Załącznik 3

AUTOREFERAT

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

dr inż. Paweł Kobis
Wydział Zarządzania
Politechnika Częstochowska

Częstochowa, grudzień 2021

1. Imię i nazwisko

Paweł Kobis

2. Posiadane dyplomy, stopnie naukowe lub artystyczne – z podaniem podmiotu nadającego stopień, roku ich uzyskania oraz tytułu rozprawy doktorskiej

1996-2001	Politechnika Częstochowska, Wydział Elektryczny Specjalność: Informatyka w Elektroenergetyce Temat pracy magisterskiej: „*Analiza inwestycji w zakresie ograniczenia emisji pyłu w elektrowniach*"
1998-2001	Politechnika Częstochowska Międzywydziałowe Studium Kształcenia Nauczycieli Przedmiotów Technicznych Fakultatywne Studia Pedagogiczne
2001-2003	Politechnika Częstochowska, Wydział Zarządzania Specjalność: Przedsiębiorczość i Rozwój Przedsiębiorstw Temat pracy magisterskiej: „*Nowoczesne technologie informatyczne w procesie usprawniania wymiany informacji w przedsiębiorstwie*"
2010	Akademia Górniczo-Hutnicza, Wydział Zarządzania Temat pracy doktorskiej: „*Wpływ Grupowych Systemów Wspomagania Decyzji na usprawnianie zarządzania dużymi przedsiębiorstwami*" Promotor: Prof. dr hab. inż. Leszek Kiełtyka Recenzenci: Prof. dr hab. Irena Hejduk Prof. dr hab. inż. Jan Tadeusz Duda Dr hab. Piotr Górski, prof. nadzw. AGH Uzyskany stopień naukowy: Doktor nauk ekonomicznych w dyscyplinie: nauki o zarządzaniu

3. Informacja o dotychczasowym zatrudnieniu w jednostkach naukowych lub artystycznych

Podstawowe miejsce pracy:

Lata	Miejsce pracy	Stanowisko	Miejsce
2001 – 2010	Katedra Informatycznych Systemów Zarządzania, Wydział Zarządzania, Politechnika Częstochowska	Asystent	Częstochowa
2010 – nadal	Katedra Informacyjnych Systemów Zarządzania (dawniej nazwa: Katedra Informatycznych Systemów Zarządzania), Wydział Zarządzania, Politechnika Częstochowska	Adiunkt	Częstochowa

Dodatkowe miejsca pracy:

Lata	Nazwa uczelni	Stanowisko	Miejsce
2001 – 2010	Wyższa Szkoła Hotelarstwa i Turystyki	Asystent	Częstochowa
2010 – 2013	Wyższa Szkoła Hotelarstwa i Turystyki	Adiunkt	Częstochowa
2002 – 2003	Wyższa Szkoła Zarządzania	Asystent	Częstochowa
2016 – 2018	Wyższa Szkoła Biznesu	Adiunkt	Dąbrowa Górnicza
2005 – 2007	Wyższa Szkoła Ekonomii i Administracji im. Prof. Edwarda Lipińskiego	Asystent	Kielce
2007 – 2010	Wyższa Szkoła Ekonomii i Prawa im. Prof. Edwarda Lipińskiego	Asystent	Kielce
2010 – 2013	Wyższa Szkoła Ekonomii i Prawa im. Prof. Edwarda Lipińskiego	Adiunkt	Kielce

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

Za swoje najważniejsze osiągnięcie naukowe uważam monografię:

Paweł Kobis, *Zarządzanie bezpieczeństwem informacji w systemach informacyjnych małych i średnich przedsiębiorstw z uwzględnieniem czynnika ludzkiego*, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, Toruń 2021, ISBN: 978-83-7285-944-0,

Recenzenci wydawniczy:

Dr hab. inż. Janusz Zawiła-Niedźwiecki, prof. uczelni - *Politechnika Warszawska*
Dr hab. Mirosław Kwieciński, prof. uczelni – *Krakowska Akademia im. Andrzeja Frycza Modrzewskiego*

Monografia jest rezultatem mojego wieloletniego zainteresowania i badań nad zagadnieniami zarządzania bezpieczeństwem informacji ze szczególnym uwzględnieniem czynnika ludzkiego jako aspektu, który w świetle współczesnej literatury naukowej stanowi najważniejszy czynnik powodujący zagrożenia dla zasobów niematerialnych w podmiotach gospodarczych.

4.1. Syntetyczne ujęcie treści poszczególnych rozdziałów monografii

Monografia składa się z pięciu rozdziałów, w tym:

- trzech rozdziałów teoretycznych w których dokonano krytycznej analizy bibliografii z zakresu zarządzania informacją, zarządzania bezpieczeństwem informacji, kompetencji pracowniczych, kompetencji na stanowisku pracy, aktualnych badań i opracowań na temat wpływu czynnika ludzkiego na zagrożenia zasobów niematerialnych oraz aktualnych badań dotyczących analiz ryzyka w procesach zarządzania informacją uwzględniających wpływ człowieka. Analizując zagadnienia dotyczące bezpieczeństwa informacji i wpływu człowieka na to bezpieczeństwo, w monografii przyjęto podział osób związanych z zarządzaniem zasobami informacyjnymi na: pracowników, klientów, partnerów biznesowych oraz osoby trzecie jako potencjalnych uczestników procesów przetwarzania, przechowywania i wymiany informacji. Rozdziały teoretyczne zawierają również autorskie opracowania modeli,

schematów, struktur i zestawień dotyczących poszczególnych obszarów zarządzania informacją oraz jej bezpieczeństwa w świetle współczesnych cyberzagrożeń. W części teoretycznej wypracowano również autorską definicję czynnika ludzkiego w bezpieczeństwie informacji.

