Dr hab. Marian Oliński, prof. UWM
Instytut Nauk o Zarządzaniu i Jakości
Wydział Nauk Ekonomicznych
Uniwersytet Warmińsko-Mazurski w Olsztynie

Olsztyn 20.02.2025

Recenzja rozprawy doktorskiej

magistra Kajetana Kozłowskiego

Zarządzanie bezpieczeństwem przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych a szpiegostwo korporacyjne

przygotowanej pod kierunkiem naukowym promotora
dr hab. inż. Anny Brzozowskiej, prof. Pcz

1. Przedmiot recenzji

Przedmiotem recenzji jest rozprawa doktorska Pana Kajetana Kozłowskiego pt. *„Zarządzanie bezpieczeństwem przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych a szpiegostwo korporacyjne”*, przygotowana pod kierunkiem naukowym promotor dr hab. inż. Anny Brzozowskiej, prof. Pcz.

Podstawą wydania opinii jest pismo dr hab. Agaty Mesjasz-Lech, prof. PCz Przewodniczącej Rady Dyscypliny Naukowej Nauki o Zarządzaniu i Jakości Politechniki Częstochowskiej z dnia 17.12.2024 r.. Pismo to dotyczy powołania mnie przez Radę Naukową Dyscypliny Nauk o Zarządzaniu i Jakości Politechniki Częstochowskiej na recenzenta powyższej rozprawy doktorskiej. Zgodnie z art. 187.1 ustawy z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2023 r., poz. 742) „rozprawa doktorska prezentuje ogólną wiedzę teoretyczną kandydata w dyscyplinie albo dyscyplinach oraz umiejętność samodzielnego prowadzenia pracy naukowej lub artystycznej”. Natomiast punkt 2 cytowanego artykułu uściśla, iż „Przedmiotem rozprawy doktorskiej jest oryginalne rozwiązanie problemu naukowego, oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w sferze gospodarczej lub społecznej albo oryginalne dokonanie artystyczne”.

Celem niniejszej recenzji jest ocena, czy przedłożona dysertacja doktorska spełnia wymagania określone w ustawie, co stanowi podstawę do dopuszczenia mgr. Kajetana Kozłowskiego do publicznej obrony. Dlatego też przy ocenie rozprawy doktorskiej mgr.

Kajetana Kozłowskiego uwzględniłem znaczenie podjętej problematyki, poprawność sformułowanych celów i hipotez, a także metodykę badawczą, strukturę pracy oraz aspekty formalne.

Przedstawiona do recenzji rozprawa doktorska w części merytorycznej obejmuje: wstęp, sześć rozdziałów oraz podsumowanie. Część uzupełniająca to bibliografia wraz z netografią oraz spis rysunków, tabel i wykresów, a także dwa załączniki. Praca zawiera również streszczenie w języku angielskim. Spis literatury zawiera 245 pozycji. Całość rozprawy obejmuje 424 strony.

2. Znaczenie podjętej tematyki

Aktualność poruszanej w rozprawie doktorskiej tematyki jest bezdyskusyjna. W dobie postępującej cyfryzacji i wzrostu znaczenia technologii informacyjno-komunikacyjnych (ICT), bezpieczeństwo informacji staje się jednym z kluczowych aspektów zarządzania strategicznego w przedsiębiorstwach. Jednocześnie szpiegostwo korporacyjne, jako jeden z głównych rodzajów zagrożeń, zyskuje na znaczeniu w warunkach globalnej konkurencji i nieustannej wymiany danych.

Współczesne przedsiębiorstwa działające w sektorze ICT charakteryzują się wysoką zależnością od kapitału intelektualnego, innowacji oraz strategicznych zasobów informacyjnych, co czyni je szczególnie podatnymi na działania wywiadowcze, cyberataki i wycieki danych. W tym kontekście zagadnienie zarządzania bezpieczeństwem organizacji z uwzględnieniem specyfiki zagrożeń wywiadowczych staje się kluczowe zarówno z perspektywy teoretycznej, jak i praktycznej. Dlatego warto podkreślić, że problematyka poruszona w rozprawie doktorskiej ma nie tylko istotne znaczenie teoretyczne, ale także wyraźny wymiar aplikacyjny. Wyniki przeprowadzonych badań oraz zaproponowany model zarządzania bezpieczeństwem mogą znaleźć zastosowanie zarówno w przedsiębiorstwach sektora ICT, jak i w organizacjach o wysokim stopniu zależności od zasobów informacyjnych.

