Dr hab. Marzena Stor, prof. UEW
Katedra Zarządzania Kadrami
Wydział Zarządzania Uniwersytet
Ekonomiczny we Wrocławiu

Wrocław, 09.06.2022 r

OCENA OSIĄGNIĘĆ
DR. INŻ. PAWŁA KOBISA UBIEGAJĄCEGO SIĘ O NADANIE
STOPNIA DOKTORA HABILITOWANEGO
W DZIEDZINIE NAUK SPOŁECZNYCH W DYSCYPLINIE NAUK O ZARZĄDZANIU

Podstawa formalno-prawna wykonania recenzji:

- Pismo sporządzone przez dr hab. Agatę Mesjasz-Lech, prof. PCz, Przewodniczącą Rady Dyscypliny Naukowej Nauki o Zarządzaniu i Jakości na Wydziale Zarządzania Politechniki Częstochowskiej z dnia 30.03.2022 r. informujące o powołaniu mnie na recenzenta przez Radę Doskonałości Naukowej w postępowaniu habilitacyjnym dra inż. Pawła Kobisa w dziedzinie nauk społecznych w dyscyplinie nauk o zarządzaniu i jakości.
- Pismo od Rady Doskonałości Naukowej z dnia 28.02.2022 roku w sprawie powołania mnie na recenzenta do komisji habilitacyjnej w sprawie nadania stopnia doktora habilitowanego dr. Pawłowi Kobisowi w dziedzinie nauk społecznych w dyscyplinie nauk o zarządzaniu i jakości.
- Uchwała nr 30/2022 z dnia 29.03.2022 roku Rady Dyscypliny Naukowej Nauki o Zarządzaniu i Jakości Wydziału Zarządzania Politechniki Częstochowskiej w sprawie powołania mnie na recenzenta do komisji habilitacyjnej w celu przeprowadzenia postępowania habilitacyjnego w dziedzinie nauk społecznych w dyscyplinie nauki o zarządzaniu i jakości wszczętego na wniosek dr. inż. Pawła Kobisa.
- Wniosek o przeprowadzenie postępowania w sprawie nadania stopnia doktora habilitowanego w dziedzinie nauk społecznych w dyscyplinie nauki o zarządzaniu i jakości z dnia 20.12.2021 roku.

* Recenzja sporządzona jest zgodnie z art. 219 ust.l pkt. 2 i 3 ustawy z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2020 roku poz. 85, z późn. zm.).

1. OGÓLNA CHARAKTERYSTYKA PRZEBIEGU PRACY NAUKOWO-ZAWODOWEJ

Stopień doktora nauk ekonomicznych w dyscyplinie nauk o zarządzaniu został nadany Habilitantowi w 2010 roku uchwałą Rady Wydziału Zarządzania Akademii Górniczo-Hutniczej w Krakowie. Poprzedzało go uzyskanie dwóch tytułów magistra na Politechnice Częstochowskiej: w 2001 roku na Wydziale Elektrycznym oraz w 2003 roku na Wydziale Zarządzania. Na tej samej Uczelni ukończył też Fakultatywne Studia Pedagogiczne w 2001 r.

Od ukończenia pierwszych studiów magisterskich (2001 rok) pracuje w Katedrze Informacyjnych Systemów Zarządzania na Politechnice Częstochowskiej. Do 2010 roku był zatrudniony na stanowisku asystenta, a następnie awansował na stanowisko adiunkta. Habilitant wskazuje tę Uczelnię jako podstawowe miejsce pracy. Dodatkowo w latach 2001-2018 w różnych przedziałach czasowych był zatrudniany na stanowisku asystenta lub adiunkta w takich szkołach, jak: Wyższa Szkoła Hotelarstwa i Turystyki w Częstochowie, Wyższa Szkoła Zarządzania w Częstochowie, Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Wyższa Szkoła Ekonomii i Prawa w Kielcach. Ponadto odbył 7-miesieczny staż przemysłowy w przedsiębiorstwie produkcyjno-handlowym Linex

w Częstochowie, w czasie którego pogłębiał wiedzę praktyczną w zakresie zarządzania informacją oraz wykorzystywania technik i technologii informatycznych.

Można zatem powiedzieć, że ścieżka rozwoju naukowego, badawczego oraz dydaktycznego dra inż. Pawła Kobisa w jego pracy zawodowej była związana z uznanymi ośrodkami badawczymi i akademickimi.

2. OCENA GŁÓWNEGO OSIĄGNIĘCIA NAUKOWEGO

Dr inż. Paweł Kobis jako swoje główne osiągnięcie naukowe wskazał monografię naukową zt. *Zarządzanie bezpieczeństwem informacji w systemach informacyjnych małych i średnich przedsiębiorstw z uwzględnieniem czynnika ludzkiego,* wydaną w 2021 roku przez Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora" w Toruniu. Wydawnictwo znajduje się pod nr 505 w wykazie wydawnictw z poziomu I wg Komunikatu Ministra Edukacji i Nauki z dnia 22 lipca 2021 r. w sprawie wykazu wydawnictw publikujących recenzowane monografie naukowe.

Praca składa się ze *Wstępu,* pięciu rozdziałów, *Zakończenia* oraz spisów rzeczowych, kwestionariusza badawczego, streszczenia w j. polskim i angielskim zamieszczonych na końcu. Jej objętość to 424 stron i zawiera bogate wsparcie wizualizacyjne: 66 rysunków i 54 tabele. Przegląd literatury obejmuje 423 pozycje literatury polskiej i zagranicznej.

Wstęp stanowi klarowne wprowadzenie merytoryczne do głównych założeń koncepcyjnych i rozwiązań metodycznych przyjętych w pracy. Poza zwięzłym streszczeniem poszczególnych rozdziałów monografii znajdujemy też tutaj bardzo dobrze napisane uzasadnienie dla podejmowanej problematyki oraz wyjaśnienie dla zidentyfikowanej **luki badawczej.** Ponadto Autor definiuje **główne założenie badawcze,** które zostało przez niego przyjęte w rezultacie przeprowadzonych studiów literaturowych, a które stanowi o tym, że w zarządzaniu współczesnymi przedsiębiorstwami istnieje potrzeba uwzględniania czynnika ludzkiego w procesach bezpieczeństwa informacji. Autor dodaje też, że nie można ignorować pozatechnicznych aspektów zwiększania ryzyka zagrożenia w postaci pejoratywnych zachowań pracowników, klientów, partnerów biznesowych lub też celowego i negatywnego działania osób, których celem jest nielegalne przejęcie lub zniszczenie informacji.

We *Wstępie* sformułowano **podstawowy cel badawczy monografii,** którym jest wykazanie, że w przedsiębiorstwach małych i średnich nie zarządza się bezpieczeństwem informacji w sposób skuteczny i kompletny z powodu pomijania aspektów związanych z czynnikiem ludzkim oraz zaproponowanie koncepcji podsystemu uwzględniającego ten czynnik. W tym kontekście Dr inż. Paweł Kobis zaznacza, że rozwiązanie systemowe powinno obejmować wszystkie procesy zarządzania informacją w przedsiębiorstwie, reprezentować podejście holistyczne uwzględniające wszystkie elementy systemu informacyjnego oraz wszystkie osoby przetwarzające informację lub mogące mieć wpływ na jej przetwarzanie. W mojej ocenie pierwsza część tego celu jest mało ambitna i nie za bardzo dopowiada monografii naukowej. Jest związana z badaniami o charakterze deskryptywnym, czyli takimi, które nie zmierzają do zidentyfikowania jakiś prawidłowości o charakterze naukowym, czy też odkrycia pewnych zależności istniejących w badanym fragmencie rzeczywistości organizacyjnej. Natomiast drugi komponent tego celu zapowiada wyjście z własną, bardzo ambitna propozycją. Celowi badawczemu monografii towarzyszy **hipoteza badawcza,** która w mojej ocenie ma słaby walor naukowy i w sensie *stricte* badawczym stanowi raczej tezę, o czym piszę w komentarzach do rozdziału 4.

Przechodząc do omówienia poszczególnych rozdziałów należy zauważyć, że każdy rozpoczyna się wyodrębnionym swego rodzaju wprowadzeniem, a kończy podsumowaniem.

Rozdział 1. poświęcony jest zarządzaniu informacją oraz systemom zarządzania informacją w przedsiębiorstwach. Komponuje go sześć podrozdziałów, w których Autor zajmuje się jakością i cechami informacji, w tym informacji zarządczej, przeciążeniami informacyjnymi, rolami systemów informacyjnych i informatycznych w przedsiębiorstwach, funkcjonalnymi komponentami systemu informatycznego w procesach zarządzania informacją, zarządzaniem zasobami informacyjnymi w modelu chmury obliczeniowej oraz aspektami pozatechnicznymi w zarządzaniu informacją.

Toczone wywody charakteryzuje wysoki poziom interdyscyplinarności, albowiem podejmowane są kwestie techniczne, psychologiczne, ekologiczne, zarządcze, społeczne, a nawet edukacyjne. Towarzyszą temu wartościowe analizy terminologiczne odnoszące się do głównych zagadnień problemowych, a dokonywane na podstawie przeprowadzonych studiów literaturowych. W tym kontekście brakuje wskazania wprost, jakie definicje zostały przyjęte przez Habilitanta dla pojęć mających fundamentalne znaczenie w jego pracy, tj. informacji, informacji zarządczej, zarządzania informacją, systemu informacyjnego czy systemu informatycznego. Jest to o tyle ważne, że są wśród nich pojęcia zawarte w tytule monografii oraz określające zjawiska będące przedmiotem badań empirycznych.

