

Uniwersytet Gdański
Wydział Zarządzania
Katedra Zachowań Organizacyjnych
dr hab. Piotr Wróbel, prof. uczelni

Sopot, 11 lutego 2025 roku

Recenzja rozprawy doktorskiej mgr. Kajetana Kozłowskiego pt. „Zarządzanie bezpieczeństwem przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych a szpiegostwo korporacyjne” przygotowanej pod opieką naukową dr hab. inż. Anny Brzozowskiej, prof. PCz

Podstawa sporządzenia recenzji

Podstawę formalną sporządzenia recenzji stanowi pismo Przewodniczącej Rady Dyscypliny Naukowej Nauki o Zarządzaniu i Jakości Politechniki Częstochowskiej, Pani dr hab. Agaty Mejsasz-Lech, prof. PCz z dnia 17.12.2024 roku, informujące o powołaniu mnie na recenzenta rozprawy doktorskiej Pana mgr Kajetana Kozłowskiego pt. „Zarządzanie bezpieczeństwem przedsiębiorstwa w sektorze technologii informacyjno-komunikacyjnych a szpiegostwo korporacyjne”. Praca została przygotowana pod kierunkiem naukowym Pani dr hab. inż. Anny Brzozowskiej, prof. PCz. Postępowanie w sprawie nadania stopnia doktora prowadzone jest w dziedzinie nauk społecznych, w dyscyplinie nauki o zarządzaniu i jakości. Recenzję sporządzono na podstawie otrzymanego maszynopisu.

1. Ocena wyboru problemu badawczego

Autor sformułował problem badawczy w postaci pytania: Jakie wyzwania dla zarządzania bezpieczeństwem informacji w przedsiębiorstwie sektora technologii informacyjno-komunikacyjnych wynikają ze zróżnicowanego postrzegania przez pracowników zagrożeń ze strony szpiegostwa korporacyjnego?

Dodatkowo wskazano szczegółowe problemy badawcze:

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 ostatnich latach badania potwierdzają rosnącą skalę zagrożeń bezpieczeństwa informacji w przedsiębiorstwach. Jednym z istotnych zagrożeń, zwłaszcza dla wiodących podmiotów sektora ICT, staje się szpiegostwo korporacyjne. Roczne straty przedsiębiorstw z powodu działań o charakterze szpiegostwa korporacyjnego szacowane są na setki miliardów dolarów (Koen, London, 2019). W opinii recenzenta wybrany problem badawczy jest więc bardzo aktualny oraz ważny poznawczo i aplikacyjnie.

Należy jednak zauważyć, że w rozprawie brakuje wyraźnego zdefiniowania luki badawczej. Trudno bowiem za takie uznać sformułowanie ze strony 154: „(...) temat podjęty w dysertacji stanowi pewne novum i nie był szerzej podejmowany przez badaczy naukowych, należy zaznaczyć, iż dostępna literatura na ten temat jest ograniczona”. Tymczasem jest to istotna kwestia przy wyborze problemu badawczego a następnie definiowaniu celów badania. Dobrą praktyką jest wykorzystanie w tym celu np. systematycznego przeglądu literatury na wybrany temat w oparciu o uznane bazy publikacji, np. Web of Science, Scopus.

2. Ocena sformułowanych celów oraz metodyki badania

Autor jako główny cel rozprawy postawił opracowanie modelu zarządzania bezpieczeństwem w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych, który uwzględni zróżnicowane postrzeganie zagrożeń wynikających ze szpiegostwa korporacyjnego przez pracowników, w celu zwiększenia ochrony danych i tajemnicy przedsiębiorstwa.

Dodatkowo w rozprawie przyjęte zostały cele szczegółowe:

C1: Identyfikacja roli i znaczenia bezpieczeństwa w zarządzaniu przedsiębiorstwem,

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

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

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

h

Główny cel rozprawy oceniam pozytywnie w świetle badań przedstawionych przez Autora, które wskazują na rosnące zagrożenie przedsiębiorstw sektora ICT zjawiskiem szpiegostwa korporacyjnego. Postawiony cel dotyczy ważnego problemu, a uzyskane wyniki badań mogą mieć potencjalnie wysoką wartość nie tylko dla podmiotów analizowanego sektora.

Każdy model powinien być dopasowany do uwarunkowań funkcjonowania odbiorcy modelu. W uzasadnieniu wybranego problemu badawczego oraz postawionego celu zabrakło jednak wskazania, dlaczego Autor spośród wielu determinant modelu zarządzania bezpieczeństwem wybrał jako krytyczny czynnik postrzeganie zagrożeń przez pracowników.