Badania zawarte w rozprawie doktorskiej stanowią podstawę do opracowania strategii zarządzania bezpieczeństwem, które zwiększają odporność przedsiębiorstwa na szpiegostwo korporacyjne. Ponadto, Autor słusznie podkreśla znaczenie zarządzania bezpieczeństwem w kontekście szpiegostwa korporacyjnego, wskazując, że kompleksowe podejście do tego problemu w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych powinno obejmować aspekty technologiczne, proceduralne i ludzkie. Zatem, istotnym atutem rozprawy jest podjęcie tematyki integracji zarządzania bezpieczeństwem z mechanizmami ochrony przed szpiegostwem korporacyjnym. Większość dotychczasowych badań koncentruje się na aspektach technologicznych cyberbezpieczeństwa, podczas gdy w niniejszej pracy Autor zwraca uwagę na szerszy kontekst organizacyjny, strategiczny oraz zarządczy. Dlatego, zważywszy na ów kontekst i podejmowaną tematykę, lukę badawczą powinno się precyzyjniej zidentyfikować, a nie ograniczyć się tylko do stwierdzenia (w części metodycznej), iż luka badawcza dotyczy relacji i powiązań zachodzących pomiędzy zarządzaniem bezpieczeństwem, zarządzaniem bezpieczeństwem informacji, a szpiegostwem korporacyjnym.

3. Cel pracy, hipotezy badawcze

Cele, problem badawczy oraz hipotezy zostały sformułowane we wstępie pracy oraz w rozdziale 4 zatytułowanym „Metodyka badań własnych". Głównym celem recenzowanej pracy jest opracowanie modelu zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych, który uwzględnia zróżnicowane postrzeganie zagrożeń wynikających ze szpiegostwa korporacyjnego przez pracowników, w celu zwiększenia ochrony danych i tajemnicy przedsiębiorstwa. W związku z tak postawionym celem głównym pracy, postawiono cztery cele szczegółowe:

- „identyfikacja roli i znaczenia bezpieczeństwa w zarządzaniu przedsiębiorstwem,
- zidentyfikowanie przesłanek oraz wyzwań związanych z wdrażaniem zarządzania bezpieczeństwem informacji w organizacji,
- ustalenie, jakie wyzwania dla zarządzania bezpieczeństwem przedsiębiorstw sektora technologii informacyjno-komunikacyjnych stwarza szpiegostwo korporacyjne,
- diagnoza zależności między poziomem świadomości pracowników a skutecznością zarządzania bezpieczeństwem w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych".

Generalnie cele te zostały sformułowane w sposób prawidłowy, choć przy ich artykułowaniu należy zadbać o precyzję wykorzystywanych pojęć (np. różnica pomiędzy rolą i znaczeniem w pierwszym celu szczegółowym). Największe wątpliwości budzi natomiast fakt pojawienia się po raz pierwszy w podsumowaniu rozprawy, głównego celu badań. Za cel ten przyjęto określenie kluczowych determinant skutecznego zarządzania bezpieczeństwem, z uwzględnieniem zróżnicowanego postrzegania zagrożeń przez pracowników oraz oceny funkcjonalności opracowanego modelu (strona 312). Nasuwa się zatem pytanie o powiązanie sformułowanego wcześniej celu pracy z tak sformułowanym głównym celem badań. Wątpliwości tym bardziej są uzasadnione, bo w tymże podsumowaniu Autor dysertacji stwierdził, iż „zrealizował postawiony cel badawczy, tworząc innowacyjny i kompleksowy model zarządzania bezpieczeństwem, który odpowiada specyfice sektora ICT" (strona 314). Sformułowanie to jest zatem bardzo podobne do sformułowanego we wstępie i metodyce badań głównego celu pracy. Zatem analizując zdanie z podsumowania (ze strony 313), które brzmi: „Postawione szczegółowe problemy badawcze miały na celu kompleksowe rozwinięcie głównego celu badawczego", nie wiadomo jaki cel Autor miał na myśli. Ponadto na stronie 154 (Rozdział 4 – „Metodyka badań własnych") pojawia się cel nadrzędny jakim jest „weryfikacja hipotezy głównej". Być może skomplikowaniu całego układu formułowanych celów sprzyja fakt ich określania dla poszczególnych rozdziałów czy też etapów procesu badawczego. Jest to dopuszczalne ale trzeba pamiętać o przejrzystości w tak zaprezentowanym układzie celów. Poza tym niektóre cele odnośnie konkretnych części rozprawy nie są prawidłowe, np. celem czwartego rozdziału (jak to określono we wstępie) „była analiza zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych (ICT) w kontekście zagrożeń związanych ze szpiegostwem korporacyjnym". Analiza sama w sobie nie jest celem. Jest to metoda, która służy realizacji celu.

