowania działań usprawniających procedurę.

W dniach 09-10.04.2025 r. przeprowadziłyśmy audyt kontrolny w nadzorze procesu zapobiegania pracy przymusowej w ramach Procedury: Przeciwdziałania pracy przymusowej, w siedzibie przedsiębiorstwa. W trakcie audytu zostały przeprowadzone wywiady z Prezesem Zarządu,

Pełnomocnikiem Zarządu ds. Zarządzania Jakością oraz wśród polskich pracowników oraz cudzoziemców. Przeprowadziłyśmy również szkolenie półgodzinne na temat "Jak rozpoznawać prace przymusową w kontekście współpracy z agencją pracy". W szkoleniu wzięli udział: Dyrektor Produkcji, Kierownik Szwalni, Kierownik Produkcji, Kierownik Ubieralni, Specjalista ds. CSR, Inspektor ds. BHP, Pracownik ds. Administracji. W trakcie kontroli audytu nie stwierdziłyśmy naruszenia Procedury przeciwdziałania pracy przymusowej. Na podstawie przeprowadzonych wywiadów stwierdziłyśmy wprowadzenie działań usprawniających procedurę po audycie wdrożeniowym, sformułowałyśmy wnioski, które posłużyły do zaproponowania działań usprawniających procedurę.

Kolejny audyt planujemy na pierwszy kwartał 2026 r.

Audyty trzeciej strony w standardzie SMETA, TCCC czy Ecovadis pozytywnie oceniają opracowaną przez nas procedurę oraz działania usprawniające.

6. Informacja o osiągnięciach dydaktycznych, organizacyjnych oraz popularyzujących naukę lub sztukę

Moja ścieżka zawodowa odzwierciedla konsekwentny rozwój w obszarze nauk o zarządzaniu, ze szczególnym uwzględnieniem działalności dydaktycznej, naukowej oraz organizacyjnej.

Od października 2021 r. jestem zatrudniona jako adiunkt badawczo-dydaktyczny w Instytucie Zarządzania na Wydziale Bezpieczeństwa, Logistyki i Zarządzania Wojskowej Akademii Technicznej w Warszawie. W ramach tej funkcji aktywnie uczestniczę w pracach zespołów uczelnianych, m.in. od maja 2025 r. jako członek zespołu ds. opracowania zasad wdrożenia sztucznej inteligencji w działalności naukowej Wydziału, a od listopada 2024 r. – zespołu ds. opracowania III kryterium ewaluacji działalności naukowej za lata 2022–2025. Od grudnia 2024 r. pełnię również funkcję Zastępcy Dyrektora ds. naukowych Instytutu Zarządzania.

W latach 2018–2021 byłam związana z Akademią Sztuki Wojennej w Warszawie jako adiunkt badawczo-dydaktyczny na Wydziale Zarządzania i Dowodzenia. W roku akademickim 2018/2019 pełniłam funkcję opiekuna Koła Naukowego Studentów Logistyki.

Wcześniej, w latach 2015–2018, pracowałam jako adiunkt w Instytucie Organizacji i Zarządzania Wydziału Cybernetyki Wojskowej Akademii Technicznej.

W latach 2006–2015 byłam zatrudniona w Akademii Finansów i Biznesu Vistula w Warszawie, gdzie pełniłam szereg funkcji akademickich i organizacyjnych. Byłam m.in. prodziekanem Wydziału Biznesu i Stosunków Międzynarodowych (2014–2015), prodziekanem Wydziału Biznesu (2013–2014), prodziekanem Wydziału Ekonomicznego (2010–2013), kierownikiem Katedry Finansów i Rachunkowości (2013–2014), a także opiekunem specjalności „Rachunkowość” oraz studiów podyplomowych z zakresu rachunkowości, audytu i kontroli wewnętrznej. Karierę akademicką rozpoczęłam jako asystent w Katedrze Rachunkowości.

