Prof. dr hab. Elżbieta Skrzypek
Uniwersytet Kaliski
im. Prezydenta St. Wojciechowskiego
w Kaliszu

Recenzja pracy doktorskiej mgr Piotra Szeflińskiego pt. Zarządzanie bezpieczeństwem wiedzy w uczelniach publicznych, Politechnika Łódzka, promotor dr hab. inż. Zbigniew Wiśniewski prof. Politechniki Łódzkiej, promotor pomocniczy dr inż. Małgorzata Wiśniewska, Politechnika Łódzka, Wydział Zarządzania, Łódź 2024

Uzasadnienie podjęcia tematu pracy

Problem podjęty w pracy doktorskiej ma charakter naukowy. Waga problemu wynika z funkcjonowania organizacji, w tym uczelni w warunkach GOW, społeczeństwa informacyjnego, sieciowego, w którym wiedza pełni zasadniczą rolę. Podjęty problem badawczy jest ważny, nierozwiązany, istotny od strony naukowej i praktycznej. Istnieje bowiem konieczność odpowiedniego zarządzania wiedzą, w tym jej ochrony i zarządzania bezpieczeństwem wiedzy.

Cel główny pracy: Ocena roli świadomości władz uczelni dotyczącej zarządzania wiedzą we wdrożeniu mechanizmów zarządzania bezpieczeństwem wiedzy.

Realizacji celu głównego służą cele szczegółowe:

1. Identyfikacja poziomu świadomości władz uczelni dotyczącej zarądzania wiedzą.

2. Identyfikacja poziomu świadomości władz uczelni dotyczącej posiadanych zasobów wiedzy i ich wartości w poszczególnych typach uczelni.

3. Identyfikacja mechanizmów ochrony wiedzy i informacji, a także stopnia ich wdrożenia w poszczególnych typach uczelni.

4. Ocena czynników wpływających na wdrożenie mechanizmów ochrony wiedzy i informacji w poszczególnych typach uczelni.

Realizacji celów rozprawy służą pytania badawcze:

1. Jaka jest świadomość władz uczelni w kwestii funkcjonowania procesu zarządzania wiedzą w uczelni i celów jego wdrożenia?
2. Jakie mechanizmy i narzędzia są stosowane do ustanawiania i egzekwowania zasad zarządzania wiedzą/bezpieczeństwem wiedzy?
3. Jakie zasoby wiedzy są w dyspozycji uczelni w poszczególnych typach uczelni?
4. Jakie jest znaczenie poszczególnych zasobów wiedzy dla uczelni i jakie są metody szacowania ich wartości w poszczególnych typach uczelni?
5. Jakie są i jak są identyfikowane ryzyka związane z poszczególnymi zasobami wiedzy?
6. Jaka jest świadomość władz uczelni na temat funkcjonowania procesów ochrony wiedzy w uczelni i celów jej wdrożenia?
7. Jakie czynniki wpływają na podjęcie decyzji o wdrożeniu mechanizmów ochrony wiedzy w poszczególnych typach uczelni?

Metoda badawcza: wywiad kwestionariuszowy

Ocena merytoryczna pracy

Praca posiada dwie warstwy teoretyczną i empiryczną, które się wzajemnie uzupełniają tworząc logiczną całość. Praca składa się z czterech rozdziałów.

Autor przedstawia znaczenie wiedzy w uczelniach, odnosi się do wiedzy i zasobów wiedzy. Omawia istotę i przydatność piramidy wiedzy: D-I-W-M. Przedstawia kategoryzację wiedzy (dostępna, ukryta,

indywidualna, grupowa, organizacyjna, międzyorganizacyjna, naukowa, potoczna). Omawia wybrane problemy związane z zarządzaniem ryzykiem związanym z zarządzaniem wiedzą i informacją.

Autor wskazuje, że zapewnienie ciągłości działania nie jest procesem metodycznie wdrożonym w uczelniach, występują tylko pewne elementy dotyczące systemów informatycznych. Przybliża istotę SZBI, przywołuje Rozporządzenie RM z 12.IV 2012 r, wskazuje, że z przepisów tych wynika, że SZBI powinien być wdrożony w uczelniach, w szczególności dla systemów teleinformatycznych przetwarzających informacje niejawne (Rozorzadzenie RODO- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016).

Autor pracy podkreśla, że każda uczelnia, ze względu na kontekstowy charakter wiedzy wdraża swoje indywidualne zasady wykorzystywania i ochrony zasobów wiedzy, uzależnione od struktury organizacyjnej, umiejscowienia, rozległości infrastruktury technicznej, używanych systemów informatycznych, organizacji pracy działów IT, stopnia i zakresu relacji z podmiotami zewnętrznymi np. realizowane usługi outsourcingu. Przedstawiono etapy zarządzania ryzykiem w uczelni (tab. 1.1.). Doktorant wskazał na przydatność normy PN-EN ISO /IEC 27005:2014-01 Technika informatyczna-Techniki Bezpieczeństwa-Zarzadzanie ryzykiem w bezpieczeństwie informacji. Autor odniósł się do wyceny zasobów wiedzy wskazując, że umożliwia ona rozwiązanie problemów poznawczych dotyczących identyfikacji, klasyfikacji i kwantyfikacji posiadanych zasobów oraz problemów decyzyjnych, dotyczących określenia sposobów okresowego raportowania wartości zasobów i ich zmian w czasie. Ponadto nawiązał do problematyki kapitału intelektualnego, który obejmuje kapitał związany z innowacjami- strukturalny, z rynkiem (klientów) i ludzki. Wskazał na trudności związane z pomiarem wiedzy i kapitału intelektualnego.