W mojej opinii lepszym podejściem byłoby przyjęcie obok celu głównego, celów szczegółowych w warstwie teoretycznej, deskryptywnej, praktycznej. Nadałoby to przejrzystości całemu układowi celów.

Główny problem badawczy sformułowano w formie pytania „Jakie wyzwania dla zarządzania bezpieczeństwem informacji w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych wynikają ze zróżnicowanego postrzegania przez pracowników zagrożeń ze strony szpiegostwa korporacyjnego?”

Natomiast szczegółowe problemy badawcze sformułowano w formie pytań:

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

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

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

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

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

W związku z tak wyartykułowanym głównym problemem badawczym, Autor sformułował hipotezę główną, zgodnie z którą „zarządzanie bezpieczeństwem informacji przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych powinno uwzględniać rozbieżności w postrzeganiu przez pracowników zagrożeń wynikających ze szpiegostwa korporacyjnego”. Dodatkowo sformułowano hipotezy szczegółowe:

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

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

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

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

Przy tym ostatnia z hipotez została zdekomponowana w rozdziale 4 (Metodyka badań własnych) do postaci ośmiu hipotez szczegółowych:

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

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

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

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

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

H4.6: Postrzegane przez pracowników skuteczność procedur ochrony, edukacja w zakresie zagrożeń oraz środki prawne wpływają na ich ocenę ryzyka szpiegostwa korporacyjnego w organizacji.
H4.7: Szkolenia i świadomość pracowników są mediatorem wpływu skuteczności zabezpieczeń organizacyjnych na postrzegane ryzyko szpiegowskie.
H4.8: Szkolenia, świadomość zagrożeń i regulacje prawne wpływają na postrzeganie zagrożenia szpiegostwem.
Generalnie hipotezy zostały sformułowane prawidłowo, wątpliwości budzi jednak używanie niedookreślonych przymiotników, które one zawierają, np. „wdrażanie odpowiednich procesów decyzyjnych", „stosowanie odpowiednich standardów". Ponadto podobnie jak przy formułowaniu celów, należy zadbać o precyzję używanych pojęć. Słowo „skuteczne" w zarządzaniu związane jest z osiąganiem celów, co w części empirycznej (przy weryfikowaniu hipotezy) nie jest uwypuklone.