- Dwóch rozdziałów empirycznych zawierających, celem weryfikacji hipotezy badawczej, cel badawczy oraz cele aplikacyjne, wyniki badań zrealizowanych na terenie Polski wśród małych i średnich przedsiębiorstw oraz projekt Podsystemu Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji (Podsystemu ZPABI) w ujęciu funkcjonalnym i przedmiotowym, na płaszczyźnie przedmiotowej i podmiotowej. Rozdziały zawierają również opis modelu oceny dojrzałości bezpieczeństwa informacji w aspekcie funkcjonowania Podsystemu ZPABI oraz ocenę proponowanego Podsystemu Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji.

Analizując zawartość poszczególnych rozdziałów z uwzględnieniem własnych dokonań badawczych, przedstawiono poniżej syntetyczne ich ujęcie.

W rozdziale pierwszym, zatytułowanym: *Zarządzanie informacją i systemy zarządzania informacją w przedsiębiorstwach*, przedstawiono podstawowe pojęcia związane z zasobami niematerialnymi funkcjonującymi w przedsiębiorstwach. Określono pojęcie jakości informacji oraz jej podstawowe cechy. Przybliżono pojęcie informacji zarządczej oraz przeciążenia informacyjnego (information overload), które w literaturze można znaleźć już od dziesięcioleci, ale nigdy w takim wymiarze, jak występuje to obecnie. Wyjaśniono pojęcie zarządzania informacją zarówno w ujęciu definicyjnym, jak i w aspekcie obszaru zarządzania i wpływu czynnika ludzkiego. Scharakteryzowano systemy stanowiące narzędzia dla zarządzania informacją w przedsiębiorstwach. Dokonano porównania systemu informacyjnego i systemu informatycznego. System informatyczny opisano, dzieląc go na trzy główne warstwy:

1) warstwę komunikacyjną;
2) warstwę sprzętową;
3) warstwę programową.

Charakterystyka tych trzech warstw pozwoliła na kompleksowe spojrzenie na system w aspekcie sposobu zarządzania informacją, a przez to możliwość łatwiejszego zrozumienia i przyswojenia mechanizmów zarządzania ryzykiem opisanym w rozdziale drugim. Opisano również strukturę modelu chmury obliczeniowej jako alternatywnego, nowoczesnego rozwiązania do przetwarzania zasobów informacyjnych.

W ostatnim podrozdziale podjęto próbę scharakteryzowania aspektów pozatechnicznych zarządzania informacją. Autorski, czteropłaszczyznowy podział analizy tego zjawiska ma za zadanie nakreślenie obszaru, w jakim należy się poruszać, analizując następnie zagadnienia związane z bezpieczeństwem informacji.

W rozdziale drugim, zatytułowanym: *Bezpieczeństwo informacji w systemach informacyjnych na płaszczyźnie technicznej oraz czynnika ludzkiego*, scharakteryzowano pojęcie bezpieczeństwa informacji wraz z określeniem płaszczyzn jego funkcjonowania. Określono atrybuty bezpieczeństwa oraz podstawowe jego składniki. Zaprezentowano kompleksowe autorskie ujęcie bezpieczeństwa informacji w systemie informatycznym uwzględniające opisane w rozdziale pierwszym poszczególne warstwy systemu informatycznego oraz czynnik ludzki. Opisano elementy funkcjonalne zapewniające bezpieczeństwo informacji, wyszczególniając wszystkie najpopularniejsze rozwiązania ochrony zasobów niematerialnych funkcjonujące w przedsiębiorstwach, stanowiące punkt wyjścia w realizacji analizy ryzyka. Przedstawiono kategorie zagrożeń informacji, podając warunki ich prawidłowej klasyfikacji. Opisano zagrożenia zewnętrzne i wewnętrzne oraz przedstawiono ich najpopularniejsze podziały definiowane przez badaczy w literaturze przedmiotu. Zaprezentowano autorski podział na rodzaje oraz wzajemne relacje zagrożeń informacji. Szczegółowo opisano najważniejsze działania, jakie należy realizować w przedsiębiorstwach celem minimalizacji zagrożenia – zarządzanie ryzykiem w procesach zarządzania bezpieczeństwem informacji. Wszystkie rozważania analizowano, wykorzystując normę ISO/IEC 27005, będącą wyznacznikiem prawidłowego postępowania podczas zarządzania ryzykiem w organizacji gospodarczej. Scharakteryzowano metody szacowania ryzyka z wyszczególnieniem tych, które pozwalają uwzględniać czynnik ludzki. Przedstawiono wykorzystanie Analizy Niezawodności Człowieka obejmującej wykorzystanie jakościowych i ilościowych metod oceny ludzkiego wkładu do ryzyka z pominięciem awarii komponentu fizycznego dla opracowania nowych metod zarządzania ryzykiem uwzględniających czynnik ludzki w bezpieczeństwie informacji. Opisano politykę bezpieczeństwa informacji wraz z przedstawieniem przykładowej struktury polityk funkcjonujących w przedsiębiorstwach i wspierających ich misję i cele. Scharakteryzowano klasyczny System Zarządzania Bezpieczeństwem Informacji i zaprezentowano jego hierarchiczną strukturę, która następnie w rozdziale 5 stanowi fundament dla implementacji opracowanego podsystemu.