Autor pracy doktorskiej szeroko odnosi się do problematyki zarządzania wiedzą, rozważania łączy odnosząc się do zarządzania informacją i wiedzą. Przedstawia wybrane podejścia do strategii zarządzania wiedzą, wskazuje na przydatność normy ISO 30401:2018 Knowledge Management Systems-Requirements. Przywołuje definicję zarządzania wiedzą, zawartą w tej normie, z której wynika, że: obejmuje ono optymalizację identyfikacji, tworzenia, analizy, przedstawiania, dystrybucji i zastosowania wiedzy w celu tworzenia wartości organizacji. Norma przedstawia przykładowe problemy związane z zarządzaniem wiedzą oraz zalety wynikające z jego wdrożenia. Wskazuje na silne powiązania pomiędzy informacją i wiedzą. Omawia procesowe podejście, dokonuje przeglądu literatury dotyczącej klasyfikacji procesów (tab. 1.2). Doktorant przywołał metodę praktycznej operacjonalizacji zarządzania więdzą opracowaną przez J. Zawiłę-Niedźwieckiego (spirala doskonalenia gromadzenia, formułowania wiedzy i korzystania z wiedzy).

W pracy ponadto przedstawiono poziomy zarządzania wiedzą, dokonano przeglądu literatury, odniesiono się do poziomów dojrzałości w obszarze zarządzania wiedzą (chaos, olśnienie, inicjacja, oswojenie i podporządkowanie). Autor powołuje się w rozważaniach na normę izraelską SI 25006 z 2011 roku. Określa ona poziomy wdrożenia odnosząc się do odpowiedzialności, zasobów wdrożenia, rozwiązań, kultury organizacji, dokumentacji, pomiaru efektywności organizacyjnej, monitorowania i ciągłej poprawy.

Ukazuje istotę i znaczenie systemu zarządzania wiedzą, przedstawia przydatność informatycznych systemów zarządzania wiedzą oraz ich klasyfikację, w tym business intelligence, systemy pracy grupowej, systemy zarządzania dokumentami i treściami.

Odnosi się do bardzo ważnego problemu, jakim jest ochrona wiedzy i ochrony informacji. Podkreśla, że problem ten jest słabo rozpoznany w literaturze. Przedstawił wybrane podejścia do rozumienia ochrony wiedzy. Wskazał na paradoks polegający na rozróżnieniu dwóch przeciwstawnych strategii zarządzania wiedzą: strategii ochrony wiedzy i strategii udostępniania wiedzy.

W dalszej części pracy Autor odnosi się do zasobów wiedzy i zarządzania wiedzą w uczelniach. Przywołuje wyniki badań przeprowadzone w Hiszpanii, z których wynika potrzeba umieszczania w systemie informacji księgowej danych o kapitale intelektualnym uczelni, wskazano tu uwarunkowania społeczne, ekonomiczne, polityczne i kulturalne, które ten proces wymuszają.

Wskazał także na klasyfikację zasobów wiedzy i informacji w uczelni (za T. Stefaniakiem i B. Mikułą), przedstawił zasoby wiedzy spersonifikowanej, skodyfikowanej, ugruntowanej. Wskazał na potrzebę

ustandaryzowania identyfikacji zasobów wiedzy uczelni i opracowanie zasad i metodyki ochrony wiedzy.

Ważnym zagadnieniem podjętym w tej części pracy jest zarządzanie wiedzą w uczelniach. Wskazał, że główną misją uczelni jest tworzenie i udostępnianie wiedzy, a jej realizacja to główny cel strategiczny uczelni. Wskazuje, że uczelnie powinny w sposób świadomy zarządzać zasobami informacji i wiedzy. Wskazuje na modele zarządzania informacją wg Deji. Podkreśla deficyt zarządzania wiedzą. Przedstawia wyniki badań różnych autorów i wskazuje na ważne problemy: związek efektywnego kierowania uczelnią z właściwym zarzadzaniem wiedzą (Australia), brak zinstytucjonalizowanych procesów zarządzania wiedzą (Słowenia), zależność skuteczności dzielenia się wiedzą od kultury organizacyjnej (W. Brytania), wpływ zaangażowania nauczycieli w problematykę zarządzania wiedzą- wpływ na wzrost efektywności procesu nauczania i rozwój uczelni (Uniwersytet w Malbourne), wpływ braku kultury dzielenia się wiedzą na porażki zarządzania wiedzą (Indie).

Autor słusznie podkreśla, że rynek pracy będzie wymuszał na uczelniach aktywniejsze podejście do dzielenia się wiedzą. Badania w Egipcie i Hiszpanii potwierdzają niedopasowanie rynku pracy i efektów kształcenia w uczelniach.

Badania 200 uniwersytetów w USA potwierdzają, że tylko 54% uczelni posiada pisemne polityki bezpieczeństwa (technologiczne i informacyjne), które często są niespójne z załączonymi dokumentami i nie zawsze są zrozumiałe. Wskazano na konieczność opracowania odpowiednich polityk bezpieczeństwa. Analiza opublikowanych prac wskazuje na duże niedostatki w zakresie zarządzania wiedzą na uczelniach zagranicznych.

Słusznie podkreśla, że trzeba wskazać na ważny problem, mocno podkreślany tj. występowanie deficytu wiedzy o wiedzy i jego konsekwencje.