4. Metodyka badań

Zastosowane w pracy metody badań zostały scharakteryzowane w podrozdziale 4.4 – Metody, techniki i narzędzia badawcze. Do metod badań zaliczono analizę literatury, wywiad ekspercki, ankietę oraz metody statystyczne (w tym chi-kwadrat przy weryfikowaniu hipotezy H4.1-H4.8) i metodę symulacji komputerowej. W części metodycznej sprecyzowano także zakres przestrzenny i czasowy badań. Zważywszy na przyjęte założenia metodyczne przyjęte metody badań można uznać za poprawne. Wątpliwości budzi jednak skąpy opis dotyczący kryteriów doboru przedsiębiorstw objętych badaniem. Cała dostępna informacja na ten temat została ograniczona do zaledwie dwóch zdań (zawartych w podrozdziale 4.1 „Zakres przedmiotowy, podmiotowy, przestrzenny i czasowy badań"). Brzmią one „Do badania wybrano sześć dużych przedsiębiorstw działających na terytorium Polski, posiadających co najmniej 5-letni staż na rynku oraz specjalizujących się w innowacyjnych rozwiązaniach w zakresie ICT" (str. 154) oraz „Etap II (wrzesień 2022 r. – marzec 2023 r.) – polegał na przeprowadzeniu wywiadów eksperckich z osobami odpowiedzialnymi za bezpieczeństwo w sześciu przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych, wybranych na podstawie precyzyjnie określonych kryteriów" (str. 154-155). Nie podano przy tym jakie to były owe „precyzyjnie określone kryteria"- czy np. największa liczba pracowników, czy też inne (samo określenie „staż pracy" w stosunku do przedsiębiorstw jest niefortunne). Natomiast za zaletę przeprowadzonych badań ankietowych wśród pracowników wybranych przedsiębiorstw należy uznać dużą próbę przebadanych pracowników (466 osób). Niestety doktorant w części metodycznej (i nie tylko - błąd ten pojawia się już we wstępie, poszczególnych rozdziałach i podsumowaniu) myli pojęcie ankiety i kwestionariusza ankiety (tzn. używa słowa ankieta jako synonimu kwestionariusza ankiety, podczas gdy ankieta to jest metoda badań). Ponadto większość pytań zawartych w kwestionariusz ankiety zaczyna się od słów „Czy uważa Pani/Pan …….". Na tak postawione pytanie odpowiada się „Uważam" lub „Nie uważam"). Natomiast warianty odpowiedzi w postaci: „Zdecydowanie się nie zgadzam"; „Nie zgadzam się", „Nie mam zdania", „Zgadzam się"; „Zdecydowanie się zgadzam", świadczą o pytanie w jakim stopniu zachodzi dane zjawisko. Ponadto brak jest w części metodycznej informacji o rzetelności skal pomiarowych.

Pomimo tych mankamentów zastosowane podejście badawcze jest uzasadnione i adekwatne do postawionych celów. Wybór metod pozwala na uzyskanie szerokiej perspektywy na badane zjawisko, uwzględniając zarówno uwarunkowania teoretyczne, jak i praktyczne doświadczenia badanych ekspertów i pracowników poszczególnych przedsiębiorstw.

5. Struktura rozprawy

Rozprawa doktorska mgr Kajetana Kozłowskiego składa się z wstępu, sześciu rozdziałów merytorycznych oraz podsumowania. Część uzupełniającą stanowią bibliografia wraz z netografią, spis rysunków, tabel i wykresów, a także dwa załączniki. Praca zawiera również streszczenie w języku angielskim.

Struktura pracy jest przemyślana i logicznie skonstruowana, co pozwala na stopniowe wprowadzanie czytelnika w problematykę badawczą oraz prezentację wyników badań.
We wstępie Doktorant przedstawia istotność podjętej tematyki oraz uzasadnia jej wybór. Określa również cel główny i cele szczegółowe pracy, a także formułuje pytania i hipotezy badawcze.

W pierwszej części rozdziału 1, Doktorant koncentruje się na problematyce zdefiniowania terminu bezpieczeństwo. Podano w tej części liczne definicje bezpieczeństwa (wykorzystując przede wszystkim autorskie zestawienie J. Woźniaka), a w kolejnej części przechodzi do zdefiniowania pojęcia systemu bezpieczeństwa. Część ta jest przedstawiona w sposób usystematyzowany i czytelny, wątpliwości budzi jednak fakt kilku przypadków zbyt nadmiernego eksploatowania poszczególnych pozycji literatury (np. artykuł N. Iershova i V. Garkusha na stronach 26-28 rozprawy). Autor słusznie rozpoczął rozprawę doktorską od kwestii ontologicznych związanych z poszczególnymi kluczowymi dla podjętej problematyki pojęciami, jednak „w gąszczu" podawanych definicji brak mi jasnego wskazania, którą definicję Autor przyjmuje w toku dalszych prac oraz jasnego zdefiniowania kluczowych zagadnień poruszanych w rozprawie, a mianowicie zarządzania bezpieczeństwem przedsiębiorstwa, zarządzania bezpieczeństwem informacji przedsiębiorstwa (mam wrażenie, iż Autor traktuje te zwroty jako synonimy) oraz zarządzania poufnością informacji.