Z pewnością zaletą tego rozdziału są własne propozycje koncepcyjne Autora. Można się tutaj odwołać choćby do ciekawego pomysłu zamkniętych procesów informacyjnych w relacji organizacja - otoczenie, który został przedstawiony na rysunku 1.7. Jednakże tytuł rysunku jest zbyt ogólny. Jest w nim mowa o wzajemnym odziaływaniu otoczenia i organizacji, ale brakuje doprecyzowania, że nie chodzi o wszelakie rodzaje oddziaływania, a właśnie o oddziaływania informacyjne. Ważniejszym rozwiązaniem koncepcyjnym jest jednak autorski podział-jak to określa sam Habilitant-„na cztery płaszczyzny odnoszące się i wpływające na pozatechniczne zarządzanie informacją" (s. 88), nazwane też obszarami analizy (s. 16), które należy uwzględnić w zapewnianiu bezpieczeństwa informacji. W tym miejscu pragnę zauważyć, że zastosowanie pojęcia płaszczyzny uważam za niefortunne, bo w sensie logicznym powstaje pytanie, w jaki sposób płaszczyzna może wpływać na zarządzanie? W każdym razie ta koncepcja, poza opisem, została ujęta w postaci rysunku 1.13. zatytułowanego *Zasoby informacyjne w aspekcie pozatechnicznego zarządzania informacją,* a jeden z jej komponentów rozwinięty został na rysunku 1.15. (s. 95) zt. *Obszary pozatechnicznego zarządzania informacją.*

Pewne kontrowersje wzbudza również dyskusja na temat czynnika ludzkiego (s. 89-90). W swojej koncepcji Autor przyjmuje, że w przypadku organizacji gospodarczych zasoby ludzkie można sklasyfikować jako: pracowników, partnerów biznesowych, klientów oraz osoby trzecie, co graficznie przedstawia na rysunku 1.14. zt. *Zasoby ludzkie w procesie pozatechnicznego zarządzania informacją.* Co więcej, dodaje, że taką klasyfikację można rozszerzyć o stanowiska zajmowane przez pracowników w organizacji czy też rodzaje partnerów biznesowych. Wzbudza to o tyle wątpliwości, że w zarządzaniu organizacją, w tym zarządzaniu zasobami ludzkimi przyjmuje się, że ludzie nie są zasobem, lecz dysponują zasobem, na który składają się m.in. ich wiedza, umiejętności, zdolności, postawy, wartości, motywacja, cechy psychologiczne, a nawet zdrowie. Niemniej jednak należy uznać, że autorskie rozwiązanie dotyczące wyróżnienia czterech obszarów w zakresie pozatechnicznych aspektów zarządzania informacją jest o tyle cenne, że stanowi podstawę do rozważań dotyczących bezpieczeństwa informacji w ze względu na czynnik ludzki podejmowanych w kolejnych rozdziałach monografii. Mimo wskazanych mankamentów w mojej opinii rozdział zasługuje na wysoka pozytywną ocenę.

W **rozdziale 2.** przedmiotem zainteresowania jest bezpieczeństwo informacji w systemach informacyjnych na płaszczyźnie technicznej oraz czynnika ludzkiego. W jego strukturze znajduje się siedem podrozdziałów, w których kolejno Autor zajmuje się współczesnymi aspektami bezpieczeństwa, elementami funkcjonalnymi zapewniającymi bezpieczeństwo informacji, kategoriami zagrożeń informacji, zarządzaniem ryzykiem w zapewnianiu bezpieczeństwa informacji, czynnikiem ludzkim w zarządzaniu ryzykiem, polityką bezpieczeństwa informacji oraz klasycznym systemem zarządzania bezpieczeństwem informacji. Warto tu nadmienić, że struktura opisanego w ostatnim podrozdziale systemu oznaczonego akronimem SZBI stanowi fundament dla opracowania przez Habilitanta autorskiego podsystemu uwzględniającego czynnik ludzki. Ten rozdział również charakteryzuje pewien stopień interdyscyplinarności. Jest to widoczne choćby w dyskusji podejmowanej na temat definicji i atrybutów bezpieczeństwa informacji z perspektywy nauk technicznych, prawnych, społecznych i humanistycznych, ale też w kontekście różnych dyscyplin naukowych.

Co do ogólnej oceny, to rozdział jest napisany na dobrym poziomie merytorycznym, ale podobnie jak w poprzednim, mimo ciekawych i rzeczowych rozważań koncepcyjnych i definicyjnych, Autor nie podał, jakie rozumienie zostaje przyjęte w jego pracy dla tak istotnych pojęć, jak bezpieczeństwo informacji, bezpieczeństwo informatyczne, zarządzanie bezpieczeństwem informacji, zagrożenie informacji, czy zarządzanie ryzykiem.

Niemniej jednak, na szczególne docenienie zasługuje autorska koncepcja kompleksowego ujęcia bezpieczeństwa informacji w systemie informatycznym uwzględniającą opisane w rozdziale 1 poszczególne warstwy systemu informatycznego oraz wpływu czynnika ludzkiego. Została ona graficznie zaprezentowana na rysunku 2.3. Ten rysunek pozwala też w pewien sposób zrozumieć, dlaczego Autor stosował w poprzednim rozdziale pojęcie płaszczyzn w zarządzaniu informacją, gdyż prezentowane na tym rysunku komponenty bezpieczeństwa informacji (nazwane warstwami) przyjmują właśnie graficzną reprezentację płaszczyzn. Odnośnie do każdej z warstw komponujących autorski model, Autor szczegółowo charakteryzuje różne rodzaje zabezpieczeń. W podsumowaniu rozdziału, Habilitant pisze, że „nakreślona na tym rysunku perspektywa spaja ze sobą wszystkie najważniejsze elementy i procesy związane z ochroną informacji łącznie z czynnikiem ludzkim przenikającym zarówno pojęcia poznawcze, jak i poszczególne warstwy" (s.159-160). Mimo generalnie ładnego i starannie dobranego języka, którym posługuje się Autor, to zastosowane tutaj sformułowanie cechuje pewna niezgrabność, czy też nawet niedopatrzenie logiczne. Powstaje bowiem pytanie, w jaki sposób czynnik ludzki może coś przenikać i to bez względu na to, czy jest on - jak w rozdziale 1 - wadliwie utożsamiany z pracownikami, czy też definiowany w kategoriach wiedzy, umiejętności itd., o czym już wcześniej pisałam.

Pozytywnie odnoszę się natomiast do faktu, że komentując koncepcje innych autorów, Habilitant wyjaśnia, dlaczego niewłaściwe jest umiejscawianie zarządzania bezpieczeństwem informacji wśród składników samego bezpieczeństwa informacji (s. 106) i dlaczego w swojej koncepcji przyjął inne rozwiązanie. Argumentacja jest logiczna i wpisuje się w dyscyplinę nauk o zarządzaniu i jakości, co dowodzi, że Autora interesują aspekty zarządcze w zakresie podejmowanej problematyki. Mimo tej ciekawej, polemicznej dyskusji, dalej jednak nie wiadomo, co dokładnie w monografii oznacza zarządzanie bezpieczeństwem informacji.

Omawiana koncepcja nie jest jedyną autorska koncepcją prezentowaną w tej części pracy. Dokonany przegląd literatury w zakresie kategoryzacji zagrożeń w zakresie przetwarzania informacji

ze względu na czynnik ludzki zainspirował bowiem dra inż. Pawła Kobisa do wyjścia z własną propozycją podziału zagrożeń informacji na określone rodzaje oraz wskazania wzajemnych relacji między nimi. Koncepcja została graficznie przedstawiona na 2.5. (s. 119). W tym miejscu należy zgodzić się z Autorem, który konstatuje, iż powiązanie ze sobą zagrożeń pod względem występowania w kilku sklasyfikowanych kategoriach stanowi wartościowy wkład do procesów szacowania ryzyka, gdyż umożliwia wypracowanie skutecznych zabezpieczeń funkcjonujących kompleksowo na kliku płaszczyznach systemu informacyjnego (s. 120).

Dokonując oceny tego rozdziału należy zauważyć, że znajdują się w nim liczne, ciekawe opracowania przykładów praktycznych, w tym z wizualizacją graficzną, omawianych problemów. Rozdział tworzy również spójną całość i jest logicznie oraz merytorycznie powiązany z zarówno z poprzednim, jak i kolejnym rozdziałem.

Rozdział 3., zgodnie ze swoim tytułem, dotyczy człowieka w procesie zarządzania bezpieczeństwem informacji i podzielony jest na pięć podrozdziałów. Dyskusja prowadzona jest nad takimi zagadnieniami, jak rola czynnika ludzkiego w procesie zarządzania bezpieczeństwem informacji, zagrożenia dla informacji ze strony działań człowieka, czynnik ludzki i kompetencje pracowników ze względu na bezpieczeństwo informacji w nowych rozwiązaniach organizacyjnych przedsiębiorstw oraz sposoby ograniczania negatywnego wpływu czynnika ludzkiego w procesach zarządzania informacją. Ostatnie zagadnienie stanowi tytuł podrozdziału 3.5., do którego zgłaszam pewne zastrzeżenie. Otóż w tytule brakuje informacji, na co ten czynnik ludzki ma wpływać. Innymi słowy, istotniejsze z merytorycznego punktu widzenia jest wskazanie w tytule nie tyle, w czym ten wpływ ma miejsce, ale na co.

Odnośnie innych uwag do zawartości rozdziału 3, to w mojej ocenie przegląd literatury w zakresie definicji czynnika ludzkiego jest słaby, w sensie ilościowym i jakościowym, mając przy tym na uwadze analizy definicji w poprzednich częściach pracy. Mimo przywołania wielu różnych pozycji podano zaledwie trzy definicje czynnika ludzkiego - w ścisłym rozumieniu tego, czym jest definicja. W pozostałych przypadkach odwołania mają jedynie charakter kontekstowy albo autorzy pozycji literaturowych wymieniani są po przecinku pod ogólnym hasłem prac z obszaru zarządzania. Jednakże autorska definicja czynnika ludzkiego zaproponowana przez Habilitanta jest oryginalna i trafna (s. 165-166). Stanowi ona, że czynnik ludzki w aspekcie bezpieczeństwa zasobów informacyjnych jest zespołem cech, zachowań i kompetencji osób w jakimkolwiek stopniu zarządzających informacją, wpływających bezpośrednio lub pośrednio na stopień ryzyka jej utraty lub zniszczenia. Sformułowanie dotyczące bezpośredniego wpływu na stopień ryzyka może bowiem oznaczać zarówno jego zmniejszenie jak i zwiększenie.