Na podkreślenie zasługuje ważny problem podjęty w dysertacji jakim jest trójkąt wiedzy (synergia między nauką-badaniami, edukacją – dydaktyka i innowacjami). Autor wskazał na jego istotę i znaczenie. Jego waga dowodzi utworzenia w 2008 roku na jego bazie Europejskiego Instytutu Innowacji i Technologii (EIT), z którym w pewnym zakresie współpracują UJ, Politechnika Krakowska, AGH, UW, Politechnika Śląska, AGH, UJ, Politechnika Krakowska, Politechnika Wrocławska. Jednocześnie podkreśla, że nie ma polskich uczelni w znaczących programach np. EIT Manufacturing Partners (wśród 21 uczelni nie ma polskich).

Doktorant wskazuje na podejście UE do wiedzy podkreślając, że w 2011 roku wiedza została uznana przez UE za zasadnicze pole działań zmierzających do osiągnięcia inteligentnego i trwałego rozwoju gospodarczego UE. Potwierdzeniem tego jest rekomendowanie zwiększania nakładów na inwestycje w edukację, badania i innowacje i wzmocnienie powiązania szkolnictwa, badań naukowych i biznesu w trójkącie wiedzy

Autor pracy stwierdza, że w dokumentach strategicznych nie ma odwołania do roli uczelni w budowaniu GOW i wskazuje na przyczyny.

Kolejno Doktorant podejmuje problemy związane z bezpieczeństwem wiedzy w uczelniach i podkreśla, w oparciu o analizę badań, że brakuje holistycznego podejścia do problemu bezpieczeństwa wiedzy w uczelniach. Odnosi się do RODO i systemu cyberbezpieczeństwa (prowadzenie rejestru incydentów bezpieczeństwa i raportowania o nich do odpowiedniej agendy rządowej). Wskazał, że nowa ustawa nakazuje spojrzenie na cyberbezpieczeństwo uczelni z poziomu jej władz, organizując ten proces na poziomie centralnym. Omawiając problematykę bezpieczeństwa wiedzy odnosi się do rozwiązań normatywnych (normy ISO i KRI- Krajowe Normy Interdyscyplinarności). Przybliża istotę SZBI.

Kolejna część pracy poświęcona została obszarom ochrony wiedzy w uczelniach. Przedstawiono rodzaje wiedzy chronionej w uczelni (Tab. 2.1). Autor omawia koncepcję otwartej nauki i jej założenia, wskazuje, że ma na celu dostęp do wszystkich elementów projektu badawczego, chodzi tu o publiczne udostepnienie cyfrowej postaci prowadzonych wyników badań i rozszerzenie zasad otwartości na cały cykl badawczy, promowanie dzielenia się i współpracę tak szybko, jak to możliwe. Jest to systemowa zmiana sposobu prowadzenia nauki i badań. Otwartą naukę rekomenduje UNESCO i KE.

Autor pracy odnosi się też do raportów, w których ogłaszane są działania. Omawia problem „drapieżnych czasopism". Wskazuje na powstanie nowego paradygmatu nauki traktującego naukę jako dobro publiczne.

Wskazuje, że w Polsce NCN od 2019 roku stawia się osobom realizującym granty warunek opracowania Planu Zarządzania Danymi DMP-Data Management Plan. W 2020 roku NCN wprowadziło „Politykę dotyczącą otwartego dostępu do publikacji naukowych" obowiązującą dla wszystkich umów podpisanych do 2021 roku. Jest to reakcja na dokument wydany w 2018 roku przez MNiSzW „Kierunki rozwoju otwartego dostępu do publikacji wyników badań naukowych w Polsce. Obecnie te kwestie reguluje ustawa o otwartych danych (Ustawa z 11.VII 2021 o otwartych danych i ponownym wykorzystaniu informacji sektora publicznego. Polityka otwartego dostępu MNiSzW opiera się na pięciu zasadach: otwartości, równoległych dróg, szybkiego dostępu, maksymalizacji jakości i maksymalizacji korzyści. Doktorant omawia te zasady. Odnosi się też do problemów związanych z dostępem do informacji publicznej, przywołuje ustawę o dostępie do informacji publicznej, wskazuje definicję informacji publicznej i sposoby udostępnienia informacji publicznej. Wskazuje zadania polityki informacyjnej uczelni, w tym odnosi się do BIP- Biuletynu Informacji Publicznej.

Podkreśla rolę wiedzy jawnej chronionej, w tym własności intelektualnej, wskazuje na zachowanie legalności oprogramowania jako ochronę własności intelektualnej strony trzeciej. Podkreśla, że wymóg ustawowy nakazuje senatowi uczelni przyjąć regulamin zarządzania prawami autorskimi i prawami pokrewnymi oraz prawami własności przemysłowej i zasad komercjalizacji. Przedstawił zawartość regulaminu. Odnosi się do postępowania patentowego, wskazuje cechy zarządzania własnością intelektualną w kontekście jej komercjalizacji. Wskazuje na Jednolity System Antyplagiatowy jako centralne działanie wspierające bezpieczeństwo wiedzy w obszarze własności intelektualnej (działający od 2019 roku). Omawia problem legalności oprogramowania i piractwa komputerowego. Odnosząc się do wiedzy ukrytej Autor pracy wskazuje na potrzebę zakwalifikowania obszarów wiedzy do właściwej grupy zasobów wiedzy chronionej. Analizie poddaje tajemnice przedsiębiorstwa i bezpieczeństwo IT odnosząc je do uczelni. Wskazano na aspekty wyróżniające uczelnie spośród innych uczestników życia społeczno-gospodarczego w aspekcie cyber-zagrożeń. Przedstawiono standardy opisujące funkcjonowanie i bezpieczeństwo systemów informatycznych (rodzina norm ISO 27000). Wskazano, że dbałość o bezpieczeństwo IT to ważny wymóg prawny. Doktorant odnosi się do ochrony danych osobowych i ochrony informacji niejawnych, przedstawia ich istotę, klasyfikacje i warunki dostępu, ukazuje prawna stronę zagadnienia.