Reasumując, uważam, iż bardziej wartościowym podejściem w tym rozdziale byłoby dokonanie analizy bibliometrycznej literatury (co sprowadza się do pytań Jak Autor dobrał poszczególne pozycje literatury? Z jakich baz korzystał? Na podstawie jakich słów kluczowych, Jaki zakres czasowy? I inne informacje charakterystyczne dla analizy bibliometrycznej). Jedynie w części metodycznej - podrozdział 4.4 pojawia się stwierdzenie, iż „zmapowano literaturę", ale nie skonkretyzowano co to właściwie znaczy. Jest to tym bardziej uzasadnione bowiem Autor na podstawie omawianej literatury stara się „potwierdzać hipotezy". Zdania takie pojawiają się na str. 45, 53 i innych. Takie same stwierdzenia pojawiają się również w rozdziale 2 (np. str. 64, 83, 92, 102 i 103) oraz rozdziale 3 (np. str. 111, 118, 137, 151). Postawione hipotezy nie powinny być weryfikowane (lub jak pisze Autor „częściowo potwierdzane") w ten sposób. Abstrahując od dyskusji na temat weryfikowania hipotez metodami jakościowymi (bez używania statystyki), z pewnością nie wolno tego robić na podstawie literatury, którą dodatkowo nie wiadomo w jaki sposób dobrano. Uważam to za duży błąd i słaby element całej rozprawy. Ten tok prac, który zaprezentował Doktorant może jedynie posłużyć do uzasadnienia sformułowania poszczególnych hipotez, a nie ich

„potwierdzania” (mam wrażenie, iż w niektórych miejscach o to Autorowi chodziło, np. ostatnie zdanie podrozdziału 1.2 „Rozważanie przedstawione w niniejszym podrozdziale częściowo potwierdzają założenia hipotezy szczegółowej, wykazując, że racjonalne zarządzanie bezpieczeństwem, łącznie z odpowiednimi strategiami oraz procesami decyzyjnymi, wpływa na zabezpieczenie zasobów i utrzymanie stabilności działania przedsiębiorstwa” (str. 37). Zresztą w podsumowaniu, Doktorant zamieścił informację, iż „wykorzystano metodę dedukcyjną wynikającą z analizy teorii do formułowania hipotezy głównej” – formułowania, a nie jak pisze Autor w pierwszych trzech rozdziałach „potwierdzania”.

Rozdział 2 koncentruje się na kluczowych aspektach implementacji zarządzania bezpieczeństwem informacji w przedsiębiorstwach. Omawia szczegółowo strategie ochrony zasobów informacyjnych, wskazując na istotę zabezpieczeń technicznych, organizacyjnych oraz proceduralnych. Analizuje także różnorodne modele zarządzania bezpieczeństwem informacji, ukazując ich zastosowanie w praktyce biznesowej. Szczególną uwagę poświęca metodom oceny ryzyka oraz systematycznemu wdrażaniu polityki bezpieczeństwa, podkreślając znaczenie zgodności z normami i regulacjami prawnymi w kontekście ochrony informacji w organizacjach. W rozdziale tym sprecyzowano też pojęcia bezpieczeństwa informacji i bezpieczeństwa informacyjnego oraz systemu zarządzania bezpieczeństwem informacji.

Rozdział 3 analizuje problematykę szpiegostwa korporacyjnego w kontekście zarządzania bezpieczeństwem informacji w sektorze technologii informacyjno-komunikacyjnych (ICT). Przedstawia różnice między szpiegostwem gospodarczym, przemysłowym i korporacyjnym, wskazując na ich kluczowe cechy, metody oraz odbiorców korzyści. Omówiono także specyfikę zarządzania bezpieczeństwem informacji w organizacjach ICT, podkreślając znaczenie ochrony przed nielegalnym pozyskiwaniem danych, m.in. poprzez analizę operacyjną, socjotechnikę i działania insiderów. W rozdziale zidentyfikowano współczesne wyzwania związane z rozwojem technologicznym, takie jak cyberzagrożenia, phishing, spoofing oraz spyware, wskazując na konieczność wdrażania zaawansowanych strategii ochrony informacji w przedsiębiorstwach. Rozdział ten jst napisany w przejrzysty i logiczny sposób. Wątpliwości budzi już wspomniana przez Doktoranta praktyka eksploatowania przez dłuższe partie tekstu jednej pozycji literatury (np. str. 106-110, artykuł K. Kozłowskiego).