Na pozytywną ocenę zasługuje też autorska koncepcja możliwych relacji i wpływu czynnika ludzkiego na bezpieczeństwo informacji między poszczególnymi podmiotami w kontekście otoczenia zewnętrznego i wewnętrznego organizacji. Warto tu przypomnieć, że wspomniane podmioty były omawiane w podrozdziale 1.6. w aspekcie pozatechnicznych czynników zarządzania informacją. Koncepcja została graficznie zaprezentowana na rysunku 3.2. (s. 169). Pozostaje ona w logicznym związku z przyjętą definicją czynnika ludzkiego, gdyż Autor podkreśla, że każdy z podmiotów może przyczyniać się zarówno do powstawania zagrożenia jaki i wzmacniania struktur systemu informacyjnego. W opinii Habilitanta najistotniejszą rolę ze wszystkich podmiotów należy jednak przypisać pracownikowi i stąd też w centrum wpływu czynnika ludzkiego Autor umieszcza pracownika. Na uwagę zasługuje dyskusja na temat interpretacji granic organizacji, która - jak

dowodzi Habilitant - ma istotne znaczenie dla przyjmowanych rozwiązań praktycznych w przedsiębiorstwach.

Kolejne autorskie rozwiązanie koncepcyjne dra inż. Pawła Kobisa w tej części pracy to zbiór kompetencji pracowników mających wpływ na bezpieczeństwo zasobów niematerialnych. Odnosząc się do tej koncepcji muszę na wstępie zaznaczyć, że Autor nie podaje przyjętej definicji dla kompetencji, a jedynie informuje, że dla niego punktem odniesienia jest struktura kompetencji pracowniczych opracowana przez T. Oleksyna (2018). W tym ujęciu kompetencje pracownicze to cechy psychofizyczne, wewnętrzna motywacja, stan zdrowia, uzdolnienia, predyspozycje, postawy, zachowania, umiejętności, doświadczenie, wiedza, wykształcenie oraz uprawnienia do działania (s. 213). Wracając do wspomnianego zbioru kompetencji, to ma on stanowić fundament w zakresie bezpieczeństwa zarządzania informacją na płaszczyźnie standardowej-jak to określa Autor-obsługi urządzeń komputerowych i komunikacji w sieciach lokalnych i sieci Internet. Płaszczyzna standardowa rozumiana jest jako przetwarzanie informacji w zakresie podmiotowej działalności organizacji gospodarczej bez działań specjalistycznych działów IT, w których należałoby ująć umiejętności związane z programowaniem, projektowaniem i modernizacją sieci, analizą kodu itp. (s. 217). W proponowanym rozwiązaniu koncepcyjnym kompetencje pracowników w zakresie bezpieczeństwa informacji na danym stanowisku są podzielone na trzy zasadnicze kategorie kompetencji, tj. cyfrowe, osobiste oraz związane ze stanowiskiem, które są precyzyjnie zdefiniowane i opisane (s. 217-218). Ponadto w sposób tabelaryczny (tabela 3.7., s. 218-212) Autor wymienia i opisuje 20 kompetencji uznanych przez niego za kompetencje mające wpływ na bezpieczeństwo zasobów informacyjnych. Ich analiza prowadzi do wniosku, że intencją Autora było uwzględnienie najważniejszych komponentów strukturalnych, na które Autor wskazywał odwołując się do koncepcji T. Oleksyna. O ile zgadzam się z ogólnym zakresem merytorycznym zaproponowanego zbioru kompetencji, to na poziomie poszczególnych jego komponentów pojawiają się różnorakie zastrzeżenia. Wymienię kilka z nich. Opisy kompetencji nie są jednorodne, w większości z nich nie ma klarownej definicji, czy też jasnego opisu behawioralnego. Zaprezentowane opisy powodują, że nie wszystkie kategorie kompetencji są rozłączne. Wiadomo, że między niektórymi kompetencjami istnieją istotne powiązania choćby z tego względu, że dotyczą tego samego podmiotu, jakim jest pracownik, ale brak rozłączności powoduje, że w praktyce trudno te kompetencje osobno identyfikować, oceniać czy też rozwijać. Jest to o tyle istotne, że w ostatnim podrozdziale Habilitant wskazuje na różne działania w obszarze zarządzania zasobami ludzkimi (ZZL), które można podejmować, aby kształtować te kompetencje we właściwy sposób i na właściwym poziomie. Ale jak to robić, skoro pojawia się problem z ich precyzyjnym określeniem, a zatem nie do końca wiadomo co tak naprawdę ma być kształtowane. Jako przykład można podać kompetencje pod nazwą postawy i zachowania - jak mają się one do kompetencji nazwanych: odpowiedzialność, profesjonalizm, asertywność czy lojalność? Tutaj pojawia się też wątpliwość co do kompetencji nazwanej wewnętrzna motywacja, albowiem brakuje wyjaśnienia do czego to ma być motywacja? W opisie są odwołania do postaw i zachowań oraz odpowiedzialności, które są przecież osobnymi kompetencjami. Inna uwaga dotyczy tego, że ZZL zdaje się być utożsamiane z przywództwem oraz kierowaniem ludźmi, co jest niewłaściwe. Z kolei profesjonalizm jest opisany jako kompetencja charakteryzująca duże umiejętności oraz wysoki poziom w procesie zarządzania zasobami informacji. Pierwsza wątpliwość dotyczy tego, czy ta kompetencja charakteryzuje umiejętności czy też tą kompetencją są umiejętności? Druga wątpliwość związana jest z tym, że w jej opisie podany już został

jej poziom, który ma być wysoki. Otóż, w ogólnych opisach kompetencji nie podaje się poziomu. Poziom jest skalowany dopiero wtedy, gdy kompetencja podlega ocenianiu ze względu na wymagania stanowiskowe, wyniki pracy czy osiągnięcia pracownika, tworzone plany szkoleniowe czy rozwojowe itp. Oznacza to-mówiąc w uproszczeniu - że na różnych stanowiskach wymagania co do poziomu poszczególnych kompetencji nie muszą być takie same i zwykle też nie są. Formułowane przeze mnie tutaj uwagi nie oznaczają, że autorska koncepcja zbioru tych kompetencji jest bezwartościowa. Wręcz przeciwnie, mimo tego, że pojawiają się pewne błędy merytoryczne, uważam, że sam pomysł na ich wyodrębnienie ze względu na bezpieczeństwo informacyjne jest w pełni uzasadniony i niezwykle przydatny z praktycznego punktu widzenia.

Poza omawianymi kompetencjami ważnym zagadnieniem podejmowanym w tym podrozdziale ze względu na jego tytuł są też sposoby ograniczania negatywnego wpływu czynnika ludzkiego na bezpieczeństwo informacji. Autor w swojej dyskusji odwołuje się do trzech etapów relacji pracownika z organizacją, które są szeroko uznawane w literaturze przedmiotu z obszaru ZZL, chociaż bywają różnie określane. Wspomniane etapy dotyczą następujących okresów: 1) kiedy pracownik przechodzi przez proces doboru, na który składają się rekrutacja, selekcja i wprowadzenie do pracy (tutaj niewłaściwe Habilitant posługuje się tylko pojęciem rekrutacji), 2) kiedy jest zatrudniony i 3) kiedy odchodzi z organizacji (s. 223). W ramach każdego z tych etapów podawane są przykłady różnych subfunkcji ZZL, które mogą zostać wykorzystane w praktyce organizacyjnej w celu takiego kształtowania kompetencji pracowniczych, który umożliwi ograniczenie negatywnego wpływu czynnika ludzkiego na bezpieczeństwo informacji. Istotnym walorem proponowanych rozwiązań jest to, że poszczególne subfunkcje ZZL są nie tylko rozpatrywane osobno, ale też w ramach wzajemnych powiązań, które można wykorzystać, aby zwiększyć możliwości pozytywnego odziaływania na kompetencje pracownicze.

W mojej opinii rozdział zasługuje na pozytywną ocenę. Warto nadmienić, że stanowią o tym nie tylko autorskie rozwiązania koncepcyjne Habilitanta, ale też dobrze dobrane, liczne przykłady wyników badań innych autorów, które doskonale ilustrują omawiane problemy, pozwalają formułować uzasadnione tezy oraz dowodzą szerokiej wiedzy Habilitanta na temat wpływu czynnika ludzkiego na bezpieczeństwo informacji oraz konieczności jego uwzględnienia w zarządzaniu bezpieczeństwem informacji.

Rozdział 4. ma charakter empiryczny i przedstawione są w nim wyniki własnych badań dra inż. Pawła Kobisa. Na rozdział składa się osiem podrozdziałów, w których opisana jest metodyka badań, próba badawcza, uzyskane wyniki badań empirycznych oraz sformułowane są wnioski końcowe z badań. Na początku sformułowanych zostaje sześć celów badawczych i dwa cele aplikacyjne. **Cele badawcze** są następujące (s. 231-232):

1) Rozpoznanie rodzajów usług i aplikacji informatycznych używanych w przedsiębiorstwach służących do zarządzania zasobami informacyjnymi w aspekcie bezpieczeństwa informacji.
2) Rozpoznanie modelu informatycznego funkcjonującego w przedsiębiorstwie, a przez to określenie poziomu wpływu czynnika ludzkiego na bezpieczeństwo informacji.
3) Rozpoznanie istniejącego poziomu wiedzy tematycznej i świadomości osób odpowiedzialnych za bezpieczeństwo zasobów informacyjnych w badanych przedsiębiorstwach w zakresie ochrony zasobów niematerialnych.