Część teoretyczna pracy została opracowana w sposób poprawny, dowodzi znajomości problemów podejmowanych w niniejszej pracy doktorskiej przez jej autora i umożliwia realizację celów postawionych przed pracą, tę część dysertacji oceniam pozytywnie.

Druga część rozprawy to część badawcza.

Autor przedstawia tu obszary badawcze i luki badawcze. Uzasadnia wybór tematu pracy wskazując, że badania obejmują zarządzanie informacją, wiedzą i bezpieczeństwo informacji i wiedzy w środowisku szkół wyższych w Polsce. Autor dokonał analizy dorobku publikacyjnego w interesującym zakresie w publikacjach w Polsce i w skali międzynarodowej (Web of Sciene i Scopus) Analizie poddano projekty, prace naukowo-badawcze, rozprawy doktorskie i habilitacyjne oraz ekspertyzy naukowe. Użyto repozytoriów utworzonych przez MEiN zawierające dane o prowadzonych pracach badawczych (Polska Bibliografia Naukowa PBN, baza SYNABA, będące częścią repozytorium Nauki Polskie)j. Wyniki badań przedstawiono w tab. 3.1, 3.2, 3.3., 3.5. Badanie baz powtórzono dla lat 2012-2023.

Zidentyfikowano trzy luki:

- teoretyczną, związaną z niedostatecznym i niejednoznacznym opisaniem zagadnienia zachowania bezpieczeństwa informacji i wiedzy w polskich uczelniach,

- empiryczną, w obszarze polskiego piśmiennictwa nie znaleziono opisów badań w obszarze zarządzania informacją i wiedzą w uczelniach,

- metodyczną- niedostatek metod i narzędzi w obszarze konceptualizacji i operacjonalizacji zmiennych badawczych związanych z zasobami wiedzy i ich bezpieczeństwem.

W pracy podjęto eksplorację luki badawczej w postaci luki empirycznej- braku badań związanych z udziałem najwyższych władz uczelni w procesie wdrażania zarządzania wiedzą, a szczególnie wdrażania zasad bezpieczeństwa wiedzy jako strategicznym procesie zarządczym.

Autor przedstawił rozumienie zarządzania wiedzą i świadomości władz uczelni w zakresie bezpieczeństwa wiedzy, którym posługuje się w pracy.

Sformułował pytanie: Czy świadomość władz uczelni w obszarze zarządzania bezpieczeństwem zasobów wiedzy jest w ogóle potrzebna i czy ma wpływ na zapewnienie tego bezpieczeństwa. Wskazał cel główny i 4 cele szczegółowe i 7 pytań badawczych, wskazał osiem etapów rozpoznania i opisania problemu badawczego.

Etap I- badanie wstępne desk research otoczenia formalno-prawnego: analiza dostępnych źródeł, badanie danych wtórnych, aktów prawnych i norm.

Etap II- dobór próby badawczej, spośród 97 publicznych szkół akademickich wybrano 20 czyli 21% liczebności całej badanej grupy. Wykorzystano ranking szkół wyższych publikowany 21 raz w Tygodniku Perspektywy, wykorzystano 7 kryteriów: prestiż 12%, absolwenci na rynku pracy 12%, innowacyjność 8%, potencjał naukowy 15%, efektywność naukowa 28%, warunki kształcenia 10%, umiędzynarodowienie 15%. Lista obejmuje 6 uniwersytetów, 7 uczelni technicznych, 6 uczelni medycznych i 2 inne szkoły (tab. 3.9). Próba nie ma cechy reprezentatywności w stosunku do całej populacji.

Etap III- analiza dokumentów uczelni z próby badawczej, analiza dostępnych publicznie wewnętrznych aktów prawnych: struktura, statut, strategia, misja, zadania przydzielone członkom władz i innych informacji ze stron internetowych uczelni i PIB. Celem tego etapu było poznanie specyfiki uczelni, uzyskanie obiektywnego materiału porównawczego dla danych uzyskanych z badania właściwego, wykonanie zobiektywizowanej analizy porównawczej uczelni na podstawie opublikowanych dokumentów.

Etap IV- opracowanie narzędzia badawczego, zastosowano triangulację metod: metodę ilościową opartą o standaryzowaną technikę ankiety badawczej, wywiad kwestionariuszowy i indywidualny. Badania przeprowadzono metodą CATI (wideokonferen). Pytania dotyczyły strategii, procedur, narzędzi wspomagających zarzadzanie wiedzą, oceny wybranych do badania zmiennych. Większość pytań to pytania zamknięte, odpowiedzi wielokrotnego wyboru, kafeterie i pytania półotwarte. Wykorzystano 5 stopniową skalę Likerta. Pytania były dyfuzyjne (możliwość wyboru tylko jednej odpowiedzi). Przyjęto skalę porządkową 1-5, w niektórych interwałową. Przyjęta skala jest jednostronna (nie ma zera). Pytania ustalono w oparciu o analizę aktów prawnych, norm, badań własnych, doświadczenia Autora zdobytego podczas pracy w Politechnice Łódzkiej.