Rozdział 4 stanowi omawianą w punkcie 4 recenzji część metodyczną. Niestety, już pierwsze zdanie tego rozdziału jest co najmniej niefortunne „Przedmiotem badań niniejszej dysertacji jest analiza zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych (ICT), ze szczególnym uwzględnieniem wpływu szpiegostwa korporacyjnego na postrzeganie zagrożeń przez pracowników”. Rozdział ten zawiera wiele cennych informacji odnośnie dobranych metod badań i organizacji całego procesu badawczego. Jednak zamiast skonkretyzować niektóre informacje, Doktorant charakteryzuje w sposób ogólny konkretne metody- co w rozprawie doktorskiej jest zbędne, bo to nie jest podręcznik. Tytułem przykładu na str. 163, Doktorant w obszerny sposób charakteryzuje czym jest (i czym nie jest) wywiad, jaki może mieć charakter pytań, jakie są cechy wywiadu, ale nie precyzuje jakiego rodzaju wywiad sam zastosował. Podobnie brak jest informacji jakiego rodzaju ankietę (mowa tu o metodzie) wykorzystano w badaniach.

Rozdział 5 pracy doktorskiej koncentruje się na analizie poziomu świadomości pracowników jako kluczowego czynnika wpływającego na efektywność zarządzania bezpieczeństwem informacji w sektorze technologii informacyjno-komunikacyjnych. Badania obejmują m.in. kwestie postrzegania zagrożeń wynikających ze szpiegostwa korporacyjnego

oraz ich wpływu na bezpieczeństwo organizacji. W oparciu o wyniki badań eksperckich i ankietowych, rozdział przedstawia zależności między świadomością pracowników a skutecznością strategii bezpieczeństwa. Formułuje rekomendacje dotyczące optymalizacji zarządzania bezpieczeństwem informacji. Ostatecznie, Autor proponuje model zarządzania bezpieczeństwem informacji uwzględniający m.in. edukację pracowników, wdrażanie technologicznych i proceduralnych zabezpieczeń oraz strategiczne podejście do minimalizacji ryzyka. Ponadto w rozdziale tym zweryfikowano przy pomocy metod statystycznych hipotezy H4.1-H4.8 (choć Doktorant w odniesieniu do numeracji hipotez H.4.6-H.4.8 sformułowanych w części metodycznej, niekonsekwentnie zastosował numerację hipoteza 6,7 oraz 8.).

Rozdział 6 koncentruje się na implementacji modelu zarządzania bezpieczeństwem informacji w sektorze technologii informacyjno-komunikacyjnych, obejmując trzy główne etapy: analizę i planowanie, wdrażenie i realizację oraz ewaluację i doskonalenie. Rozdział ten zawiera także przeprowadzone symulacje wdrożenia modelu zarządzania bezpieczeństwem informacji w organizacjach sektora ICT, ze szczególnym uwzględnieniem zagrożeń związanych ze szpiegostwem korporacyjnym. Wykorzystując oprogramowanie AnyLogic, przeprowadzono analizę wpływu trzech kluczowych czynników (znaczenia szkoleń, zapotrzebowania na regulacje prawne oraz postrzegania szpiegostwa jako zagrożenia) na gotowość przedsiębiorstw do reagowania na incydenty. Następnie rozdział ten koncentruje się na monitorowaniu i ewaluacji skuteczności wdrożenia modelu zarządzania bezpieczeństwem oraz jego optymalizacji. Przedstawiono kluczowe wskaźniki efektywności (KPI) oraz narzędzia analityczne, takie jak drzewa decyzyjne, regresja logistyczna i metoda Random Forest, umożliwiające ocenę skuteczności działań. Następnie omówiono proces optymalizacji, wskazując obszary wymagające usprawnień oraz zalecenia dotyczące dalszego doskonalenia strategii bezpieczeństwa. Podkreślono znaczenie integracji systemów, automatyzacji procesów oraz personalizacji szkoleń w celu zwiększenia odporności organizacji na zagrożenia.