Cele szczegółowe oceniam również pozytywnie, układają się one w sekwencję prac badawczych od studiów literaturowych poprzez zebranie i zinterpretowanie materiału empirycznego. W szczególności istotne znaczenie mają cele trzeci i czwarty, które bezpośrednio są związane z zagrożeniem szpiegostwa korporacyjnego.

W pracy przyjęto 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. Uzupełnieniem hipotezy głównej były hipotezy szczegółowe. Zaproponowane hipotezy są bezpośrednio związane z problemem badawczym, są spójne z głównym celem pracy oraz mają istotne znaczenie dla badanych zagadnień.

Autor podzielił proces badawczy na pięć etapów:

- etap I: studia literaturowe,
- etap II: indywidualne wywiady z 12 ekspertami w zakresie bezpieczeństwa z 6 przedsiębiorstw sektora ICT,
- etap III: badanie ankietowe pracowników 6 przedsiębiorstw sektora ICT (466 respondentów),
- etap IV: opracowanie modelu zarządzania bezpieczeństwem przedsiębiorstwa sektora technologii informacyjno-komunikacyjnych,
- etap V: symulacja komputerowa mającą na celu sprawdzenie stworzonego modelu oraz przygotowanie proponowanych narzędzi do ewaluacji i monitorowania wdrożenia oraz optymalizacji modelu na podstawie wyników wdrożenia.

Doktorant zastosował zróżnicowane metody badawcze, zarówno jakościowe jak i ilościowe, a kolejność ich wykorzystania jest logiczna. Duża różnorodność zastosowanych metod i technik badawczych pozytywnie świadczy o warsztacie badawczym Pana Kajetana Kozłowskiego.

Badania empiryczne zostały zawężone do dużych przedsiębiorstw sektora ICT, co oceniam pozytywnie. Dzięki temu udało się zachować Autorowi dużą porównywalność wyników. Na podkreślenie zasługuje uwzględnienie etapu walidacji modelu, co nie zawsze jest standardem w rozprawach doktorskich. Załączone

narzędzia badawcze opracowane przez Autora oceniam pozytywnie. Podsumowując, zaprojektowana metodyka badania jest adekwatna do postawionych celów i stanowi pozytywną stronę recenzowanej rozprawy doktorskiej.

3. Ocena merytoryczna pracy

Praca doktorska ma objętość 318 stron tekstu podstawowego, dodatkowo Autor dołączył bibliografię oraz załączniki, w tym treść wywiadów z ekspertami (załącznik nr 1) oraz kwestionariusz ankiety (załącznik nr 2). Struktura pracy jest następująca: wstęp, sześć rozdziałów, podsumowanie, bibliografia, netografia, spis rysunków, tabel, wykresów, załączniki. Układ pracy jest czytelny i logiczny, zachowana została równowaga pomiędzy częścią teoretyczną a empiryczną.

Autor korzysta z licznych źródeł, bibliografia liczy 200 pozycji, w tym około 40% stanowią publikacje anglojęzyczne. Pozytywnie należy ocenić aktualność źródeł, pozycje opublikowane po 2015 roku to 100 książek i artykułów. Osobno przedstawiona została netografia, na którą składa się 45 pozycji. Dobór literatury wskazuje na dobrą znajomość przedmiotu badań, Autor korzystał z dorobku różnych dyscyplin, m.in. nauk o zarządzaniu i jakości, nauk o bezpieczeństwie, informatyki, psychologii.

W części teoretycznej rozprawy Autor skoncentrował swój wywód na zagadnieniach bezpieczeństwa przedsiębiorstwa, bezpieczeństwa informacji w przedsiębiorstwie oraz szpiegostwa korporacyjnego w kontekście sektora technologii informacyjno-komunikacyjnych. Na podstawie przeglądu literatury z zakresu zarządzania, bezpieczeństwa, informatyki Autor prezentuje kluczowe zagadnienia dla wybranego problemu badawczego. Wywód jest logiczny i konsekwentny.