4) Określenie poziomu wiedzy na temat wybranych aspektów znaczenia czynnika ludzkiego w bezpieczeństwie informacji wśród osób odpowiedzialnych za ochronę zasobów informacyjnych.
5) Rozpoznanie stopnia wpływu najważniejszych czynników ludzkich budzących sytuacje zagrożenia informacji na bezpieczeństwo zasobów niematerialnych.
6) Rozpoznanie poziomu świadomości osób odpowiedzialnych za bezpieczeństwo informacji w przedsiębiorstwach na temat potrzeb poszerzania wiedzy w kwestii ochrony własności intelektualnej wśród pracowników organizacji.

Natomiast **cele aplikacyjne** przybrały następująca postać (232):

1) Opracowanie koncepcji podsystemu zarządzania bezpieczeństwem informacji z uwzględnieniem czynnika ludzkiego w przedsiębiorstwach sektora małych i średnich przedsiębiorstw.
2) Dokonanie oceny proponowanego podejścia systemowego.

W mojej ocenie przyjęty podział celów jest zbyt ogólny i nie do końca właściwy, albowiem cele generatywne (teoriotwórcze) mieszają się z aplikacyjnymi i utylitarnymi, co jest widoczne w celach, które Autor nazwał aplikacyjnymi. Podobnie, jak cele eksploracyjne, deskryptywne, diagnostyczne i eksplanacyjne występują w dosyć dziwnych konfiguracjach pod hasłem celów badawczych. Ponadto w piątym celu badawczym czynnik ludzki jest w liczbie mnogiej i nie jest to spójne z tym, co zdawało się, że Autor przyjął w części teoretycznej pracy. Być może wynika z tego, że czynnik ludzki został utożsamiony z zasobami ludzkimi, które z kolei Habilitant utożsamia z pracownikami, na co wcześniej już zwracałam uwagę.

W dalszej części podana jest następująca **hipoteza badawcza:** W przedsiębiorstwach małych i średnich nie zarządza się bezpieczeństwem informacji w sposób kompletny (holistyczny), marginalizując aspekty pozatechniczne ochrony informacji, w tym wpływ czynnika ludzkiego, co prowadzi do zwiększenia ryzyka zagrożenia zasobów niematerialnych przedsiębiorstw. Wzbudza ona wątpliwości, gdyż w świetle ustaleń dokonanych w części teoretycznej pracy nie jest ona hipotezą a tezą, która z naukowego punktu widzenia powstaje ze względu na przyjęcie określonych przesłanek, zdań uznanych za prawdziwe i wynikających z dokonanego przeglądu literatury. A to właśnie z części teoretycznej pracy dowiadujemy się, że jedną z przyczyn podjęcia określonej problematyki w monografii był brak kompleksowych rozwiązań w zakresie zarządzania bezpieczeństwem informacji ze szczególnym uwzględnieniem roli czynnika ludzkiego (patrz *Wstęp),* który autor potwierdza przywołując liczne badania innych autorów. W mojej ocenie tak sformułowana hipoteza pomniejsza znaczenie ustaleń dokonanych przez Habilitanta w wyniku przeprowadzonych badań empirycznych. Jednocześnie sugeruje, że pojawiają się jakieś trudności z poprawnym sformułowaniem hipotezy o rzeczywistej wartości naukowej.

W badaniach empirycznych zastosowano metodę CAWI oraz CAPI, przy czym w przypadku tej drugiej wykorzystano ją zarówno w wywiadach bezpośrednich jak i za pomocą komunikatorów z funkcją audiowizualną. Ankieta badawcza jest dołączona do pracy w postaci załącznika. Mimo tego, że Autor pisze, iż w czasie wywiadów starano się rozwiać wszelkie wątpliwości respondentów co do zadawanych pytań, to chciałam zwrócić uwagę na dwie rzeczy. Po pierwsze, w załączonej ankiecie nie zawsze podano, ile odpowiedzi może wybrać respondent. Po drugie, pytanie 12 wzbudza wątpliwości, gdyż chodzi w nim o największe inwestycje w różne obszary bezpieczeństwa organizacji, przy czym inwestycje rozumiane są jako środki pieniężne i jako zaangażowanie specjalistów. Rzecz w tym, że z jednej strony respondent może mieć problem z udzieleniem odpowiedzi, gdy jeden i drugi

element pytania ocenia inaczej, a z drugiej strony badacz napotyka trudności z właściwą interpretacją uzyskanych odpowiedzi. Nie wiadomo bowiem, czy wybory odpowiedzi dokonywane przez respondentów były podyktowane jednakową oceną jednego i drugiego elementu pytania, czy też
0 wyborze decydował tylko jeden nich. Z pewnością jednak, w kontekście bezpieczeństwa informacji
1 angażowanych zasobów, nie można uznać, że to wszystko jedno.

Badania zostały przeprowadzone w dwóch etapach. Pierwszy miał miejsce od 11. 2018 roku do 09.2019 roku w małych i średnich przedsiębiorstwach w Polsce. Drugi, mający na celu ocenę opracowanego systemu, przeprowadzono w okresie 01.-02.2020 roku. W badaniu uczestniczyło 367 podmiotów gospodarczych - małych i średnich przedsiębiorstw. Autor szczegółowo podaje, w jaki sposób obliczono liczbę przedsiębiorstw, która powinna uczestniczyć w badaniu oraz w jaki sposób dokonano wyboru kwotowego i jakimi kierowano się kryteriami. Należy tutaj wysoko ocenić skrupulatność i rzetelność podjętych w tym zakresie działań. Podobnie, bardzo dokładnie zostaje opisany dobór konkretnych respondentów z organizacji oraz struktura próby badawczej. Podano też, jakiego rodzaju testy statystyczne wykorzystano do analizy zgromadzonych danych empirycznych (chi-kwadrat, Z, Fischera, U Manna Whitneya). Nie są to jednak wyszukane metody analityczne.

Rozdział został tak ustrukturyzowany, że w kolejnych podrozdziałach prezentowane są wyniki badań odnoszące się do każdego pytania badawczego. Dane prezentowane są jako liczność i częstość wyrażona w procentach w postaci tabelarycznej lub wykresu. W pierwszej kolejności poznajemy wyniki dotyczące usług i aplikacji informatycznych wspomagających zarządzanie zasobami informacyjnymi w przedsiębiorstwach. Autor komentuje je ze względu na charakter wykorzystywanych aplikacji i programów oraz związane nimi zagrożenia od strony użytkowania. Następnie przedstawiane są dane empiryczne z obszaru modeli wykorzystywania zasobów informatycznych. Mowa jest o modelu tradycyjnym oraz usługowym *(cloud computing).* Dane są analizowane ze względu na wielkość przedsiębiorstwa, zasięg jego działalności oraz rodzaj prowadzonej działalności. W swoich komentarzach Habilitant zwraca uwagę na rodzaje zagrożeń związanych ze stosowanym w organizacji modelem wykorzystania zasobów IT. Zgodnie z założeniami przyjętymi przez Autora zgromadzone dane w omawianym zakresie miały umożliwić osiągnięcie drugiego celu badawczego. Należy stwierdzić, że o ile udało się zidentyfikować modele informatyczne stosowane w przedsiębiorstwach, to nie znajdujemy w tej części pracy żadnej informacji na temat tego, jaki jest poziom wpływu czynnika ludzkiego na bezpieczeństwo informacji. Zatem drugi człon wspomnianego celu pozostaje bez odpowiedzi.

W dalszej kolejność omawiane są wyniki badania dotyczące obecnego poziomu wiedzy i świadomości osób odpowiedzialnych za bezpieczeństwo zasobów informacyjnych. Omawiane są różnice między małymi i średnimi przedsiębiorstwami. W analizie uwzględnia się też grupę, do której należał respondent. Szczegółowa analiza problemowa danych dotyczy realnego ryzyka kradzieży lub zniszczenia informacji, rodzaju zagrożeń dla informacji, znaczenia wartości informacji i jej bezpieczeństwa, obszarów bezpieczeństwa, w które dokonywane są inwestycje finansowe i związane z zaangażowaniem specjalistów, oraz działań podejmowanych w ciągu ostatnich 3 lat w celu zwiększenia bezpieczeństwa informacji. W tym miejscu należy zwrócić uwagę, że o ile zaprezentowane w tabeli 4.12. zestawienie odpowiedzi respondentów w zakresie dwóch zagadnień, tj. oceny stopnia znaczenia informacji i jej bezpieczeństwa z faktycznie podejmowanymi działaniami minimalizującymi ryzyko wystąpienia zagrożeń jest poznawczo interesujące, a eksplanacyjnie bardzo inspirujące, czego dowodzą też komentarze samego Autora, to tytuł tej tabeli jest niepoprawny.

Otóż, mowa jest w nim o zależnościach między wspomnianymi zagadnieniami, a tymczasem w sensie analizy statystycznej nie są tam prezentowane żadne zależności (czy choćby korelacje), a jedynie rozkład dwóch badanych zmiennych pogrupowany wg skal zastosowanych w kwestionariuszu ankiety.

Następnie Autor przechodzi do zaprezentowania wyników badania, które mają związek z trzecim celem badawczym, tj. poziomem wiedzy na temat wybranych aspektów znaczenia czynnika ludzkiego w bezpieczeństwie informacji wśród osób odpowiedzialnych za ochronę zasobów informacyjnych. Analizie poddano takie zagadnienia, jak poziom zabezpieczeń informatycznych, źródła zagrożeń dla systemu informatycznego, dostęp z firmowych urządzeń do sieci społecznościowych, czatów, itp., zbiór zasad korzystania z Internetu, kontrola nad przenośnymi magazynami danych, wykorzystywanie i monitorowanie prywatnych urządzeń w sieci przedsiębiorstwa, miejsca obsługi osób spoza organizacji, uprawnienia dostępowe do zasobów informacyjnych oraz techniki monitoringu. W omawianiu uzyskanych danych Autor nie tylko podejmuje się ich interpretacji, co jest oczywiście konieczne, ale niepotrzebnie robi też odwołania do literatury przedmiotu, które niekiedy przyjmuję formę uzasadnienia dla badanych zagadnień. Tego rodzaju odniesienia powinny mieć miejsce w części teoretycznej, a nie empirycznej pracy. Przy okazji krytycznie też oceniam zamieszczanie w tytułach tabel pytań ankietowych, które się tutaj pojawiają. Tytuły powinny mieć charakter problemowy.