Autor wyjaśnił, że cel badania, jakim jest ocena poziomu świadomości władz uczelni- nie może być osiągnięty wprost w wyniku badania, dlatego zastosowano operacjonalizację poprzez wprowadzenie pięciu wskaźników oceny poziomu świadomości władz w zakresie zarządzania bezpieczeństwem wiedzy.

Badanie praktycznego poziomu zarządzania wiedzą celowo przeprowadzono przez pryzmat zarządzania bezpieczeństwem informacji stosując metodę korelacji empirycznej. W rozumieniu prowadzonych rozważań informacja nabiera znamion wiedzy. Autor uzasadnił przyjęcie w badaniu zmiennych związanych z ochroną informacji do badania poziomu ochrony wiedzy. W rozprawie badano następujące mechanizmy bezpieczeństwa wiedzy:

- obecność zagadnień zarządzania wiedzą w dokumentach strategicznych uczelni,

- delegowanie zadań związanych z zarządzaniem wiedzą i jej bezpieczeństwem,

- wdrożenie w uczelni centralnych mechanizmów zarządzania bezpieczeństwem wiedzy,

- prowadzenie i monitoring wniosków analizy ryzyka, analizy incydentów bezpieczeństwa, audyty z zakresu bezpieczeństwa informacji, szkolenia,

- wdrożenie technicznych narzędzi bezpieczeństwa informacji.

Ankieta zawiera 60 pytań w 5 tematycznych częściach:

- charakterystyka organizacji- 12 pytań,

-charakterystyka zarządzania wiedzą w uczelni- 6 pytań,

- zasoby uczelni – 3 pytania,

- procesy zarządzania wiedzą w uczelni- 11 pytań,

- charakterystyka zarządzania bezpieczeństwem informacji w uczelni- 22 pytań.

Etap V : walidacja narzędzia badawczego- panel ekspertów w celu sprawdzenia ankiety pod względem językowym, metodologicznym i odpowiedniości poziomu percepcyjnego. Panel stanowiło 10 ekspertów, ankietę oceniło 8. Ocena była pozytywna.

Etap VI: badanie właściwe- wywiad kwestionariuszowy

Etap VII: analiza i synteza wyników badań i konfrontacja z literaturą. Wykorzystano tu analizę i syntezę oraz dedukcję. Proces syntezy dotyczył każdej uczelni oraz agregacji odpowiedzi udzielonych przez przedstawicieli różnych typów uczelni. Ostateczna synteza dotyczyła sformułowania wniosku generalnego, będącego odpowiedzią na główne pytania badawcze. W pracy nie zastosowano metod statystycznych. Celem badania nie była ekstrapolacja wyników na całą populację uczelni publicznych. Badaniem objęto 16 studiów przypadku opartych o pogłębiony wywiad. Wybór uczelni nie był probabilistyczny, a oparty na rankingu uczelni.

Etap VIII- ograniczenia badawcze i dalsze kierunki badań

Ocena wyników badań

Wyniki badania wstępnego (02. 2020-01.2021, 01.2012-07.2021). Wykorzystano dokumenty: misję i wizję uczelni, strukturę organizacyjną, strategię, zakresy kompetencji władz uczelni, centrum transferu technologii. W badaniu przedmiotowym wyróżniono zarządzanie wiedzą, trójkąt wiedzy i bezpieczeństwo wiedzy. Stwierdzono małe zaangażowanie uczelni w tematykę zarządzania wiedzą i bezpieczeństwo wiedzy. Badanie nie przyczyniło się w sposób znaczący do rozpoznania wdrożonych procedur i mechanizm związanych z zarządzaniem wiedzą i bezpieczeństwem wiedzy w badanych uczelniach. Analiza dokumentów (www, BIP) wykazała brak holistycznego podejścia do zarzadzania wiedzą, ponadto dokumenty strategiczne nie zawierały odniesienia do procesów zarządzania wiedzą.

Wyniki badań podstawowych (19.01 2021-14.07. 2021)- udział w badaniu wzięło 16 uczelni, odpowiedzi udzieliło 3 rektorów, 10 prorektorów i 3 inne osoby. Czas wypełnienia ankiety wynosił średnio 40-50 minut. Z badań wynika, że uczelnie nie planują wdrożenia normatywnych rozwiązań w obszarze zarządzania wiedzą, stwierdzono niski poziom wiedzy w tym obszarze. Potwierdzono, że badani mają poczucie ważności zarządzania wiedzą, ale nie przypisano jej do najważniejszych władz uczelni. W żadnej badanej uczelni proces zarządzania wiedzą nie jest zdefiniowany ani przypisany w sposób formalny do przedstawicieli władz.