Pewną wątpliwość budzi jednak wprowadzenie w tytule pkt. 2.2 pojęcia zarządzania poufnością informacji, podczas gdy w całym dotychczasowym i późniejszym wywodzie Autor konsekwentnie stosuje termin zarządzania bezpieczeństwem informacji. Inne wątpliwości związane są z porównaniem terminów szpiegostwa gospodarczego, przemysłowego i korporacyjnego (pkt. 3.1 i 3.2). Autor wskazując na podobieństwa i różnice pomiędzy tymi terminami decyduje się poświęcić swoje badanie problematyce szpiegostwa korporacyjnego wskazując, że jest to specyficzna forma szpiegostwa przemysłowego, lecz często realizowana z większą precyzją i skierowana na bardzo szczegółowe cele strategiczne wewnątrz sektora korporacyjnego. Takie rozróżnienie nie wynika jednak z dokonanego przeglądu literatury. Przeciwnie przeprowadzona analiza wskazuje, że pojęcia szpiegostwa korporacyjnego i przemysłowego w znacznym stopniu się pokrywają. Pomimo wskazanych usterek uważam, że część teoretyczna rozprawy stanowi wartościowe i solidne wprowadzenie w kontekst badania empirycznego.

Kluczową część rozprawy stanowi prezentacja przeprowadzonych badań empirycznych, wypracowanego modelu oraz efektów jego walidacji. Wprowadzenie do tej części stanowi rozdział czwarty, który prezentuje

metodykę badań własnych. W syntetyczny sposób przedstawiony został zakres badań, cele i hipotezy badawcze oraz sekwencja badań wraz z metodami, technikami i narzędziami badawczymi. Rozdział stanowi właściwe wprowadzenie do prezentacji wyników badań.

Rozdział 5 opisujący wyniki badań empirycznych oraz proces opracowania modelu zarządzania bezpieczeństwem informacji stanowi najobszerniejszą część recenzowanej rozprawy licząc 87 stron. Połowę tego tekstu stanowi omówienie wywiadów z ekspertami oraz badań ankietowych z udziałem pracowników (pkt. 5.1). Niezależnie od wartości merytorycznej tego punktu, którą oceniam wysoko, dyskusyjne jest połączenie wyników wywiadów z wynikami badania ankietowego (różny zakres tematyczny). Wydaje się, że z punktu widzenia czytelnika lepsze było rozdzielenie tych treści na dwa podrozdziały. Przeprowadzone wywiady umożliwiły Autorowi poznanie zagrożeń, z którymi muszą sobie radzić badane przedsiębiorstwa oraz podejmowanych działań im przeciwdziałającym. Wywiady potwierdziły znaczenie podjętego problemu badawczego, a jednocześnie dostarczyły Autorowi szeregu informacji przydatnych do opracowania kwestionariusza ankiety w celu przeprowadzenia kolejnego etapu badania. Warto podkreślić, że sposób opisanie wyników wywiadów jest przejrzysty, a Autor podkreśla kluczowe wnioski z nich płynące.

Następnie opisane zostały wyniki badań ankietowych. Na uwagę zasługuje stosunkowo duża próba badawcza (466 respondentów) oraz jej struktura (dość równomierny rozkład pod względem reprezentowanych przedsiębiorstw, pełnionego stanowiska i wieku). Uzyskane odpowiedzi zostały przedstawione w postaci rysunków wraz z analizą i interpretacją Autora. Badania wskazują na duże zróżnicowanie wiedzy respondentów na temat zagrożenia w postaci szpiegostwa korporacyjnego, a w przypadku wielu pytań znaczna część udzielonych odpowiedzi to: „Nie mam zdania”. Szkoda, że w ankiecie nie znalazły się pytania o działania badanych przedsiębiorstw związane ze zwalczaniem szpiegostwa, a które mogli obserwować lub w nich uczestniczyć respondenci, np. szkolenia, kampanie informacyjne, wdrażanie procedur, audyty. Ankieta nie dostarcza więc wiedzy czy pracownicy badanych firm są przygotowywani do radzenia sobie z analizowanym zagrożeniem. Niezależnie jednak od tej uwagi, uważam, że przeprowadzone badanie jest istotne i stanowi ważny krok w kierunku zaproponowania modelu zarządzania bezpieczeństwem informacji, co była nadrzędnym celem rozprawy.

Wyniki badań kwestionariuszowych zostały poddane analizie statystycznej w celu weryfikacji pięciu hipotez. Ta część daje pogłębione spojrzenie w zagadnienie postrzegania problematyki szpiegostwa korporacyjnego przez różne grupy pracowników i stanowi wartościową część rozprawy.