6.1. Osiągnięcia dydaktyczne

Moja działalność dydaktyczna związana jest przed wszystkim z doświadczeniami, jakie zdobyłam podczas pracy na trzech uczelniach będących moim podstawowym miejscem pracy: Akademii Finansów i Biznesu Vistula (lata 2006-2015), Akademii Sztuki Wojennej (lata 2018-2021) i Wojskowej Akademii Technicznej (lata 2015-2018 oraz od 2021 r. i nadal).

W zakresie pracy dydaktycznej prowadziłam i prowadzę zajęcia na studiach stacjonarnych i niestacjonarnych w formie wykładów, ćwiczeń, laboratoriów oraz konwersatorium. W trakcie mojej pracy dydaktycznej zajęcia prowadziłam na kierunkach m. in.: Zarządzanie, Logistyka, Finanse i Rachunkowość.

Przedmioty, które najczęściej prowadziłam, to m.in.:

- Podstawy zarządzania i przedsiębiorczości (wykład, ćwiczenia dla studentów I stopnia);
- Zarządzanie kapitałem niematerialnym (wykład, ćwiczenia dla studentów I stopnia);
- Mikroekonomia (wykład, ćwiczenia dla studentów I stopnia);
- Makroekonomia (wykład, ćwiczenia dla studentów II stopnia);
- Rachunkowości finansowa (wykład, ćwiczenia dla studentów I stopnia);
- Rachunkowość zarządcza (wykład, ćwiczenia dla studentów II stopnia);
- Audyt w zarządzaniu kryzysowym (wykład, ćwiczenia dla studentów I stopnia);

W ramach zatrudnienia w innych jednostkach naukowych w Polsce prowadziłam zajęcia dydaktyczne ze studentami studiów stacjonarnych i niestacjonarnych na siedmiu uczelniach. Obecnie prowadzę zajęcia w dwóch uczelniach:

- Akademia Finansów i Biznesu Vistula Oddział w Olsztynie – konwersatorium na studiach Master of Business Administration z przedmiotów: zarządzanie cyberbezpieczeństwem oraz finanse publiczne z elementami rachunkowości.
- Akademia WIT w Warszawie – wykłady i laboratorium z przedmiotów m.in.: controlling finansowy w przedsiębiorstwie (studia magisterskie) i podstawy rachunkowości (studia licencjackie).

Prowadząc zajęcia dydaktyczne, koncentruję się na przekazywaniu wiedzy w sposób praktyczny i nowoczesny, tak aby wspierać rozwój kompetencji studentów i ich przygotowanie do wyzwań zawodowych.

W ramach realizacji projektu pt. „Innowacyjna i sprawna administracja źródłem sukcesu w gospodarce opartej na wiedzy", współfinansowanego z Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Kapitał Ludzki, przeprowadziłam cykl szkoleń z zakresu zarządzania projektami. Szkolenia obejmowały zagadnienia z zakresu sterowania projektem, planowania, budżetowania, prognozowania oraz estymowania kosztów.

W ramach realizacji projektu (grudzień 2013 r. – marzec 2015 r.), szkoleniami objęto pracowników dwunastu jednostek samorządu terytorialnego: Powiat Krapkowicki, Powiat Wolsztyński, Powiat

Zgorzelecki, Powiat Średzki, Miasto na prawach powiatu Świętochłowice, Powiat Jarociński, Powiat Oleski, Powiat Sulęciński, Powiat Zielonogórski, Powiat Opolski, Gmina Brudzew, Powiat Gliwicki.

Dwukrotnie zorganizowałam i prowadziłam warsztaty metodyczne w zakresie negocjacji dyplomatycznych. Współprowadzącymi warsztaty byli: eksperci z wieloletnim doświadczeniem w dyplomacji multilateralnej: ambasador dr Zdzisław Rapacki, ambasador Grzegorz Poznański oraz płk dr inż. Marek Zadrożny.