Całość zamyka podsumowanie, w którym krótko opisano zawartość pracy oraz uzyskane wyniki. Podsumowanie kończy się wymienionymi enumeratywnie wnioskami końcowymi, co nadaje całemu wywodowi klarowności.

Ponadto, w części podsumowującej Autor dokonuje syntetycznej oceny wyników badań, odnosząc je do sformułowanych hipotez oraz celów pracy. Słusznie wskazuje również, iż opracowany model zarządzania bezpieczeństwem może służyć jako fundament dla dalszych badań w zakresie skuteczności ochrony danych, zwiększania świadomości pracowników w kontekście zagrożeń informacyjnych oraz optymalizacji procedur zarządzania ryzykiem.

Niewątpliwie mocną stroną pracy jest przejrzyste wprowadzanie do konkretnych zagadnień w poszczególnych częściach (rozdziałach i podrozdziałach), a także podsumowania w tychże częściach, co porządkuje i ułatwia czytelnikowi zrozumienie głównych wątków oraz pozwala na śledzenie logicznego toku argumentacji.

Podsumowując, struktura rozprawy jest adekwatna do przedmiotu badań. Kolejne rozdziały prowadzą czytelnika w sposób logiczny od podstaw teoretycznych, przez analizę zagrożeń i metod badawczych, aż do wyników badań i wniosków końcowych. Układ pracy pozwala na spójne przedstawienie kluczowych problemów oraz zaproponowanie autorskich rozwiązań.

6. Ocena formalna pracy

Dysertacja napisana poprawnym i zrozumiałym językiem, aczkolwiek występują liczne błędy stylistyczne i literówki (np. str. 20: „…tworzone są niezbędne warunku…"; str. 25 „*Taki sposób podejścia do zagadnienie…*"; str. 26 *„…rozważań na temat systemy bezpieczeństwa w przedsiębiorstwie …*"; str. 33 „*b) wektor procesów przetwarza" – i od następnej linijki „c) nia*"; str. 39 „a*) „zagrożenia niezależne od specjalistyczne wiedzy danej organizacji*"; strona 74 - punkt g - zamknięty nawias ale brak otwartego; str. 96 „*Model TSIM wyróżnia się poziomy …*"; str. 97 „*Zgodnie przedstawionym schematem …*"; str. 104 - „*W dalszej części przedstawiona zostanie szczegółowa analizy…*"; str. 108 *„…. działania związane z nwigilacją…*" ; str. 119 *„…którymi podąża atakowana organizacji*"; str. 146 „ *… problem współczesnej zarządzania…*"; str. 263„*Średniw wynik testu początkowego*"; str. 285 „*Wariant 8 jest szczególnie rekomendowana dla dużych organizacji. Ze względu na koszty, jej wdrożenie jest najbardziej uzasadnione…*". To są wybrane z pracy przykłady unaoczniające dużą skalę tego typu błędów. Ponadto autor niekonsekwentnie używa przecinków i kropek w tabelach, tzn. raz są przecinki w zdaniach w odpowiednich polach tabeli a raz nie ma – np. tab. 8, lub raz są kropki, a raz przecinki, np. tab. 12. Występują też sytuacje, w których kropka nie pojawia się na końcu zdania, np. „…*działań korygujących.(podetap 3)*" - str. 268.