W dalszej kolejności, odnosząc się do piątego celu badań, Autor przechodzi do wpływu najważniejszych czynników ludzkich na bezpieczeństwo zasobów informacyjnych. Jak już wcześniej wspomniałam, razi zastosowanie liczby mnogiej w czynniku ludzkim. Stoi to nie tylko w pewnej logicznej sprzeczności z przyjętą przez Habilitanta definicją, ale też tytułem monografii. W każdym razie rozpatrywanych jest tutaj 8 czynników, tj., jednostajność wykonywanych obowiązków, pośpiech i zmęczenie, przesadne zaufanie w stosunku do osób trzecich, nadmierne gadulstwo, podatność na działania socjotechniczne, niezadowolenie z szeroko rozumianych warunków pracy, celowe działania wspierane przez konkurencję (szpiegostwo gospodarcze), oraz brak dostatecznej wiedzy w zakresie zasad ochrony informacji. W badaniu respondenci zostali poproszeni o dokonanie ich oceny na 5-stopniwej skali Likerta ze względu na tworzenie sytuacji sprzyjających wyciekowi iub utracie informacji w przedsiębiorstwie. Przy okazji zwrócę uwagę, że pytanie ankietowe dotyczące tego zagadnienia zostało niepoprawnie zbudowane pod względem merytorycznym i językowym. Inne zastrzeżenie dotyczy wyróżnienia dwóch czynników, tj. przesadnego zaufania do osób trzecich oraz podatności na działania socjotechniczne. Wątpliwość dotyczy ich zakresu merytorycznego. Oto, bowiem, komentując wyniki badania uzyskane w zakresie przesadnego zaufania Autor pisze, że czynnik ten odnosi się do wszelkiego rodzaju działań socjotechnicznych, a jako przykład podaje podszywanie się pod znane organizacje i ich przedstawicieli (s. 289). Jednocześnie komentując wyniki dotyczące podatności na działania socjotechniczne podaje m.in.' przykłady podszywania się pod znane marki czy kontrahentów. Powstaje zatem pytanie, czy te czynniki mają rzeczywiście charakter rozłączony skoro pierwszy z wymienionych zdaje się wchodzić w skład drugiego? Czy jest to jedynie kwestią nieprecyzyjnego ich opisania? Pewne niejasności dotyczącą też czynnika o nazwie gadulstwo. Nazwa jest kolokwialna, mało precyzja i może być myląca.

Chociaż wyniki badań w zakresie piątego celu badawczego są bardzo ciekawe i omawiane w stosunkowo merytoryczny i zręczny sposób, to krytycznie należy ocenić to, że omawiane czynniki nie zostały w części teoretycznej pracy precyzyjnie zdefiniowane przez Autora dla celów badawczych

i zgodnie z przyjętymi w tym zakresie zasadami naukowymi, chociaż były tam omawiane. Dodatkowo mylący jest tytuł podrozdziału 4.6., w którym prezentowane są te wyniki badań. Jest w nim bowiem mowa o wpływie czynników ludzkich na bezpieczeństwo zasobów informacyjnych. Jednakże po jego lekturze należy stwierdzić, że ani nie zbadano ani też nie analizowano takiego wpływu. Prezentowane są jedynie opinie respondentów na temat intensywności, z jaką wybrane bodźce mogą generować sytuacje sprzyjające wyciekowi lub utracie informacji w przedsiębiorstwie. Nadmienię jeszcze, że do ustalenia wpływu jednej zmiennej na inną stosuje się odpowiednie metody analizy statystycznej, co nie miało tutaj miejsca. W rezultacie należy uznać, że nie osiągnięto celu piątego pytania badawczego, w którym - przypomnę - chodziło nawet nie tyle o zidentyfikowanie samego wpływu czynnika ludzkiego, ale o stopnień tego wpływu.

Przechodząc do szóstego celu badawczego Autor skupia się na poziomie świadomości osób odpowiedzialnych za bezpieczeństwo informacji na temat potrzeb poszerzania wiedzy pracowników w zakresie tego bezpieczeństwa. Temu poświęcony jest podrozdział 4.7., którego tytuł jest zbieżny z tym celem. Jednakże pierwsze zdanie tej części pracy wzbudza zdziwienie. Autor pisze, że - cytuję - realizując szósty cel badawczy, podjęto próbę określenia poziomu realizacji szkoleń w przedsiębiorstwach jako kluczowego sposobu poszerzania wiedzy w zakresie bezpieczeństwa informacji. Wskazuje jednocześnie, że dane w tym zakresie były zbierane w pytaniach ankietowych o numerach 6, 7 i 8 (s. 302). Wspomniane zdziwienie wynika z tego, że po pierwsze, poziom realizacji szkoleń ani nie stanowił szóstego celu badawczego ani też nie był przedmiotem badania we wspomnianych pytaniach, gdyż dotyczą one następujących zagadnień: do kogo powinny być skierowane ogólne szkolenia w zakresie bezpieczeństwa informacji w przedsiębiorstwie, czy respondent odczuwa potrzebę organizowania cyklicznych zewnętrznych lub wewnętrznych szkoleń w tym zakresie i jak często powinny być organizowane takie szkolenia. W treści samego podrozdziału znajdujemy odniesienia właśnie do tych zagadnień, a nie do innych. Prowadzi to do kolejnego spostrzeżenia, a mianowicie, że przedmiotem badania nie był też - mimo zapowiedzi - poziom świadomości osób odpowiedzialnych za bezpieczeństwo informacji na temat potrzeb szkoleniowych pracowników w zakresie tego bezpieczeństwa.

Pytanie dotyczące odbiorcy ogólnych szkoleń i wybór odpowiedzi zostały tak sformułowane, iż można je zinterpretować jako pytanie o to, czy obecnie należy do kogoś takie szkolenie skierować. Respondent odnosząc się do praktyki własnej organizacji, w której na przykład takie szkolenia właśnie zakończono, może mieć problem z wyborem odpowiedzi. Problematyczne wydaje się też zaznaczenie odpowiedzi w sytuacji, kiedy mowa jest o ogólnych szkoleniach, a w wyborze odpowiedzi są osoby, które zajmują się w organizacji bezpieczeństwem systemów czy też pracują w działach IT. Do takiej grupy kieruje się nie ogólne szkolenia, ale bardziej specjalistyczne.

Pytanie o potrzebę organizacji cyklicznych szkoleń w zakresie bezpieczeństwa jest nieprecyzyjne, bo nie wiadomo, czy to ma być szkolenie dla respondenta czy dla pracowników przedsiębiorstwa. Dylemat wynika z tego, że respondentami nie były przecież ani osoby na szeregowych stanowiskach ani osoby spoza szeroko rozumianego IT. W tym kontekście kolejne pytanie o częstotliwość takich szkoleń również nie wyjaśnia, dla kogo takie szkolenia miałyby być. Oznacza to, że wnioski formułowane na podstawie tak zebranych danych mogą być wadliwe. Mamy zatem do czynienia z sytuacją, w której narzędzie badawcze w pewnej części nie odpowiada założonemu celowi badawczemu ze względu na to, iż zgromadzone za jego pomocą dane nie są relewantne.

Ostania część tego rozdziału to wnioski z badań. Habilitant formułuje tutaj dwa wnioski główne i szereg wniosków szczegółowych. Wnioski główne logicznie wynikają z przeprowadzonych badań empirycznych i toczonych względem nich dyskusji. W sensie merytorycznym i logicznego wnioskowania są uprawnione. Jeżeli chodzi o wnioski szczegółowe to niektóre z nich idą za daleko, co ma związek z zastrzeżeniami, które zgłaszałam recenzując ten rozdział. Mieszane odczucia pojawiają się odnośnie do hipotezy, którą Autor uznaje tutaj za zweryfikowaną pozytywnie. Nie miała ona żadnego charakteru odkrywczego, a co więcej, dotyczyła zjawisk, które zostały już zbadane przez innych badaczy. Sam autor zauważa, że przedstawione wyniki badań potwierdziły większość rozważań teoretycznych prowadzonych w poprzednich rozdziałach nie tylko odnośnie do marginalizowania czynnika ludzkiego w bezpieczeństwie zasobów niematerialnych, ale też innych zagadnień badanych w Polsce i na świecie (s. 312). To w zasadzie potwierdza zasadność zgłaszanej przeze mnie wcześniej uwagi dotyczącej tego, że mamy tutaj raczej do czynienia z tezą niż hipotezą.

W ogólnym rozrachunku uważam jednak, że przeprowadzone badania mają znaczący walor poznawczy, umożliwiający eksploracje badanego fragmentu rzeczywistości organizacyjnej i dający podstawy do wskazania konkretnych zaleceń o charakterze praktycznym, co Autor czyni w tej części pracy. W mojej ocenie proponowane rekomendacje są nie tylko na wysokim poziomie merytorycznym, ale też cechują się wysokim poziomem użyteczności. Z perspektywy zarządczej dają szeroką paletę różnych rozwiązań w zakresie zwiększania bezpieczeństwa informacji w przedsiębiorstwie. Obejmują zarówno kwestie organizacyjne, techniczne, jak i odnoszące się do roli czynnika ludzkiego.