W rozdziale trzecim, zatytułowanym: *Człowiek w procesie zarządzania bezpieczeństwem informacji*, opisano pojęcie czynnika ludzkiego w procesie zarządzania bezpieczeństwem informacji. Scharakteryzowano podejście szerokie oraz wąskie w postrzeganiu zespołu cech

i zachowań ludzkich, prezentując definicje proponowane przez badaczy zarówno w kraju, jak i na świecie. Zaproponowano również własną, autorską definicję pojęcia. Opisano zagrożenia dla informacji ze strony działań człowieka, prezentując rodzaje błędów ludzkich oraz dokładny ich opis wraz z praktycznymi przykładami zagrożeń mogącymi potencjalnie wystąpić podczas zarządzania informacją w przedsiębiorstwie. W sposób schematyczny i opisowy pokazano relacje międzyludzkie w aspekcie zagrożeń powodowanych czynnikiem ludzkim, uwzględniając osoby, które w jakikolwiek sposób mają lub mogą mieć dostęp do zasobów informacyjnych przedsiębiorstwa. Przedstawiono przykładowe motywacje osób stwarzających zagrożenie w cyberprzestrzeni oraz najczęstsze formy, jakie przybierają metody socjotechniczne stosowane przez cyberprzestępców. Wyszczególniono rozwiązania organizacyjne funkcjonujące w przedsiębiorstwach na tle zagrożeń dla informacji płynących z celowych i przypadkowych negatywnych działań człowieka. Opisano tym samym telepracę, pracę zdalną, pracę w modelu chmury obliczeniowej, zjawisko BYOD (Bring Your Own Device) oraz funkcjonowanie zespołów wirtualnych. Przedstawione zostało pojęcie kompetencji jako to, które bezpośrednio wpisuje się w aspekt wpływu czynnika ludzkiego na bezpieczeństwo informacji. Scharakteryzowano wybrane kompetencje w organizacji gospodarczej, przedstawiono relacje pojęć kwalifikacji i kompetencji. Wyszczególniono kryteria definiowania kompetencji. Opisano kompetencje na stanowisku pracy, kompetencje pracownicze, określając je za pomocą tzw. modelu holistycznego, w którym wyróżniono kompetencje społeczne, kompetencje poznawcze, kompetencje funkcjonalne i metakompetencje. Określono zbiór kompetencji w obszarze bezpieczeństwa informacji w przedsiębiorstwach. Rozpatrzono je w trzech obszarach: kompetencji cyfrowych, kompetencji związanych ze stanowiskiem pracy oraz kompetencji osobistych. Na podstawie powyższych rozważań i wyszczególnionych zbiorów kompetencji opracowano autorski zbiór kompetencji mających wpływ na bezpieczeństwo zasobów niematerialnych. Przedstawiono sposoby ograniczania negatywnego wpływu czynnika ludzkiego w procesach zarządzania informacją. Opisano trzy etapy, okresy funkcjonowania relacji pracownik-przedsiębiorstwo w aspekcie zapewnienia bezpieczeństwa dla zasobów informacyjnych.

W rozdziale czwartym, zatytułowanym: *Bezpieczeństwo informacji z uwzględnieniem czynnika ludzkiego wśród polskich przedsiębiorstw sektora MSP w świetle własnych badań empirycznych*, przedstawiono badania własne przeprowadzone w grupie małych i średnich przedsiębiorstw w Polsce. Badania dotyczyły rozpoznania funkcjonującego w przedsiębiorstwach zaplecza IT, kreującego potencjalne ryzyka wystąpienia zagrożeń z uwzględnieniem czynnika ludzkiego, określenia wiedzy, doświadczenia i świadomości osób

zarządzających bezpieczeństwem informacji w zakresie ochrony zasobów niematerialnych z uwzględnieniem czynników pozatechnicznych, analizę zabezpieczeń funkcjonujących w organizacjach gospodarczych. Nakreślono cele badawcze, które następnie zrealizowano za pomocą analizy wyników badań. Na podstawie sformułowanych celów postawiono hipotezę badawczą, którą poddano weryfikacji. Na podstawie przeprowadzonych badań empirycznych sformułowano następnie dwa główne wnioski podsumowujące przeprowadzoną analizę i potwierdzające postawioną hipotezę.