Autor używa także „co najmniej niefortunnych zdań", np. podrozdział 1.4 - 5 linijka od góry: „*Niniejszy wstęp do rozdziału pracy naukowej ma na celu …*"; lub str. 122 „*W polskiej literaturze prawniczej i ustawodawstwie istnieje brak szczegółowych uregulowań….*" Kolejne zdanie ze str. 131 „*Selekcja konkretnej treści służącej za podstawę szantażu polega na dokładnej analizie zgromadzonych informacji oraz ocenie własnych zasobów do uzyskania (lub stworzenia) wymaganych dowodów, można podejść do organizacji strategii szantażu*". Autor odwołuje się do pozycji, które trudno ustalić lub używa odwołań, które trudno zidentyfikować, np. str. 71 „Niniejszy artykuł ma na celu zgłębienie definicji danych osobowych …." - nie wiadomo czy chodzi o artykuł 55, który jest podany w źródle pod tabelą 7 (5 linijek wcześniej), czy też o inny artykuł.

W pracy występują też nieprecyzyjne sformułowania, np. główka tabeli 17 lub 18 tytuł - „*organizacja zatrudnienia*" a chodzi o konkretne przedsiębiorstwo, w którym pracuje respondent. Ponadto bardzo wiele zdań (szczególnie w rozdziale 5) zaczyna się od liczby – zdania te w łatwy sposób można było skonstruować inaczej.

Nagminne pozostawiano też pół strony pustej (a czasami większej jej części jak choćby na stronie 51), albo pozostawiano jedynie tytułu tabeli – str. 69 lub tytułu podrozdziału str. 111.

Prezentowane wykresy powinny mieć opisane osie (np. oś X to najczęściej liczba osób), natomiast oś Y w zależności od prezentowanych badań to: poziom wykształcenia, wiek, staż pracy, stanowisko służbowe itp.).

Ponadto numeracja stron kończy się na stronie 318 – bibliografia. spis rysunków, tabel i wykresów, załączniki, abstract nie są już numerowane.

Reasumując, wskazane przykłady uchybień stylistycznych, redakcyjnych oraz niekonsekwencje w formatowaniu, choć liczne, nie mają wpływu na ogólną wartość merytoryczną rozprawy. Należy jednak zwrócić na nie uwagę, aby w przyszłości poprawić klarowność i spójność językową.

7. Konkluzja końcowa

Rozprawa doktorska mgr Kajetana Kozłowskiego pt. „Zarządzanie bezpieczeństwem przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych a szpiegostwo korporacyjne" stanowi wartościowe i oryginalne opracowanie naukowe, które wpisuje się w dyscyplinę nauk o zarządzaniu i jakości.

Badania zawarte w rozprawie doktorskiej, analizują zagrożenia wynikające ze szpiegostwa korporacyjnego oraz strategie zarządzania bezpieczeństwem przedsiębiorstw działających w sektorze ICT - podejmują tym samym aktualny i istotny problem z perspektywy zarówno teoretycznej, jak i praktycznej.

Najważniejszym osiągnięciem rozprawy jest opracowanie autorskiego modelu zarządzania bezpieczeństwem, który integruje podejście techniczne, organizacyjne i proceduralne w celu ochrony przed zagrożeniami wynikającymi z działań szpiegowskich. Model obejmuje kluczowe aspekty zarządzania bezpieczeństwem, w tym identyfikację zagrożeń, precyzyjne określenie ról i odpowiedzialności, podnoszenie świadomości pracowników, zastosowanie zaawansowanych technologii ochronnych oraz systematyczne monitorowanie efektywności działań. Jego struktura została dostosowana do specyfiki sektora ICT, który cechuje się dynamicznym rozwojem technologicznym, wymagającym wysokiego stopnia elastyczności i zdolności adaptacyjnych. Dodatkowo model ten opiera się na wynikach przeprowadzonych badań empirycznych oraz symulacji komputerowych, co czyni go użytecznym narzędziem dla menedżerów i specjalistów ds. bezpieczeństwa informacji.

Do słabych stron zaliczyć można nieprecyzyjny układ celów, sposób weryfikowania hipotez badawczych, a także niedookreślenie metod badań (Jakiego rodzaju wywiad? Jakiego rodzaju ankieta?)

Stwierdzam, że oceniana dysertacja spełnia wymogi stawiane pracom doktorskim zgodne z ustawą z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce (Dziennik Ustaw z 2022 r. poz.574). Wnioskuję zatem o jej przyjęcie i dopuszczenie przedłożonej mi do recenzji rozprawy Pana mgr Kajetana Kozłowskiego do publicznej obrony.