W odpowiedzialności za bezpieczeństwo informacji można stwierdzić, że istnieje ono w sferze formalnej a świadomość respondentów w zakresie funkcjonowania w uczelni jego procesów nie odpowiada stanowi formalnemu (znajomość ról i zadań). W strukturach uczelni brakuje jednostek wydzielonych do kompleksowego i scentralizowanego zarządzania wiedzą w organizacjach, stwierdzono występowanie przypadków wybiórczego i rozproszonego podejścia. Z badań dotyczących charakterystyki zarządzania wiedzą wynika, że występuje duża świadomość władz uczelni w stosunku do strategii w zakresie obecności lub jej braku w zakresie zarządzania wiedzą. Spośród 16 uczelni tylko 4 planuje zbudowanie SZW, a jego elementy wskazuje 7 uczelni. Wśród dokumentów związanych z zarządzaniem wiedzą są zarządzenia rektora (4), kodeks dobrych praktyk (7), polityka

bezpieczeństwa informacji(6), regulamin zarzadzania wiedzą (0), inne (4). Uczelni nie wprowadziły dokumentów odnoszących się w sposób ogólny do zarządzania wiedzą. Z przeprowadzonych badań wynika, że uczelnie jednocześnie wprowadzają wybrane dokumenty szczegółowe związane z problemem zarządzania wiedzą i ochrony zasobów wiedzy wynikających z obowiązków ustawowych. (tab. 3.12).

W tab. 3,13 i 3.14 wskazano cele zarządzania wiedzą, najczęściej wskazywano rozwój zasobów wiedzy i kompetencji, zabezpieczenie wiedzy dla uczelni, jak najszersze udostępnianie wiedzy wewnątrz uczelni. Niskie oceny przypisano celom związanym z rozwojem wiedzy wewnętrznej i związanym z ochroną wiedzy. W tab. 3.15 odniesiono się do beneficjentów wdrożenia zarządzania wiedzą.

Kolejny obszar badań dotyczył zasobów wiedzy w uczelniach. Średnią ocen priorytetu przypisanego zasobom wiedzy zawiera tabela 3.16. Dominuje postrzeganie wiedzy przez pryzmat zarządzania nauką i dydaktyką. Związek zasobów wiedzy z przewagą konkurencyjną przedstawiono w tab. 3.17. Władze uczelni postrzegają przewagę swoich organizacji w indywidualnych osiągnięciach naukowych np. prowadzenie unikatowych badań, unikatowego potencjału badawczego, publikacji, organizowanych konferencji i czasopism. Najsłabiej spośród elementów trójkąta wiedzy ocenione zostały innowacje.

Z badań wynika, że uczelnie nie dokonują inwentaryzacji zasobów wiedzy ani jej wyceny.

Kolejną częścią badań były procesy zarządzania wiedzą w uczelni. Stwierdzono brak mechanizmów egzekwowania zasad zarządzania wiedzą, ponadto szacowanie ryzyka nie zostało formalnie wprowadzone w uczelniach.

Wdrażanie procesów i technologii zarządzania wiedzą przedstawiono w tab. 3.18, 19, 20, 21 i 22. Z badań wynika, że wdrażane są procesy wynikające z bieżącego funkcjonowania organizacji i jej głównych procesów. W najmniejszym stopniu procesy zarządzania wiedzą wdrożone są w obszarze dydaktyki, najszerzej w obszarze zdobywania wiedzy. Ochrona wiedzy postrzegana jest w uczelniach przez poufność i to najszerzej w odniesieniu do ochrony danych osobowych.

Respondenci odnieśli się do narzędzi wykorzystywanych w zarządzaniu wiedzą (tab. 3.24), stwierdzili, że najczęściej są to narzędzia usprawniające bieżącą komunikację i pracę grupową, w tym zdalną.

Ważnym obszarem badań był transfer wiedzy (tab. 3.26) i usługi doradztwa naukowego (tab. 3.26). Uczelnie posiadają świadomość potrzeby transferu wiedzy na zewnątrz organizacji i to realizują. Wynika to z przepisów prawa (celowe spółki transferu technologii). Tworzone są też w sposób niewymuszony inkubatory przedsiębiorczości, parki i klastry technologiczne. Uczelnie dokonują transferu i upowszechniania wiedzy. Jednocześnie wskazują, że potencjał w tym zakresie nie jest w pełni wykorzystany.

Z badań wynika, że 10 spośród 16 uczelni przeprowadza szkolenia wewnętrzne z zakresu zarządzania wiedzą. Badano także opinię na temat zabezpieczenia wiedzy w procesie transferu wiedzy. Niektórzy respondenci posiadali odpowiednie dokumenty (regulamin własności intelektualnej), 30% badanych kojarzy ten dokument z zarządzaniem bezpieczeństwem wiedzy. Ochrona zasobów wiedzy w uczelniach nie jest procesem w pełni uświadomionym ani realizowanym samoistnie.

Rola bibliotek w zarządzaniu wiedzą – to kolejny problem objęty badaniem, biblioteki postrzegane są jako ważny element realizujący procesy zarządzania wiedzą w uczelni, podobnie postrzegane są repozytoria i bazy danych gromadzące tworzone w uczelni zasoby wiedzy.

Kolejny obszar badawczy dotyczy zarządzania bezpieczeństwem informacji w uczelniach. W tab. 3.27 przedstawiono ważność celów ochrony informacji. Najwyżej (4,9) oceniono: zapewnienie ciągłości działania uczelni i jej systemów informatycznych, zachowanie poufności danych i zabezpieczenie własności intelektualnej (4,8). Działania związane z zapewnieniem bezpieczeństwa informacji zawiera tab. 3.28, należą tu szkolenia, działania informacyjne i audyty. Z badań wynika istnienie świadomość konieczności ich przeprowadzania wśród badanych przedstawicieli uczelni.