W rozdziale piątym, zatytułowanym: *Podsystem Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji*, przedstawiono koncepcję podsystemu będącego rozszerzeniem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Opisano umiejscowienie Podsystemu Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji w przedsiębiorstwach, jego zależność od SZBI. Przedstawiono hierarchiczną strukturę bezpieczeństwa informacji uwzględniającą Podsystem Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji (Podsystem ZPABI). Scharakteryzowano podsystem w ujęciu funkcjonalnym, opisując kluczowe działania minimalizujące zagrożenie informacji z powodu czynnika ludzkiego w podziale na etapy relacji pracownik-przedsiębiorstwo w ramach Podsystemu ZPABI oraz w relacjach przedsiębiorstwo-klient, przedsiębiorstwo-partner biznesowy i przedsiębiorstwo-osoby trzecie. Scharakteryzowano podsystem w ujęciu przedmiotowym, wyszczególniając i opisując jego składniki materialne i niematerialne. Opisano koordynację pracy podsystemu, analizując poszczególne płaszczyzny współdziałania pracowników organizacji między sobą oraz z osobami odpowiedzialnymi za bezpieczeństwo informacji. Wyjaśniono proces implementacji i funkcjonowania podsystemu na płaszczyźnie przedmiotowej i podmiotowej. Uwzględniono tym samym wszystkie elementy materialne, niematerialne podsystemu oraz składniki systemu informacyjnego przedsiębiorstwa i osoby mające jakikolwiek wpływ na bezpieczeństwo informacji. Obie płaszczyzny przedstawiono również w postaci graficznej (schematu) z dokładnym usytuowaniem poszczególnych elementów i powiązań między nimi. Podsystem przedstawiono również w ujęciu kompleksowym ukazującym połączenia między płaszczyznami a Systemem ZBI. W dalszej kolejności zaproponowano autorski model oceny dojrzałości bezpieczeństwa informacji w aspekcie funkcjonowania Podsystemu ZPABI bazujący na wybranych założeniach modelu CMMI (Capability Maturity Model Integration). W ostatnim podrozdziale dokonano oceny zaproponowanego podsystemu.

4.2. Uzasadnienie podjęcia tematu

Obecnie informacja stanowi determinantę rozwoju przedsiębiorstw. W epoce organizacji wirtualnych można zaryzykować stwierdzenie, że jest czynnikiem najważniejszym. Świadczy o potencjale rozwoju każdego przedsiębiorstwa. Jest miarą ich konkurencyjności. Zarządzanie zasobami informacyjnymi koncentruje w sobie kluczowe procesy funkcjonowania każdego podmiotu gospodarczego.

Informacja, będąc strategicznym zasobem przedsiębiorstw, stała się jednocześnie najbardziej pożądanym zasobem dla osób chcących nielegalnie ją pozyskać lub zniszczyć. Stała się więc zasobem, który należy chronić. Przez kolejne lata rozwoju technik i technologii można było zauważyć wzrost liczby zagrożeń pojawiających się w sieci globalnej. Postęp w obszarze komunikacji i informatyki pozwalał na opracowywanie coraz skuteczniejszych metod łamania zabezpieczeń. Technologia dawała cyberprzestępcom coraz nowsze narzędzia do przeprowadzania ataków na sieci wewnętrzne przedsiębiorstw. Równolegle opracowywano coraz bardziej skomplikowane metody ochrony, które z mniejszą lub większą skutecznością eliminowały potencjalne zagrożenia. Specyficzny „wyścig zbrojeń" między stronami tworzącymi skuteczne zabezpieczenia dla informacji a stronami starającymi się je pokonać trwa do dziś. Poziom skomplikowania narzędzi ochrony informacji jest już jednak na tyle duży, że próby łamania dobrze skonfigurowanych zabezpieczeń coraz częściej kończą się dla agresorów niepowodzeniem. Dlatego obserwuje się wzrost prób nielegalnego pozyskania informacji poprzez wykorzystanie innego, najsłabszego „elementu" każdego systemu: człowieka. Próby te bazują na błędach popełnianych przez pracowników w procesie zarządzania informacją powodowanych zbiorem czynników wynikających z kompetencji, doświadczenia, zbiorem zachowań o podłożu celowym lub przypadkowym oraz wpływem działań socjotechnicznych ze strony potencjalnego agresora. Wszystkie te czynniki w literaturze przedmiotu określane są jako „czynniki ludzkie".

Pojęcie czynnika ludzkiego było obecne i rozpatrywane w literaturze naukowej w różnych kontekstach. Było utożsamiane z różnymi obszarami działalności w ramach funkcjonowania przedsiębiorstw, począwszy od znaczenia relacji międzyludzkich na stanowiskach pracy, problemami ergonomii pracy, problemami bezpieczeństwa pracy aż po czasy współczesne, w których pojawia się w publikacjach z zakresu zarządzania zasobami ludzkimi, zarządzania kapitałem ludzkim oraz z zakresu przedmiotowej monografii: bezpieczeństwa zasobów informacyjnych. Bez względu jednak na kontekst czynnik ludzki zawsze dotyczył zachowania człowieka, jego mocnych stron i słabości, jego wiedzy i doświadczenia, podatności

i kompetencji. Podmiot był zatem zawsze ten sam, zmieniał się tylko przedmiot jego rozpatrywania.