Kolejnym krokiem prowadzącym do stworzenia modelu była analiza regresji mająca na celu zidentyfikowanie czynników wpływających na świadomość pracowników i kontrahentów o zagrożeniu ze strony szpiegostwa oraz czynników wpływających na postrzeganie szpiegostwa korporacyjnego jako zagrożenia dla przedsiębiorstwa. Ta część badań umożliwiła określenie konstrukcji modelu. Następnie opracowany model został zwalidowany przy pomocy symulacji komputerowej. Wyniki symulacji umożliwiły na dopracowanie wypracowanych wcześniej wariantów modelu.

Zaproponowany model oceniam pozytywnie, jego wdrożenie powinno, w mojej opinii, wzmocnić odporność organizacji na zagrożenia związane ze szpiegostwem korporacyjnym. Warto podkreślić, że wypracowany model ma na tyle uniwersalny charakter, że może być zastosowany nie tylko do przeciwdziałania zagrożeniom wynikającym ze szpiegostwa korporacyjnego, ale także z innych źródeł, np. z cyberprzestępczości. O utylitarnym charakterze rozprawy świadczy nie tylko użyteczność samego modelu zarządzania bezpieczeństwem, ale również propozycja działań składających się na wdrożenie modelu (pkt. 6.1). W ten sposób Autor wypracował kompleksowe rozwiązanie możliwe do zastosowania w przedsiębiorstwach sektora technologii informacyjno-komunikacyjnych.

Podsumowując, uważam, że główny cel rozprawy wraz z celami szczegółowymi zostały osiągnięte w zadowalającym stopniu.

Zagadnienia do dyskusji:

1/ Zaproponowany model zarządzania bezpieczeństwem powstał na bazie badań z udziałem dużych przedsiębiorstw sektora technologii informacyjno-komunikacyjnych. Czy model może być stosowany w małych i średnich podmiotach z tego sektora? A jeżeli tak, to jakich wymaga zmian?

2/ Czym różni się zaproponowany model od dotychczas opisywanych w literaturze modeli zarządzania bezpieczeństwem?

3/ Współczesne organizacje wiedzy kładą duży nacisk na proces dzielenia się wiedzą pomiędzy pracownikami. Z drugiej strony, wiedza jako źródło przewagi konkurencyjnej powinna podlegać ochronie. Jak można pogodzić te cele w trakcie wdrażania kultury bezpieczeństwa, która powinna wspierać zaproponowany przez Autora model zarządzania bezpieczeństwem?

4. Ocena redakcji pracy

Praca napisana jest poprawnym i fachowym językiem, a liczne tabele i rysunki wzbogacają tekst rozprawy. Autor nie ustrzegł się jednak błędów językowych oraz redakcyjnych. Przykładowo na stronie 16 używa sformułowania „ujęcie statystyczne” zamiast „ujęcie statyczne”; na stronie 69 znajduje się tytuł tabeli, a samą tabelę można odnaleźć na kolejnej stronie; na stronie 73 Autor stosuje niewłaściwe wyliczenie danych (punkty od a do g). Należy przypomnieć, że błędem jest używanie słowa ryzyko w liczbie mnogiej jako „ryzyka” (strony 84, 87). Część rysunków została wykorzystana bez tłumaczenia na język polski (np. rysunki nr 5, 21, 22).

5. Ocena końcowa dysertacji

Recenzowana praca doktorska stanowi wartościowe badanie osadzone na ugruntowanych podstawach teoretycznych. Podjęty problem badawczy jest istotny i odpowiada na aktualne potrzeby przedsiębiorstw nie tylko sektora ICT. Autor udowodnił swoje kompetencje w zakresie dostrzegania, formułowania i rozwiązania postawionego problemu badawczego. W swojej pracy potwierdził dobrą znajomość przedmiotu badań, umiejętność wyboru i zastosowania właściwych metod badawczych oraz dojrzałej interpretacji uzyskanych wyników.

Pomimo pewnych uwag krytycznych i niedoskonałości, praca Pana mgr Kajetana Kozłowskiego spełnia wymagania ustawy Prawo o szkolnictwie wyższym i nauce z 20 lipca 2018 roku, w szczególności:

- wykazuje ogólną wiedzę teoretyczną kandydata w dyscyplinie Nauki o zarządzaniu i jakości,
- wykazuje umiejętność samodzielnego prowadzenia pracy naukowej,
- stanowi oryginalne rozwiązanie problemu naukowego.

Moja opinia o recenzowanej rozprawie jest więc pozytywna. Rekomenduję Radzie Dyscypliny Naukowej Nauki o Zarządzaniu i Jakości Politechniki Częstochowskiej dopuszczenie Pana mgr Kajetana Kozłowskiego do publicznej obrony.