Wyniki badania w zakresie wdrożenia norm, przepisów i wytycznych związanych z bezpieczeństwem informacji zawarto w tab. 3.29, 30, 31,32. Wynika z nich, że rozwiązania te nie są wdrażane w uczelniach w dużym zakresie. Procesy te jednocześnie realizowane są niezależnie od woli, wpływu

czy świadomości władz uczelni (dane osobowe, informacje niejawne, bezpieczeństwo informacyjne). Stwierdzono słabe działanie ustrukturyzowanych i ustandaryzowanych procesów ochrony informacji. W tab. 3.33 odniesiono się do stanowisk odpowiedzialnych za ochronę informacji.

Badano ciągłość działania uczelni, zapewnienie ciągłości działania nie jest procesem metodycznie wdrożonym w uczelniach, występują tylko pewne elementy dotyczące systemów informatycznych. Podobna sytuacja występuje w obszarze wdrażania mechanizmów zarządzania incydentami bezpieczeństwa. Świadomość władz uczelni w tym obszarze oceniono jako niską.

Szacowanie ryzyka związanego z bezpieczeństwem informacji (tab. 3.34) dowodzi, że najwięcej procesów szacowania ryzyka dotyczy ochrony danych osobowych, ochrony informacji niejawnych i kontroli zarządczej. Wskazano też osoby odpowiedzialne w uczelni za szacowanie ryzyka związanego z bezpieczeństwem informacji (tab. 3.35).

Z badań wynika, że w 50% badanych uczelni procesy szacowania ryzyka są wdrożone, w większości dotyczą obszarów, gdzie to szacowanie wynika z przepisów prawa. Tylko w 30% uczelni istnieje świadomość prawnego wymogu zapewnienia audytu bezpośredniego informacji i audyty te są wykonywane (nie mają miejsca w uniwersytetach). Tylko w 5 spośród 16 badanych uczelni władze mają świadomość funkcjonowania w uczelni SZBI. W tab. 3.36 i 3.37 wskazano przeszkody we wdrażaniu SZBI, lokowane są one w obszarze zasobów ludzkich i kultury organizacyjnej uczelni. W tab. 3.38 wskazano korzyści związane z wdrożeniem SZBI. Respondenci widzą te korzyści w obszarze doraźnego i krótkoterminowego bezpieczeństwa związanego z odpowiedzialnością za naruszenie prawa oraz w osiągnięciu celów operacyjnych, związanych z udoskonaleniem procesów wewnątrzorganizacyjnych.

Badaniu poddano ponadto ocenę wpływu pandemii COVID-19 na bezpieczeństwo informacji w uczelni. Podkreślano, że sytuacja ta miała wpływ na funkcjonujące zasady zachowania bezpieczeństwa informacji, wskazano na wprowadzane rozwiązania.

Autor pracy w tab. 4.1 przedstawił pytania badawcze w powiązaniu z realizowanymi celami i pytaniami kwestionariuszowymi. Stwierdził, że:

- istnieje niewielka świadomość władz uczelni dotycząca strategicznego i holistycznego charakteru procesu zarządzania wiedzą,

- strategiczne i przemyślane zarządzanie wiedzą jest szansą na zdobycie przewagi konkurencyjnej- z badań wynika wątpliwość czy uczelnie korzystają z tej szansy,

- władze uczelni nie posiadają wiedzy dotyczącej zasobów, jakimi uczelnie dysponują,

- znaczenie zasobów wiedzy dla uczelni i metody szacowania ich wartości są różnie postrzegane, w uczelniach nie prowadzi się kompleksowej, systematycznej i zobiektywizowanej klasyfikacji i wyceny zasobów wiedzy-proces szacowania ryzyka w tym obszarze nie jest prowadzony w sposób całościowy i formalny, nie wskazano najważniejszych, zidentyfikowanych ryzyk związanych z bezpieczeństwem informacji (10 spośród 16 uczelni nie udzieliło odpowiedzi),

- świadomość władz uczelni w zakresie funkcjonowania w nich procesów ochrony wiedzy jest niejednorodna. Istnieje ona w obszarze funkcjonowania regulaminu ochrony własności intelektualnej, w obszarze ochrony danych osobowych i ochrony informacji niejawnych. Niski poziom świadomości występuje w stosunku do KSC-Krajowego Systemu Cyberbezpieczeństwa. Brakuje świadomości władz w zakresie istnienia w uczelniach procesów i mechanizmów bezpieczeństwa informacji. Stwierdzono niski poziom świadomości w zakresie szacowania ryzyka związanego z ochroną informacji.

Autor pracy w sposób syntetyczny podsumował wnioski z badań. Odniósł się w szczególny sposób do czynników wpływających na podjęcie decyzji o wdrożeniu mechanizmów ochrony wiedzy w uczelniach. Do czynników o charakterze pozytywnym zaliczył: wymogi prawne i ryzyko poniesienia kar umownych, potrzebę zapewnienia poufności danych, zapewnienie ciągłości działania uczelni, wyższe zabezpieczenie przed incydentami i sprawniejsze ich wykrywanie, samodzielność działu IT i Inspektora Ochrony Danych, utratę wizerunku.

Wśród barier wdrożenia mechanizmów ochrony wiedzy w uczelni Doktorant wskazał: jakość danych, brak rzetelnie zidentyfikowanych ryzyk lub instrumentalne podejście do procesu szacowania ryzyka, przeświadczenie, że analiza ryzyka i zaistniałych incydentów nie ma praktycznego znaczenia dla zmniejszenia ich występowania, niska praktyczna dbałość o wizerunek uczelni. Ponadto niepopularność i brak tradycji stosowania KRI i KSC (Krajowe Ramy Interoperacyjności, Krajowy System Cyberbezpieczeństwa), samoistne funkcjonowanie procesów ochrony danych, brak świadomości kontroli nad mechanizmami ochrony informacji, niska wiedza na temat wdrożonych już mechanizmów ochrony, wysokie koszty wdrożenia i brak ekonomicznego uzasadnienia, kultura organizacyjna uczelni, brak wykwalifikowanego personelu, brak potrzeby usprawniania procesów i poprawy efektywności funkcjonowania uczelni i uzyskania przewagi konkurencyjnej.