Obecnie pojęcie czynnika ludzkiego pojawia się coraz częściej w obszarze zagadnień dotyczących ochrony zasobów informacyjnych przedsiębiorstw. Publikowane corocznie badania, zarówno przez jednostki naukowe, jak i największe wywiadownie na świecie oraz organizacje międzynarodowe zajmujące się cyberbezpieczeństwem pokazują, że czynnik ludzki jest obecnie przyczyną większości naruszeń bezpieczeństwa zasobów niematerialnych w organizacjach.

Nowe sposoby prób nielegalnego pozyskiwania informacji wykorzystujące czynniki ludzkie i bazujące na technikach inżynierii społecznej wymagają od przedsiębiorstw stanowczych działań w obszarze zmiany funkcjonowania Systemów Zarządzania Bezpieczeństwem Informacji (SZBI). Obecny kształt tych systemów oraz wykorzystywane w ramach ich funkcjonowania narzędzia nie są w stanie zapewnić należytej ochrony zasobom niematerialnym. W określonych przypadkach stają się bezużyteczne. Istnieje potrzeba opracowywania nowych sposobów zarządzania bezpieczeństwem informacji, nastawionych przede wszystkim na działania człowieka. Trzeba w procedurach zarządzania ryzykiem uwzględniać wszystkie osoby, grupy osób, które w jakimkolwiek stopniu narażają informację na niebezpieczeństwo. Są to zarówno pracownicy przedsiębiorstw, jak i ich klienci, partnerzy biznesowi oraz wszystkie osoby trzecie, które przez jakiekolwiek działania naruszają jej główne elementy bezpieczeństwa, tzw. CIA triad:

- poufność (Confidentality) – dostępność informacji tylko dla osób do tego upoważnionych;
- spójność (Integrity) – własność wykluczająca wprowadzenie zmian do informacji w sposób nieautoryzowany;
- dostępność (Availability) – dostęp do informacji tylko w sposób określony w polityce bezpieczeństwa.

W literaturze przedmiotu występują również oprócz powyższej trójki elementy:

- rozliczalności (Accountability) charakteryzujący się możliwością przypisania określonych działań na zasobach informacyjnych konkretnej osobie w danym czasie;
- niezaprzeczalności (Non-repudiation) określający brak możliwości zaprzeczenia określonej informacji;
- autentyczności (Authenticity), czyli pewności co do pochodzenia informacji.

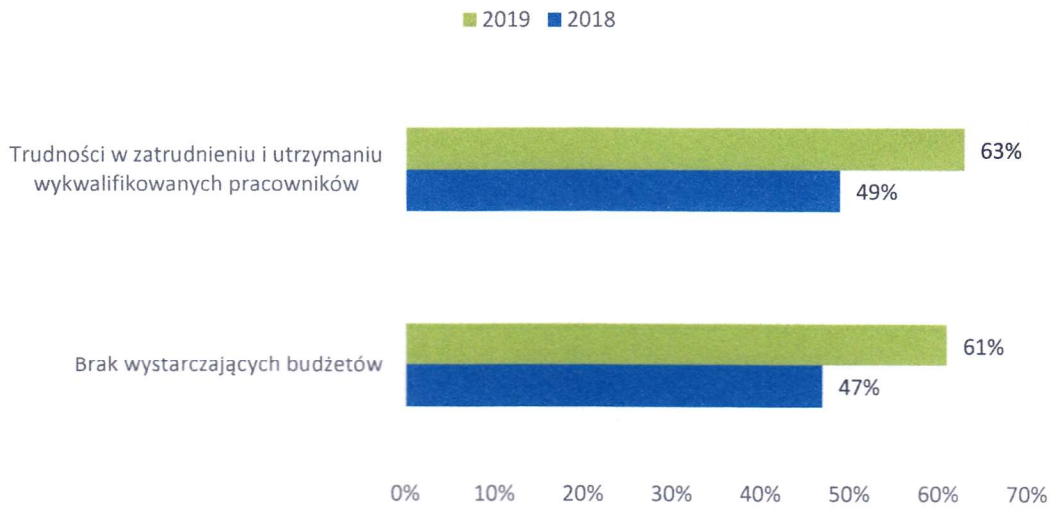
Tylko podejście synergiczne łączące ze sobą tradycyjne metody ochrony informacji oraz metody minimalizujące wpływ czynnika ludzkiego na powstawanie zagrożeń mogą zapewnić organizacji gospodarczej maksymalnie możliwe bezpieczeństwo zasobów niematerialnych.