Pierwsze edycja warsztatów odbyła się w dniach 11 i 18 kwietnia 2016 r. w Instytucie Organizacji i Zarządzania Wydziału Cybernetyki WAT. Celem warsztatów było praktyczne zapoznanie doktorantów i studentów z procesem negocjacyjnym w systemie ONZ, ze szczególnym uwzględnieniem tematyki rozbrojeniowej. Pierwszy dzień obejmował wykłady oraz przygotowanie uczestników do symulacji. W drugim dniu przeprowadzono symulację posiedzenia Konferencji Rozbrojeniowej nt. rozbrojenia nuklearnego, z udziałem delegacji państw i grup regionalnych, która odbyła się w 2006 r. w Genewie. Uczestnicy wcielili się w role przedstawicieli państw, prowadząc konsultacje i debaty nad projektem rezolucji.

Druga edycja warsztatów odbyła się w dniach 30 marca i 6 kwietnia 2017 r. w Instytucie Organizacji i Zarządzania Wydziału Cybernetyki WAT. Celem warsztatów było praktyczne zapoznanie doktorantów i studentów z technikami negocjacji multilateralnych, ze szczególnym uwzględnieniem tematyki broni chemicznej. Pierwszy dzień obejmował wykłady wprowadzające, natomiast drugi – symulację obrad w sprawie rezolucji chemicznej I Komitetu Zgromadzenia Ogólnego ONZ, podczas której uczestnicy wcielali się w role delegatów państw i prowadzili formalne oraz nieformalne konsultacje nad projektem rezolucji.

Obie edycje warsztatów spotkały się z bardzo pozytywnym odbiorem wśród studentów i doktorantów. Uczestnicy wysoko ocenili poziom merytoryczny zajęć oraz kompetencje prowadzących. Na podstawie przeprowadzonych warsztatów powstała współautorska monografia oraz artykuł:

- *[e_II.1.1_3]* **Antczak J.**, Rapacki Z., Poznański G. M. (2017), *Warsztaty jako nowoczesna forma zajęć akademickich*, Wydawnictwo Akademii Finansów i Biznesu Vistula, Warszawa 2017, ISBN 978–83–64614–35-4.
- **Antczak J.**, Rapacki Z. (2016), *Warsztaty jako nowoczesna forma prowadzenia zajęć na przykładzie symulacji konferencji rozbrojeniowej*, WAT Studia Bezpieczeństwa Narodowego *10*(2), s75–90. https://doi.org/10.37055/sbn/129840.

W ramach rozwoju dydaktycznego uczestniczę w szkoleniach, m.in.:

- styczeń 2024 r. – REVAS, szkolenie z zakresu wykorzystania Branżowych Symulacji Biznesowych w nauczaniu:
  - *poziom trener Branżowych Symulacji Biznesowych – Zarządzanie firmą;*
  - *poziom trener Branżowych Symulacji Biznesowych – Zarządzanie projektami;*
- listopad 2020 r. – SEKA S. A. – *kurs nt. MS Teams – zdalne nauczanie;*

- marzec 2019 r. – ASzWoj – kurs nt. Podstawy tworzenia materiałów i prowadzenia zajęć z wykorzystaniem technik i metod kształcenia zdalnego *KOD 8101051.*

Moje zaangażowanie w pracę dydaktyczną zostało docenione przez studentów i zostałam przez nich oceniona jako najlepszy dydaktyk na Wydziale Zarządzania i Dowodzenia ASzWoj w 2019 r. otrzymując Złotą kredę od Wydziałowej Rady Samorządu Studentów, Wydziału Zarządzania i Dowodzenia ASzWoj. W 2024 i 2025 r. otrzymałam od prof. dr hab. inż. Macieja Krawczaka Rektora Akademii WIT dyplom uznania za zaangażowanie w promowanie najlepszych absolwentów Uczelni. W 2025 r. otrzymałam od prof. dr hab. inż. Macieja Krawczaka Rektora Akademii WIT dyplom uznania za opiekę naukową nad pracą konkursową studenta reprezentującego Uczelnię w XVII Ogólnopolskim Międzyuczelnianym Konkursie Młodych Mistrzów 2025 organizowanym przez Forum Teleinformatyki.