Na szczególne podkreślenie zasługuje niezwykła dbałość Habilitanta o zachowanie logicznych powiązań pomiędzy poszczególnymi częściami pracy, czy też konkretnymi problemami poruszanymi w różnych jej miejscach. Jest to dokonywane poprzez odwoływanie się do konkretnych numerów podrozdziałów, tabel czy rysunków zarówno tych, które znajdowały się w poprzednich częściach pracy, jak i tych, które dopiero się pojawią. Skrupulatność w zachowaniu logicznej ciągłości jest też widoczna w samej strukturze tego rozdziału. Podrozdziały oraz wnioski końcowe uporządkowano według kolejności postawionych celów badawczych.

Rozdział 5. jest ostatnim. Habilitant prezentuje w nim autorską koncepcję *Podsystemu zarządzania pozatechnicznymi aspektami bezpieczeństwa informacji* (Podsystem ZPABI). Rozdział składa się z sześciu podrozdziałów, w których dokonywana jest charakterystyka tego systemu, w tym w ujęciu funkcjonalnym i przedmiotowym, opisana jest jego struktura oraz umiejscowienie w innym systemie przedsiębiorstwa oraz proces implementacji i funkcjonowania, jak również proponowany jest autorski model oceny dojrzałości bezpieczeństwa informacji ze względu na Podsystem ZPABI oraz dokonywana jest ocena zaproponowanego systemu.

System ma w swoich założeniach stanowić dodatkowy element *Systemu zarządzania bezpieczeństwem informacji* (SZBI), a jego celem jest minimalizacja wpływu czynnika ludzkiego na powstawanie zagrożeń dla zasobów niematerialnych organizacji gospodarczej (s. 313 i s. 317). Obejmuje on takie obszary jak polityka bezpieczeństwa informacji, zarządzanie ryzykiem, uświadamianie i podnoszenie poziomu wiedzy pracowników oraz monitoring związanych z zarządzaniem informacją. W tym kontekście nieco razi posługiwaniem się przez Habilitanta takimi określeniami, jak „zarządzanie polityką" czy „podnoszenie wiedzy" (s. 315). Pierwsze wzbudza zastrzeżenia merytoryczne z perspektywy nauk o zarządzaniu i jakości, a drugie jest niepoprawne ze względów logicznych i językowych.

W opisie modelu zwraca uwagę to, że Autor sprawnie przywołuje ustalenia czy też propozycje szczegółowych rozwiązań koncepcyjnych prezentowanych we wcześniejszych częściach pracy. Dodatkowo na podkreślenie zasługują samodzielne opracowania tabelaryczne dotyczące: działań minimalizujących zagrożenie informacji z perspektywy zarządzania zasobami ludzkimi (tab. 5.1., s. 321) i podmiotów wchodzących w relacje z organizacją (tab. 5.2., s. 323) oraz materialnych i niematerialnych składników systemu (tab. 5.3., s. 324). Istotne znaczenie ma też syntetycznie dokonane zestawienie konsekwencji utraty lub zniszczenia informacji dla przedsiębiorstwa z perspektywy zarządzania (s. 336-338).

Jeżeli chodzi o elementy komponujące autorski podsystem ZPABI oraz relacje między nimi to zostały one graficznie zaprezentowane na rys. 5.3. (s. 343), który Autor omawia w bardzo precyzyjny i przystępny sposób. Rozwinięciem prezentowanej koncepcji są zależności między elementami Podsystemu ZPABI a osobami mającymi wpływ na bezpieczeństwo systemu informacyjnego w przedsiębiorstwie, które graficznie zaprezentowano na rys. 5.4 (s. 344). Towarzyszy temu szczegółowy opis tych relacji oraz procesu implementacji systemu w organizacji. Należy zauważyć, że w zamyśle Autora proponowany system ma stanowić kompleksowe ujęcie zabezpieczeń przed wszystkimi rodzajami zagrożeń mających swój początek w zachowaniu człowieka (s. 238), przy czym ma on charakter otwarty, tzn., stwarza możliwość dołączania kolejnych elementów zgodnie z potrzebami organizacji oraz pojawiającymi się nowymi rozwiązaniami w zakresie zabezpieczania informacji. Całościowe ujęcie systemu, uwzględniające płaszczyznę przedmiotową i podmiotową zamieszczono na rys. 5.5. (s. 349). Habilitant zaznacza przy tym, że tylko strukturalne współistnienie tych dwóch płaszczyzn, które łączą ze sobą działania człowieka, składniki materialne i niematerialne przeciwdziałające utracie lub zniszczeniu informacji umożliwia uzyskanie kompleksowego rozwiązania minimalizującego ryzyko zagrożenia dla zasobów niematerialnych. Ważne jest też właściwa współpraca tego systemu z istniejącym systemem zabezpieczeń w organizacji (s. 349).

Na tym tle zgłaszana jest potrzeba opracowania skutecznego modelu dojrzałości modelu bezpieczeństwa informacji, który miałby za zadanie oszacować skuteczność zaimplementowanych rozwiązań w zakresie ochrony informacji na każdym etapie jego funkcjonowania. Stąd też Autor wychodzi z kolejną, własną propozycją w tym zakresie, w której wykorzystane są pewne założenia modelu CMMI (s. 350-353). W ramach tej koncepcji zaproponowano pięć poziomów modelu dojrzałości (scharakteryzowanych w tab. 5.4.S. 352) oraz skalę 5-stopniwą skalę oceny (s. 351).

W ostatniej części rozdziału prezentowane są wyniki oceny Podsystemu ZPABI. Ocena została dokonana za pomocą ankiety elektronicznej skierowanej do 24 respondentów odpowiedzialnych za bezpieczeństwo zasobów informacyjnych wśród przedsiębiorstw, które brały udział w badaniu opisywanym w rozdziale 4. Ankietowani oceniali system nie z perspektywy własnych doświadczeń jako użytkownika, a na podstawie informacji pozyskanej na temat tego systemu w czasie szkolenia zorganizowanego przez Habilitanta. Generalnie ocena wypadła pozytywnie.

Na zakończenie mojej opinii na temat tego rozdziału muszę zwrócić uwagę na dwie rzeczy. Po pierwsze, jego tytuł nie jest w pełni poprawny. Jest w nim mowa o umiejscowieniu proponowanego systemu w przedsiębiorstwie, a przecież nie chodzi o przedsiębiorstwo jako takie, a o wbudowanie proponowanego systemu w istniejący system zabezpieczeń w organizacji. Po drugie, w nazwie systemu wykorzystano pojęcie aspekt. Nie jest to trafne, gdyż w wyjaśnieniach słownikowych - tak najkrócej mówiąc - aspekt to wzgląd, spojrzenie czy punkt widzenia. W tym kontekście trudno mówić na przykład o zarządzaniu pozatechnicznym punktem widzenia

bezpieczeństwa informacji, bo to w ogóle zmienia sens rozwiązań koncepcyjnych Autora. Co prawda, autor zdaje się przyjmować, że aspekt to czynności, procesy i decyzje (s. 315), ale i tak uważam, że należało poszukać lepszego określenia, adekwatnego do terminologii stosowanej w naukach
0 zarządzaniu i jakości.

W swojej ogólnej ocenie uważam, że zarówno autorskie koncepcje prezentowane w tym rozdziale jak i sam rozdział zostały starannie przemyślane i logicznie ustrukturowane. Toczone wywody są racjonalne, a formułowane wnioski i rekomendacje rzeczowo argumentowane, zarówno z naukowego i praktyczne punktu widzenia. Tym samym Autorowi udało się zrealizować cele aplikacyjne pracy, chociaż nie ukrywam, że Kiedy Habilitant mówił w drugim celu o ocenie systemu, to sądziłam, że będzie chodziło o jego ocenę po dokonanym wdrożeniu.

Ostatnia wyodrębniona część monografii to *Zakończenie.* Zamieszczono w nim najważniejsze konkluzje z przeprowadzonych rozważań teoretycznych i badań empirycznych. Autor odwołuje się też **do celu monografii,** którym było zidentyfikowanie współczesnego środowiska bezpieczeństwa informacji zarówno w kształcie organizacyjnym, jak i technicznym. W tym miejscu zgłaszam dwie uwagi. Po pierwsze, ten cel nie został podany we *Wstępie* do pracy. Po drugie, gdyby taki był faktyczny cel monografii, to nie miałaby ona zbytniej wartości naukowej. Uważam, że Autor pomniejszył tutaj znaczenie wykonanej przez siebie pracy. Monografia realizuje też cele wyższego rzędu naukowego, o bardziej ambitnym charakterze, a zatem dokonane w niej ustalenia nie ograniczają się tylko do identyfikacji wspomnianego środowiska. Krótko mówiąc, bo rolą recenzenta nie jest też formułowanie celów za Habilitanta, mamy tutaj: identyfikację, analizę, diagnozę
1 rekomendacje.

Moja końcowa opinia na temat recenzowanej monografii jest następująca. Praca została właściwe zaklasyfikowana do dziedziny nauk społecznych w dyscyplinie nauk o zarządzaniu i jakości zarówno ze względu na przedmiot jej zainteresowania jak i specyficzny język stosowany w tej dyscyplinie. Jest to spójne i logicznie ustrukturyzowane dzieło, chociaż o przeciętnym poziomie naukowości. Zostało opracowane w oparciu o bogaty i różnorodny przegląd literatury. Jej szczególnym walorem jest to, że w wielu aspektach uwidacznia się jej interdyscyplinarny charakter, chociaż pewien niedosyt budzą nieco słabsze studia literaturowe z obszaru zarządzania zasobami ludzkimi w porównaniu do innych obszarów problemowych podejmowanych w pracy, a trzeba mieć na względzie, że już w tytule pracy wyróżniony został czynnik ludzki. W monografii zaprezentowano wyniki bardzo wnikliwych studiów literaturowych oraz badań empirycznych o charakterze deskryptywnym. Wniesiono też liczne propozycje własnych rozwiązań koncepcyjnych. Podjęta problematyka jest aktualna i ważna. Habilitant poprzez przyjętą strukturę pracy konsekwentnie dążył do realizacji założonego w niej celu i w rezultacie ten cel udało mu się osiągnąć. Uznaję jednak tutaj, że jednym z zasadniczych celów było zaproponowanie autorskiej koncepcji Podsystemu ZPABI, chociaż Autor-jak już wspominałam-nieco inaczej podszedł do formułowania celów. Praca posiada wiele elementów o nowatorskim charakterze. Wiele problemów rozwiązywanych jest w sposób twórczy, co szczegółowo akcentowano recenzując każdy rozdział. Z pewnością jednak za szczególne osiągnięcie Habilitanta należy uznać wspomniany autorski *Model* Podsystemu ZPABI, który w powiązaniu z pozostałymi rozwiązaniami, jak choćby modelem dojrzałości bezpieczeństwa informacji, stanowi oryginalne rozwiązanie koncepcyjne. Charakteryzuje je wysokim poziom oryginalności i użyteczności. W mojej ocenie Habilitant wykazał się dobrymi kompetencjami teoriotwórczymi w zakresie konceptualizacji podejmowanej problematyki i odpowiednimi

kompetencjami metodycznymi w zakresie badań empirycznych, które maja służyć wypracowaniu rozwiązań aplikacyjnych.