Tymczasem w literaturze przedmiotu brak jednolitego podejścia do aspektów ochrony informacji przed działaniami powodowanymi czynnikiem ludzkim. Nie ma kompleksowych rozwiązań podejmujących próby chociażby przeciwdziałania inżynierii społecznej, wpływom socjotechnicznym na pracowników, ograniczających zarówno celowe, jak i przypadkowe działania szkodzące zasobom informacyjnym. Brak jest rozwiązań wewnątrzorganizacyjnych, przeciwdziałających ryzykownym zachowaniom pracowników, zarówno celowym, jak i wynikającym z braku doświadczenia, kompetencji, wiedzy. Tym bardziej nie ma rozwiązań, które łączyłyby zabezpieczenia tradycyjne z zabezpieczeniami przed działaniami pozatechnicznymi. Istniejące rozwiązania traktują problem pobieżnie, podejmując implementacje zabezpieczeń jedynie w określonych obszarach całego spektrum zagrożeń powodowanych przez człowieka. Nie proponują ochrony informacji w odniesieniu do całości zasobów przedsiębiorstw. Opracowana monografia ma za zadanie wypełnić tę lukę.

W literaturze naukowej można spotkać opracowania traktujące zarówno aspekt kompetencji pracowniczych, jak i odpowiedniego traktowania pracownika od dnia rekrutacji aż po okres zakończenia pracy na płaszczyźnie minimalizowania utraty i zniszczenia informacji. Można spotkać opracowania dotyczące inżynierii społecznej, socjotechnik wraz z próbą opisania sposobów na ich niwelowanie w pracy przedsiębiorstw. Istnieją próby adaptacji istniejących rozwiązań z innych dziedzin do ochrony zasobów niematerialnych. Można wreszcie znaleźć obszerne opracowania o zagrożeniach sieciowych, szczególnie w obszarze sieci Internet. Trudno jednak spotkać kompleksowe podejście do istniejącego problemu. Podejście, które w sposób systemowy podjęłoby próbę stworzenia rozwiązania chroniącego organizacje, w tym gospodarcze, przed współczesnymi sposobami nielegalnego pozyskiwania i prób niszczenia informacji.

Czynnik ludzki stanowi największe wyzwanie dla przedsiębiorstw w zapewnieniu oczekiwanego poziomu zabezpieczeń, a brak wykształconej kadry jest większym problemem w zbudowaniu skutecznego systemu ochrony niż zbyt mały budżet podmiotów gospodarczych (rys. 1). Człowiek jest „nieprogramowalnym elementem systemu", trudno przewidzieć jego zachowanie w procesie zarządzania informacją oraz w obliczu wystąpienia określonego incydentu. Nie jest zaprogramowany tak jak wybrane aplikacje o charakterze ochronnym lub rozwiązania sprzętowe, których wynik działania możemy przewidzieć. Działania podejmowane przez człowieka mają bardzo często stochastyczny wpływ na funkcjonowanie systemu. Są one

nieprzemyślane, przypadkowe, podyktowane emocjami i wykonywane bez należytej uwagi i często „podszyte" brakiem wiedzy i doświadczenia. Wszystkie te „niedoskonałości" wykorzystywane są przez osoby, których celem jest zniszczenie lub nieuprawnione pozyskanie informacji. Jak wynika z danych publikowanych przez szereg firm zajmujących się bezpieczeństwem informacji, ataki przeprowadzane przez specjalnie przygotowane do tego celu roboty i aplikacje internetowe wykorzystujące czynnik techniczny (np. luki systemowe) są coraz rzadsze, a zastępują je ataki, w których interakcja międzyludzka jest kluczowa. Instynkt ciekawości i zaufania, prowadzący osoby o dobrych intencjach do klikania, instalowania, otwierania i wysyłania informacji, jest wykorzystywany przez cyberprzestępców coraz bardziej doskonalących swoje umiejętności w posługiwaniu się technikami inżynierii społecznej [1].



Rys. 1. Najczęściej występujące ograniczenia w możliwości uzyskania oczekiwanego poziomu zabezpieczeń w organizacji gospodarczej

Źródło: opracowanie własne na podstawie raportu KPMG[2]

Aby przeciwdziałać zagrożeniom informacji, w których człowiek jest kluczowym „elementem" powodującym ryzyko ich wystąpienia, należy stworzyć koncepcję rozwiązania systemowego. Próba stworzenia takiej koncepcji była inspiracją do napisania przedmiotowej monografii. Głównym motywem podjęcia tematu pracy była próba zespolenia podejść w aspekcie ochrony zasobów niematerialnych zarówno od strony technicznej, jak i strony

[1] Exclusive Networks (2019), *Proofpoint - human factor report 2019*, https://www.exclusive-networks.com/se/proofpoint-human-factor-report-2019/, access date: 20.12.2021.

[2] KPMG (2019), *Barometr cyberbezpieczeństwa. W obronie przed cyberatakami*, https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-KPMG-Barometr-Cyberbezpieczenstwa-W-obronie-przed-cyberatakami.pdf, s. 5, data dostępu: 20.12.2021 r.

czynnika ludzkiego. Opracowany Podsystem Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji (Podsystem ZPABI) w przedsiębiorstwach, będący wynikiem badań literaturowych, badań empirycznych, wpisuje się w obszar wielowymiarowych działań dotyczących ochrony informacji i stanowi unikalne, według mojej opinii, podejście uwzględniające oprócz rozwiązań technicznych również aspekty czynnika ludzkiego.