Uzyskane wyniki badań umożliwiają realizację celów postawionych przed praca.

Ocena realizacji celów badawczych:

Cztery cele szczegółowe i cel główny pracy zostały zrealizowane. Wykazano, że rola świadomości władz uczelni we wdrażaniu mechanizmów zarządzania bezpieczeństwem wiedzy jest niewielka w stosunku do standaryzowanych, wymaganych prawem, operacyjnych mechanizmów i narzędzi ochrony wiedzy. Badanie wykazało, że do wdrożenia holistycznego, strategicznego zarządzania bezpieczeństwem wiedzy taka świadomość jest niezbędna. Wskazana w pracy luka empiryczna została wypełniona. Wskazano także ograniczenia badawcze i kierunki dalszych badań (siedem problemów). Wskazano także kierunki dalszych badań i rekomendacje.

Podstawy teoretyczne pracy: praca została oparta na dobrych podstawach teoretycznych. Wykorzystana literatura jest aktualna, wystarczająca i odpowiednio dobrana oraz dobrze wykorzystana. Praca oparta została na 172 pozycjach literatury, w tym 96 czyli 55,8% stanowi literatura anglojęzyczna. Ponadto wykorzystano 36 aktów prawnych i 33 stron netografii. Percepcję treści pracy ułatwiają 35 tabel i 23 rysunki.

Problemy wymagające ustosunkowania się Autora pracy zawarto w następujących pytaniach:

Pyt. 1. Jak strategia ochrony wiedzy i strategii udostępniania wiedzy są ze sobą powiązane, w czym przejawia się istota paradoksu polegającego na wyróżnieniu dwóch przeciwstawnych strategii zarządzania wiedzą?
Pyt. 2. Jakie modele pomiaru kapitału intelektualnego funkcjonują w teorii i praktyce?
Pyt. 3. Jaka jest rola trójkąta wiedzy w opinii UE ?
Pyt. 4. Jaki jest stosunek przedstawicieli badanych uczelni do transferu wiedzy i technologii do przedsiębiorstw oraz usług doradztwa naukowego, jakie są przesłanki podjęcia takiej współpracy?
Pyt. 5. Jaka jest przydatność wyników badań dla uczelni objętych badaniem i dla pozostałych polskich uczelni?

Reasumpcja

1. Podjęty temat badawczy jest ważny, zarówno z teoretycznego, jak praktycznego punktu widzenia. Układ pracy umożliwił zrealizowanie celów pracy.
2. Praca pod względem merytorycznym i formalnym nie budzi zastrzeżeń
3. Struktura treści (część teoretyczna i praktyczna) sporządzona została prawidłowo.
4. Styl pisarski zaprezentowany w pracy jest poprawny.
5. Autor posiada rozwinięty warsztat badawczy umożliwiający samodzielne prowadzenie badań naukowych.
6. Terminologia stosowana w pracy jest odpowiednia dla nauk społecznych. Praca została oparta na dobrych podstawach teoretycznych.
7. Dobór literatury i sposób jej wykorzystania nie budzą zastrzeżeń i umożliwiają osiągnięcie celów postawionych przed pracą.
8. Cel pracy został w sposób jasny określony i w pełni zrealizowany. Wskazano i omówiono metody badawcze wraz z uzasadnieniem ich wyboru i stosowania. Nie sformułowano w pracy hipotezy badawczej.

9. Przedstawiona została procedura badań i narzędzie badawcze.
10. Przedstawiono sposób opracowania wyników badań. Wyniki badań przedstawiono w sposób poprawny i przejrzysty. Przedstawione wyniki badań służą rozszerzeniu wiedzy teoretycznej i zawierają wskazania praktyczne.
11. Praca doktorska prezentuje ogólną wiedzę teoretyczną Doktoranta w dyscyplinie nauki o zarządzaniu i jakości oraz dowodzi umiejętności samodzielnego prowadzenia badań naukowych. Autor w sposób oryginalny rozwiązał postawiony problem badawczy o charakterze naukowym.

Wniosek końcowy

Rozprawa doktorska mgr Piotra Szeflińskiego pt. „Zarządzanie bezpieczeństwem wiedzy w uczelniach publicznych" stanowi rozwiązanie problemu naukowego zawartego w tytule rozprawy. Autor zrealizował w pełni cele postawione przed pracą. Praca wnosi do podjętej problematyki nowe treści w sferze teoretycznej i metodycznej do dyscypliny Nauki o Zarządzaniu i Jakości. Przedłożona praca doktorska spełnia wymagania stawiane rozprawom doktorskim zawarte w Ustawie Prawo o szkolnictwie wyższym i nauce z dnia 20 lipca 2018 r. (t.j. Dz. U. 2023 r., poz. 742, z późn. zm.). W związku z tym wnoszę o jej przyjęcie przez Radę ds. Stopni Naukowych Wydziału Organizacji i Zarządzania Politechniki Łódzkiej w Łodzi oraz dopuszczenie do publicznej obrony.

Lublin, 15.10 2024

Elżbieta Skrzypek