Jestem promotorem oraz recenzentem łącznie kilkudziesięciu prac inżynierskich, licencjackich oraz magisterskich prowadzonych na Wydziale Bezpieczeństwa, Logistyki i Zarządzania WAT, Akademii Finansów i Biznesu Vistula, Akademii WIT w Warszawie, Akademii Sztuki Wojennej. Tematyka prac dyplomowych związana jest z zagadnieniami prowadzonych przeze mnie przedmiotów dydaktycznych oraz zainteresowaniami naukowymi dotyczącymi zarządzania cyberbezpieczeństwem, controllingiem, analizą finansową.

Pełnie funkcję promotora pomocniczego:

- mgr Mateusz Roszkiewicz - temat rozprawy doktorskiej *Bezpieczeństwo komunikowania się organizacji sektora zbrojeniowego wobec zachodzących zmian technologicznych*; Promotor płk prof. dr hab. Szymon Mitkow.

  Wspólnie z promotorem i doktorantem opublikowaliśmy artykuły:

  - *[e_II.4.2_4]* **Antczak J.,** Mitkow S., Roszkiewicz M. (2023), *Zarządzanie innowacjami w przemyśle zbrojeniowym przy współpracy startupu jako istotny element budowy bezpieczeństwa*
    w dobie zagrożenia ze Wschodu, Studia Wschodnioeuropejskie Nr 19/2023, s. 222-249, DOI:10.31971/24500267.19.18
  - *[e_II.4.2_7]* **Antczak J.**, Mitkow S., Roszkiewicz M. (2022), *Challenges for the Defense Industry Against the Background of ESG (Environmental, Social, Governance),* Concepts European Research Studies Journal, Volume XXV, Issue 4, 177-194, 2022, DOI: 10.35808/ersj/3074

Pełniłam funkcję **promotora pomocniczego** w przewodach doktorskich:

- dr Adam Stolarz - temat rozprawy doktorskiej *Zarządzanie innowacjami w segmencie lotniczym przemysłu zbrojeniowego w Polsce*; Promotor: dr hab. inż. Stanisław Smyk (nadanie stopnia doktora 18.02.2022 r.)

Wspólnie z doktorantem opublikowaliśmy:

- **Antczak. J.**, Stolarz A. (2022), *Determinants of the armament industry strategy in the time of war and unrest*, Wiedza Obronna 2022, t. 280, nr 3, ISSN: 0209-0031, DOI 10.34752/2022-i280, s. 187-210.
- **Antczak J.**, Stolarz A. (2018), *Kodeks Grupy PGZ jako determinant prawidłowego funkcjonowania grupy kapitałowej* [w:] Nowakowska-Krystman A., Sieci biznesowe i uwarunkowania ich tworzenia w przemyśle zbrojeniowym. Wybrane problemy, Wydawnictwo Akademii Sztuki Wojennej, Warszawa s. 34-50, ISBN: 978-83-7523-673-6.

- dr Agata Wasilewska - temat rozprawy doktorskiej *Znaczenie funduszy unijnych w rozwoju grup producentów rolnych w Polsce;* Promotor: dr hab. Kazimierz Olesiak (nadanie stopnia doktora 30.09.2019 r.)
- dr inż. Artur Kuchciński - temat pracy *Ocena efektywności działania regionalnych funduszy pożyczkowych finansujących MSP w województwie świętokrzyskim;* Promotor: dr hab. inż. Andrzej Dąbkowski (nadanie stopnia doktora 15.06.2015 r.)

6.2. Osiągnięcia organizacyjne

W pracy aktywnie angażuję się w realizację działań organizacyjnych. W latach 2006–2015 byłam związana z Akademią Finansów i Biznesu Vistula, gdzie po obronie doktoratu oprócz obowiązków dydaktycznych i naukowych, pełniłam szereg funkcji organizacyjnych, m.in. Prodziekana Wydziału Biznesu i Stosunków Międzynarodowych (2014–2015), Prodziekana Wydziału Biznesu (2013–2014), Prodziekana Wydziału Ekonomicznego (2010–2013) oraz Kierownika Katedry Finansów i Rachunkowości (2013–2014). Byłam również opiekunem specjalności „Rachunkowość" oraz merytorycznym opiekunem studiów podyplomowych z zakresu rachunkowości, audytu i kontroli wewnętrznej.