Opracowana monografia wpisuje się w obszar zagadnień związanych z zarządzaniem informacją, a w szczególności zarządzania bezpieczeństwem informacji.

4.3. Cel badawczy, częściowe cele badawcze, cele aplikacyjne, hipoteza badawcza

Na podstawie analizowanych w literaturze przedmiotu obszarów problemowych dotyczących zarządzania bezpieczeństwem informacji z uwzględnieniem czynnika ludzkiego oraz przyjętych założeń badawczych nakreślono cel badawczy monografii:

Podstawowym celem badawczym monografii 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.

Na podstawie tak sformułowanego celu badawczego, badań literaturowych, analizy teoriopoznawczej oraz badań obcych dla jego realizacji postawiono również częściowe cele badawcze:

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.

Obok celów badawczych postawiono dwa cele aplikacyjne:

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

Na podstawie tak sformułowanych celów badawczych postawiono następującą hipotezę badawczą, którą poddano weryfikacji:

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.

4.4. Syntetyczny opis metod badawczych i populacji badawczej oraz wyniki badań

Do realizacji badań przyjętymi technikami badawczymi były bezpośredni wywiad kwestionariuszowy F2F (Face to Face) z użyciem komputera (CAPI – Computer Aided Personal Interview), który w części przypadków został zastąpiony wywiadem realizowanym przez komunikatory internetowe pozwalające na bezpośredni, naturalny kontakt audiowizualny z respondentem z zachowaniem obowiązujących zasad przeprowadzania badania, oraz technika CAWI (Computer-Assisted Web Interview). Zastosowano tym samym tzw. tryb mieszany (Mixed-Mode). W obu technikach użyto tego samego kwestionariusza. Implementacja narzędzi informatycznych była konieczna i wynikała w większości przypadków z ograniczonego czasu respondentów oraz z odległości geograficznej dzielącej autora badań z respondentem.

Badania przeprowadzone zostały w dwóch etapach:

1) Etap pierwszy (główny) w okresie od listopada 2018 roku do września 2019 roku wśród małych i średnich przedsiębiorstw w Polsce.
2) Etap drugi, mający na celu ocenę opracowanego systemu, przeprowadzono w miesiącach styczniu i lutym 2020 roku.

Wybór przedsiębiorstw do badań głównych był realizowany w trzech etapach.

W pierwszym etapie liczba przedsiębiorstw została określona na podstawie zależności:

$$N_{min} = \frac{P(1-P)}{\frac{e^2}{z^2} + \frac{P(1-P)}{N}}$$

Gdzie:

N_{min} – minimalna próba badawcza – najmniejsza możliwa liczba przedsiębiorstw do przeprowadzenia badania;

N – wielkość populacji generalnej;

c – maksymalny błąd oszacowania;

z – wartość wynikająca z przyjętego poziomu ufności (α), obliczana za pomocą dystrybuanty rozkładu normalnego. Dla 95% poziomu ufności z=1,96;

P – szacowana wielkość frakcji.

Do obliczeń przyjęto wartość N= 69 098 (53 763 przedsiębiorstwa małe i 15 335 przedsiębiorstwa średnie). Jest to liczba małych i średnich przedsiębiorstw niefinansowych podana przez Główny Urząd Statystyczny za rok 2017. Dokonując podziału przedsiębiorstw, uwzględniono liczbę zatrudnionych osób (10-49 pracowników to przedsiębiorstwa małe i 50-249 to przedsiębiorstwa średnie). Dane nie obejmowały: rolnictwa, leśnictwa, łowiectwa i rybactwa (sekcja A według PKD 2007), działalności finansowej i ubezpieczeniowej (sekcja K według PKD 2007); szkół wyższych; samodzielnych publicznych zakładów opieki zdrowotnej; instytucji kultury posiadających osobowość prawną oraz organizacji członkowskich (GUS, 2018a).

Maksymalny błąd oszacowania przyjęto na poziomie 5%, co jest wartością ogólnie dopuszczalną przy badaniach naukowych. Wartość szacowanej wielkości frakcji (P) określa procentową liczbę badanej populacji, u której przewidujemy wystąpienie badanej cechy. Jako że przedmiotem badań są zagadnienia dotyczące bezpieczeństwa informacji oraz czynnika ludzkiego wpływającego na to bezpieczeństwo, przyjęto, że u większości badanych przedsiębiorstw cecha ta występuje (większość przedsiębiorstw informacją zarządza). W badaniach ujętych w monografii przyjęto wartość równą 60%. Jest to poziom wartości z dużym prawdopodobieństwem spełniający wymogi badania. Poziom ufności uzyskania właściwych rezultatów został oszacowany na 95%.

Na podstawie przyjętych, wymienionych powyżej wartości uzyskano wynik 367 przedsiębiorstw, w których należy przeprowadzić badania.