Zatem stosując wprost kryterium ustawowe stwierdzam, że monografia naukowa zt. *Zarządzanie bezpieczeństwem informacji w systemach informacyjnych małych i średnich przedsiębiorstw z uwzględnieniem czynnika ludzkiego* wskazana przez Dr inż. Paweła Kobisa jako jego główne osiągnięcie naukowe wnosi znaczny wkład w rozwój dyscypliny naukowej nauk i zarządzaniu i jakości.

3. OCENA INNYCH OSIĄGNIĘĆ NAUKOWO-BADAWCZYCH

Po uzyskaniu stopnia doktora zainteresowania Habilitanta były ukierunkowane na cztery główne obszary naukowo-badawcze, tj.:

1) zarządzanie informacją - w którym szczególnym przedmiotem zainteresowania były wymiana i przetwarzanie informacji między pracownikami z wykorzystaniem chmury obliczeniowej w przetwarzaniu zasobów niematerialnych, zarządzanie bezpieczeństwem, efektywność wdrożeń cloud comouting, ekonomiczne aspekty implementacji CC w podmiotach gospodarczych, zarządzanie procesami biznesowymi i użyciem technik i technologii informatycznych, outsourcing usług informatycznych,
2) praca grupowa - na który składała się problematyka związana z modelowaniem funkcjonowania systemów pracy grupowej w organizacjach gospodarczych, tworzeniem efektywnych zespołów, konfliktami i podejmowaniem decyzji w zespołach, preferowane tryby pracy, rolą lidera w zespole zadaniowym, wirtualizacja spotkań grup roboczych,
3) kapitał ludzki - który dotyczył problematyki zdolności umysłowych i postaw pracowników, ich cech psychologicznych i kompetencji, samooceny preferowanego trybu pracy, wpływu czynnika ludzkiego na zarządzanie bezpieczeństwem informacji, pracy mobilnej pracowników, świadomości menedżerów oraz pracowników z obszaru IT na temat możliwości wykorzystania CC, ochrony danych i informacji, konieczności organizowania odpowiednich szkoleń w tym zakresie dla pracowników przedsiębiorstw, socjotechniki i inżyniera społeczna,
4) techniki multimedialne - który komponowały takie zagadnienia, jak implementacja określonych rozwiązań multimedialnych w środowisku systemów operacyjnych,

Szczegółowa charakterystyka tych obszarów oraz powiązań między nimi zostały opisane przez Habilitanta w *Autoreferacie.* Do każdego z obszarów przypisano też odpowiednie publikacje oraz projekty badawcze. Prace były publikowane w języku polskim i angielskim zarówno w czasopismach jak i wydawnictwach o uznanej renomie, ale są też takie, które ostatnio wzbudzają pewne kontrowersje w świecie nauki, a mam tutaj na myśli - IBIMA.

Dr inż. Paweł Kobis wskazuje w *Autoreferacie* 10 najbardziej znaczących, jego zdaniem, publikacji z zakresu zarządzania bezpieczeństwem zasobów informacyjnych (s. 66-67). Ich kopie są dołączone do dokumentacji. Są to:

- jeden rozdział w monografii w j. angielskim, wydany przez wydawcę zagranicznego spoza listy MEiN,
- trzy artykuły w j. angielskim w zagranicznych materiałach pokonferencyjnych spoza listy MEiN,
- jeden artykuł w j. angielskim w zagranicznych materiałach konferencyjnych z listy MEiN (70 pkt), wydany przez IBIMA,
- jeden artykuł w j. angielskim w czasopiśmie zagranicznym spoza listy MEiN,

■ cztery artykuły w czasopismach polskich - w tym jeden wydany po polsku w czasopiśmie spoza listy MEiN, a trzy w czasopismach z listy MEiN, w tym jeden po polsku (40 pkt) i dwa po angielsku (40 pkt i 70 pkt).

Po zapoznaniu się ze wskazanymi przez Habilitanta publikacjami stwierdzam, że są to prace 0 przeciętnej jakości naukowo-badawczej, a niekiedy nawet nieco słabszej. Większość z nich ma charakter empiryczny, przy czym dotyczą one jedynie opisu badanego fragmentu praktyk organizacji lub też pozyskania opinii respondentów na jakiś temat, a nie zidentyfikowania jakiś prawidłowości czy odkrycia nowych zjawisk. Pozostałe prace mają charakter przeglądowy lub wnoszą własne propozycje Autora co do rozwiązywania problemów o charakterze praktycznym. Niektóre z podejmowanych zagadnień prezentowane są też w monografii zgłoszonej przez Habilitanta jako główne osiągnięcie naukowe.

Sumarycznie, Dr inż. Paweł Kobis opublikował łącznie 66 prac po uzyskaniu stopnia doktora, na które składają się: 1 samodzielna monografia, 35 rozdziałów w monografiach (w tym 10 w j. angielskim), 1 fragment w monografii, 7 współredakcji naukowych monografii, 17 artykułów w czasopismach naukowych (w tym 7 w j. angielskim), 2 fragmenty w książkach i 3 referaty (w tym dwa w j. angielskim). Opracowania monograficzne były publikowane przez uznanych wydawców, takich jak, Towarzystwo Naukowe organizacji i Kierownictwa - Dom Organizatora, Wydawnictwo Politechniki Częstochowskiej, Wydawnictwo uniwersytety Ekonomicznego w Katowicach, Dubnica Institute of Technology, Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku Białej, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Oficyna Wydawnicza Szkoły Głównej Handlowej w Warszawie, Wydawnictwo Akademii Górniczo-Hutniczej W Krakowie, Wydawnictwo Akademii Nauk Stosowanych Łomży, Wydawnictwo Politechniki Śląskiej, Szent lstvan University Publishing, ale też przez International Business Information Management Association (IBIMA), który ostatnio wzbudza kontrowersje, a jego przypadek jest szczegółowo opisany choćby przez E. Radosińskiego w Forum Akademickim nr 3/2021 (https://miesiecznik.forumakademickie.pl/czasopisma/fa-3-2021/punkty-na-sprzedaz/). Z kolei artykuły zostały opublikowane w następujących czasopismach: Przegląd Organizacji, Zeszyty Naukowe Politechniki Częstochowskiej - Zarządzanie, Przedsiębiorczość i Zarządzanie, Marketing

1 Rynek, Informatyka Ekonomiczna, Przegląd nauk Ekonomicznych, Zeszyty Naukowe Wyższej Szkoły Humanistycznej - Zarządzanie, Prace Narodowego Uniwersytetu Politechnika Lwowska, International Scientific Journal Industry 4.O., Operation Research and Decisions. Są to zatem czasopisma znajdujące się poza listą MEiN, jak i na liście, w tym takie, które mają obecnie 40 pkt i 70 pkt. Kopie wszystkich publikacji zostały dołączone do dokumentacji Habilitanta. Po zapoznaniu się z nimi stwierdzam, że są to prace, w których podejmowana jest szeroko rozumiana problematyka zarządzania informacją oraz wsparcia technologicznego dostarczanego w tym zakresie organizacjom gospodarczym w powiązaniu z różnymi procesami biznesowymi oraz obszarami funkcjonalnymi zarządzania przedsiębiorstwem. Publikacje mają różny charakter. Są takie, w których są prezentowane wyniki badań empirycznych, aczkolwiek nie są to jakieś ambitne badania, w których - jak już wcześniej pisałam - nie dąży się do zidentyfikowania jakiś nowych zjawisk czy prawidłowości o charakterze naukowym. Zwykle celem Autora jest pozyskanie informacji na temat tego, jakie są praktyki w zakresie zarządzania informacją w organizacjach lub jakie opinie wyrażają respondenci na jakiś związany z tym temat. Wśród publikacji są też takie, w których dokonuje się przeglądu literatury

w celu opisania jakiegoś zagadnienia, zaproponowania wybranych rozwiązań o charakterze koncepcyjnym lub praktycznym, ale są też takie, które przypominają opracowania podręcznikowe.

Informacje naukometryczne są podane w dokumentacji na dzień 27.12.2021 roku. Liczba cytowań zarówno w bazie Scopus, jak i Web of Science wynosi 2, a indeks Hirscha 1 natomiast wg Google Scholar liczba cytowań wynosi 44, przy czym autocytowania to 16, a indeks Hirscha 3. Z kolei liczba punktów wg mierników MEiN wynosi 631,92.