W latach 2018–2021 jako adiunkt badawczo-dydaktyczny w Akademii Sztuki Wojennej w Warszawie, aktywnie angażowałem się w działalność studencką, pełniąc funkcję opiekuna Koła Naukowego Studentów Logistyki (KNSL) w roku akademickim 2018/2019. Wraz KNSL w dniach 04-05.04.2019 r. zorganizowałam jubileuszową X Ogólnopolską konferencję studencką Logistyka a Bezpieczeństwo. Wnioski i dorobek naukowy zaprezentowany podczas konferencji znalazły ujęcie syntetyczne w formie monografii zbiorowej:

- **Antczak J.**, Grala D., Fornal M. (red.) (2020), *Logistyka a bezpieczeństwo. Innowacyjne rozwiązania logistyczne*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa, ISBN 978-83-7523-773-3 (s. 163).

Za wsparcie KNSL otrzymałam od członków KNSL statuetkę. Byłam również zaangażowana w Program Top Young 100 coroczną inicjatywę rozwojową skierowaną do najlepszych studentów kierunków związanych z łańcuchem dostaw w Polsce.

Byłam współorganizatorem rocznych studiów podyplomowych pt. Zarządzanie przedsiębiorstwem z branży zbrojeniowej w latach akademickich: 2017/2018; 2018/2019, 2019/2020. Studia uzyskały Certyfikat „Studiów z Przyszłością" w ramach III edycji Konkursu i Programu Akredytacji „Studia z Przyszłością" (2017/2018), którego celem jest wyróżnianie najbardziej innowacyjnych i nowoczesnych kierunków i programów studiów na polskich uczelniach. Byłam również konsultant merytoryczny Programu (dwuletnich) studiów podyplomowych MBA Security & Defence, w roku akademicki 2019-2021.

Od października 2021 r. pracuje jako adiunkt badawczo-dydaktycznego w Instytucie Zarządzania na Wydziale Bezpieczeństwa, Logistyki i Zarządzania Wojskowej Akademii Technicznej w Warszawie. Moja aktywność organizacyjna koncentruje się na wspieraniu rozwoju instytucjonalnego oraz wdrażaniu innowacyjnych rozwiązań w obszarze nauki i dydaktyki.

Od grudnia 2024 r. pełnię funkcję Zastępcy Dyrektora Instytutu Zarządzania ds. naukowych, gdzie odpowiadam za koordynację działań naukowych, wspieranie inicjatyw badawczych oraz rozwój współpracy naukowej. Równolegle, od listopada 2024 r. uczestniczę w pracach zespołu ds. opracowania III kryterium ewaluacji działalności naukowej za lata 2022–2025, co wiąże się z analizą dorobku naukowego jednostki oraz przygotowaniem dokumentacji ewaluacyjnej.

Od maja 2025 r. jestem również członkiem zespołu ds. opracowania zasad wdrożenia sztucznej inteligencji na Wydziale Bezpieczeństwa, Logistyki i Zarządzania w obszarze działalności naukowej, co stanowi istotny wkład w rozwój nowoczesnych kierunków badań i innowacyjnych metod analizy danych.

W zakresie działań organizacyjnych również współorganizowałam i brałam dwukrotnie udział w wyjeździe studyjnym do Brukseli realizowanych w ramach pierwszej oraz drugiej edycji studiów Master of Business Administration (MBA) na Akademii Finansów i Biznesu Vistula, Filia w Olsztynie w dniach 15-17.10.2024 r. oraz 24-26.06.2025 r. Aktualnie trwają prace nad wyjazdem słuchaczy z trzeciej edycji.

W przedłożonym autoreferacie, w syntetyczny sposób przedstawione zostały moje osiągnięcia naukowo-badawcze. Szczegółowy ich wykaz natomiast znajduje się w załączniku 4 do wniosku przewodniego.

(podpis wnioskodawcy)