Dr inż. Paweł Kobis nie wykazał uczestnictwa w pracach zespołów badawczych realizujących projekty badawcze finansowane w drodze konkursów krajowych lub zagranicznych po uzyskaniu stopnia doktora. Jednakże uczestniczył w innych zespołach badawczych. W latach 2015-2017 był współwykonawcą projektu realizowanego wraz z Narodowym Funduszem Ochrony Środowiska i Gospodarki, pt. *Zanim udusi nas smog - Społecznościowa Platforma Transferu Wiedzy.* Od 2020 roku w ramach współpracy z Uniwersytetem Narodowym Politechnika Lwowska uczestniczy w realizacji projektu pt. *Transformacja cyfrowa marketingu szkół wyższych.* W dokumentacji Habilitant wymienia też projekt zt. *Technologie informacyjne w zarządzaniu organizacjami* pod kierunkiem prof. dr hab. inż. Leszka Kiettyki, ale nie podaje żadnych dodatkowych informacji.

Dr inż. Paweł Kobis po uzyskaniu stopnia doktora brał udział łącznie w 39 konferencjach, na których wygłosił w sumie 26 referatów (w tym 4 na konferencjach zagranicznych oraz 9 na konferencjach międzynarodowych organizowanych w Polsce) i raz występował z posterem. W okresie pandemicznym (lata 2020-2021) w większości konferencji uczestniczył poprzez aplikację MS Teams lub Google Meet. W dokumentach Habilitanta brakuje jednak szczegółowej informacji na temat organizatorów tych konferencji.

Po uzyskaniu stopnia doktora otrzymał dwie Nagrody Rektora Politechniki Częstochowskiej za prace zespołowe w obszarze naukowym, tj. 1. stopnia w 2014 r. i 3. stopnia w 2016 r.

Moja ocena osiągnięć naukowo-badawczych Dra inż. Pawła Kobisa, poza monografią - ocenioną już w poprzedniej części recenzji, jest pozytywna.

4. AKTYWNOŚĆ NAUKOWA W WIĘCEJ NIŻ JEDNEJ UCZELNI LUB INSTYTUCJI NAUKOWEJ, W SZCZEGÓLNOŚCI ZAGRANICZNEJ

Od 2018 roku Habilitant współpracuje z Katedrą Zarządzania Organizacjami Narodowego Uniwersytetu Politechnika Lwowska. Rezultatem tej współpracy są cztery wspólne publikacje (dodatkowo jest jeszcze jedna po pozytywnej recenzji przyjęta do druku): dwa artkuły (jeden w j. angielskim w czasopiśmie spoza listy MEiN, jeden w j. polskim z listy MEiN - 40 pkt) oraz dwa rozdziały w dwóch monografiach (wydawca z listy MEiN - poziom I). Habilitant jest też recenzentem jednego z czasopism w tej uczelni.

Ponadto w ramach współpracy z tym uniwersytetem oraz Wielkopolską Wyższą Szkołą Społeczno-Humanistyczną od 2020 roku realizowany jest wspólny projekt badawczy dotyczący transformacji cyfrowej marketingu szkół wyższych. Odnośnie do tej drugiej uczelni to w latach 2018- 2021 Habilitant był członkiem Rady Redakcyjnej jednego z czasopism oraz członkiem Komitetu Redakcyjnego dwóch monografii.

Można zatem powiedzieć, że wyraźna intensyfikacja współpracy z innymi ośrodkami w obszarze naukowo-badawczym nastąpiła w ciągu ostatnich kilku lat. Aktywność Habilitanta w tym zakresie uznaję za istotną i oceniam pozytywnie.

5. DOROBEK ORGANIZACYJNY, POPULARYZATORSKI I DYDAKTYCZNY

Po uzyskaniu stopnia doktora Dr inż. Paweł Kobis był współorganizatorem 15 krajowych i międzynarodowych konferencji naukowych, w których pełnił funkcje sekretarza naukowego i członka komitetu organizacyjnego lub członka komitetu programowego. W ich ramach prowadził też jedną sesję naukową i dwie biznesowe.

Do tej kategorii osiągnięć należy też zaliczyć członkostwo od 2005 roku w Towarzystwie Naukowym Organizacji i Kierownictwa w Częstochowie. Od 2013 roku Habilitant jest członkiem jej Zarządu. W latach 2015-2017 był tam współwykonawcą projektu realizowanego wraz z Narodowym Funduszem Ochrony Środowiska i Gospodarki Wodnej. Był też autorem i wykonawcą internetowej platformy transferu wiedzy.

Od 2015 roku bierze udział w pracach Zespołu Redakcyjnego czasopisma *Przegląd Organizacji,* w którym pełni też funkcję redaktora opracowania elektronicznego. Uczestniczył w działaniach popularyzujących to czasopismo, w tym w trzech większych projektach oraz wspomagających archiwizację i funkcjonalność strony internetowej.

Był recenzentem oraz aktywnym uczestnikiem komitetów organizacyjnych pięciu konferencji międzynarodowych. Jedna to International Conference on Engineering Optimization (2012 rok), a cztery organizowane w ramach IBIMA (lata 2020-2021). Wykonywał też recenzje dla czasopisma *Zarządzanie Publiczne* - Zeszytów Naukowych Instytutu Spraw Publicznych Uniwersytetu Jagiellońskiego oraz dla czasopisma *Journal of Lviv Politechnic Natinal University* - Series of Ecomomics and Management Issues.

Odnośnie do współpracy z otoczeniem społecznym i gospodarczym, to Habilitant wymienia współpracę z przedsiębiorstwem Kaspersky Lb Polska, Paragon-Software Poland (obecnie XON Investment) oraz konsorcjum FEN. Współpraca dotyczy wymiany doświadczeń z zakresu ochrony danych i informacji, udostępniania nowych rozwiązań do pracy naukowej i partycypacji w sesjach praktyków na konferencjach naukowych.

W ramach prac organizacyjnych na własnej Uczelni brał udział w komisjach rekrutacyjnych, badaniach opinii studentów na temat nauczycieli akademickich oraz komisji odpowiedzialnej za komunikacje internatową Wydziału Zarządzania z otoczeniem.

Natomiast w swojej pracy dydaktycznej Habilitant prowadził wykłady, ćwiczenia, laboratoria i projekty (w tym poprzez system e-learningowy) z 14 przedmiotów, takich jak: Komunikacja w zarządzaniu, Finanse i rachunkowość w chmurze obliczeniowej, Technologie informacyjno- komunikacyjne, Systemy finansowo-księgowe w modelu cloud comuting, Systemy informatyczne w turystyce i rekreacji. Informatyczne systemy finansowo-księgowe, metody i obszary modelowania procesów produkcyjnych, Arkusze kalkulacyjne w analizie finansowej, Informatyka, Information Technology, Projekt inżynierski, Nowoczesne technologie w turystyce, hotelarstwie i gastronomii, Technologia informacyjna oraz Makroekonomia.

Dr inż. Paweł Kobis podaje również, że był promotorem i recenzentem łącznie kilkudziesięciu prac inżynierskich, licencjackich i magisterskich, których tematyka była związana z prowadzonymi przez niego zajęciami dydaktycznymi oraz pracą badawczą, ale nie podaje ani struktury tej aktywności ze względu na pełnione role ani dokładnych danych liczbowych. Należy jednak dodać, że jest promotorem pomocniczym w przewodzie doktorskim otwartym w 2019 roku na macierzystej Uczelni. Ponadto do osiągnięć dydaktycznych i organizacyjnych można zaliczyć jego rolę

organizatorem i członka Komitetu Głównego *Olimpiady Przedsiębiorczości,* która miała miejsce na Politechnice Częstochowskiej w 2020 roku.

Habilitant po uzyskaniu stopnia doktora otrzymał też trzy odznaczenia: Medal 20-lecia Wydziału Zarządzania Politechniki Częstochowskiej (2017 rok), Medal Brązowy za Długoletnią Służbę nadany przez Prezydenta RP (2018 rok) oraz Medal Komisji Edukacji Narodowej za szczególne zasługi dla oświaty i wychowania nadany przez Ministra Edukacji i Nauki (2021 rok). Ponadto został wielokrotnie nagrodzony Nagrodą Rektora Politechniki Częstochowskiej za prace zespołowe, w tym sześć razy w obszarze organizacyjnym (2 st. - 2012 r., 2013 r., 2014 r., 2016 r.; 3 st. - 2016 r., 2017 r.) oraz raz w dydaktycznym (2 st. - 2016 r.).

Można zatem powiedzieć, że dorobek organizacyjny, popularyzatorski oraz dydaktyczny Dra inż. Pawła Kobisa jest różnorodny i wartościowy merytorycznie. W związku z tym i ten dorobek zostaje przez mnie oceniony pozytywnie.

6. KONKLUZJA

W świetle zaprezentowanych ocen dotyczących głównego osiągnięcia Habilitanta (tj. monografii), jego dorobku naukowo-badawczego, aktywności naukowej w więcej niż jednym ośrodku naukowym oraz osiągnięć organizacyjnych, dydaktycznych i popularyzatorskich stwierdzam, że chociaż kompetencje badawcze Dra inż. Pawła Kobisa w minimalnym stopniu spełniają oczekiwania stawiane przez osoba ubiegającą się o stopień naukowy doktora habilitowanego, to jest on samodzielnym i doświadczonym badaczem, który w swoich badaniach jest przede wszystkim ukierunkowany na identyfikowanie niewłaściwych praktyk organizacyjnych w zakresie zarządzania bezpieczeństwem zasobów informacyjnych, aby zaproponować stosowane rozwiązania poprawiające to bezpieczeństwo. Cechuje go konceptualna dociekliwość, dobry warsztat metodyczny użytkownika systemów zarządzania informacją, wykazał się kompetencjami potrzebnymi zarówno do współpracy w zespołach badawczych jak i publikacyjnych, ale przede wszystkich wysoko należy ocenić jego kreatywność i nowatorskie podejście do rozwiązywania problemów o charakterze naukowo-praktycznym. W związku z tym uważam, że Dr inż. Paweł Kobis spełnia wymogi ustawowe stawiane kandydatom w postępowaniu habilitacyjnym i w pełni popieram jego wniosek o nadanie mu stopnia naukowego doktora habilitacyjnego nauk społecznych w dyscyplinie nauk o zarządzaniu.

Wrocław, 09.06.2022 r.