W kolejnym etapie wyodrębniania podmiotów gospodarczych do badań zastosowano dobór kwotowy. Wartościami wejściowymi dla doboru kwotowego były dane Głównego Urzędu Statystycznego przedstawiające liczbę funkcjonujących małych i średnich przedsiębiorstw w poszczególnych województwach Polski w roku 2017. Wyniki przedstawiono w tabeli 1.

Tabela 1. Dobór kwotowy grupy badawczej

Województwo	Przedsiębiorstwa małe			Przedsiębiorstwa średnie		
	Liczba w 2017 roku	Udział procentowy	Liczba do badań	Liczba w 2017 roku	Udział procentowy	Liczba do badań
Dolnośląskie	3914	5,7%	21	1126	1,6%	6
Kujawsko-pomorskie	2730	4,0%	14	793	1,1%	4
Lubelskie	2397	3,5%	13	536	0,8%	3
Lubuskie	1283	1,9%	7	405	0,6%	2
Łódzkie	3339	4,8%	18	952	1,4%	5
Małopolskie	5566	8,1%	30	1358	2,0%	7
Mazowieckie	8313	12,0%	44	2686	3,9%	14
Opolskie	1251	1,8%	7	326	0,5%	2
Podkarpackie	2778	4,0%	15	720	1,0%	4
Podlaskie	1317	1,9%	7	374	0,5%	2
Pomorskie	3308	4,8%	18	996	1,4%	5
Śląskie	7011	10,1%	37	1 900	2,7%	10
Świętokrzyskie	1403	2,0%	7	363	0,5%	2
Warmińsko-mazurskie	1426	2,1%	8	461	0,7%	2
Wielkopolskie	5639	8,2%	30	1739	2,5%	9
Zachodniopomorskie	2088	3,0%	11	600	0,9%	3
SUMA	**53 763**	**77,8%**	**287**	**15 335**	**22,2%**	**80**

Źródło: obliczenia własne na podstawie danych z GUS

Na podstawie liczby przedsiębiorstw w poszczególnych województwach określono ich udział procentowy w stosunku do całej populacji małych i średnich przedsiębiorstw w Polsce. Następnie na podstawie udziału procentowego wyliczono liczbę przedsiębiorstw do badań dla każdego województwa, przyjmując wartość 100% dla obliczonej wcześniej grupy badawczej 367 organizacji gospodarczych. Wartość „Liczba do badań" uzyskano poprzez zaokrąglenie otrzymanego wyniku do najbliższej liczby całkowitej. Uzyskano w ten sposób rozkład grupy badawczej proporcjonalny do rzeczywistego rozkładu małych i średnich przedsiębiorstw niefinansowych w województwach polskich.

W kolejnym (ostatnim) kroku wygenerowano w poszczególnych lokalizacjach określone grupy przedsiębiorstw z użyciem metody doboru celowego. Jedynym przyjętym kryterium (oprócz wielkości przedsiębiorstwa) było przetwarzanie większości zasobów informacyjnych w postaci cyfrowej.

Badaniem objęte zostały osoby, które w podmiotach gospodarczych miały największą wiedzę z zakresu bezpieczeństwa informacji oraz które bezpośrednio były zaangażowane w procesy ustanawiania i aktualizowania polityki bezpieczeństwa w organizacji. Tym samym były to takie

osoby, jak: szefowie działów IT, pracownicy działów IT, osoby specjalnie (etatowo lub w części etatu) zajmujące się bezpieczeństwem cyfrowych zasobów informacyjnych, prezesi, dyrektorzy, właściciele i współwłaściciele. W badaniu udział wzięło 268 mężczyzn i 99 kobiet mających wykształcenie: średnie (114 osób), wyższe I stopnia (74 osoby), wyższe II stopnia (175 osób) oraz wyższe III stopnia (4 osoby) (tab. 2). Wszystkie badane osoby deklarowały posiadanie wiedzy i doświadczenia w zakresie bezpieczeństwa informacji na podstawie zdobytego wykształcenia, przebytych kursów, szkoleń, wieloletniego stażu pracy.

Tabela 2. Stanowiska i wykształcenie respondentów z podziałem na wielkość przedsiębiorstw

Stanowisko w przedsiębiorstwie	**Wykształcenie**	**Wielkość przedsiębiorstwa**	
		Małe (n = 287)	**Średnie (n = 80)**
Prezes, wiceprezes, dyrektor, właściciel, współwłaściciel	Średnie	47	0
	Wyższe I stopnia (inżynier, licencjat)	40	0
	Wyższe II stopnia (magisterium)	107	0
	Wyższe III stopnia (doktorat)	2	0
Szef działu IT, pracownik działu IT, osoba zajmująca się w firmie bezpieczeństwem cyfrowych zasobów informacyjnych	Średnie	31	36
	Wyższe I stopnia (inżynier, licencjat)	20	14
	Wyższe II stopnia (magisterium)	40	28
	Wyższe III stopnia (doktorat)	0	2

Źródło: opracowanie własne

Przedmiot prowadzonej działalności w badanych organizacjach gospodarczych i ich zasięg działania w podziale na przedsiębiorstwa małe i średnie przedstawiono w tabeli 3.

Tabela 3. Podział przedsiębiorstw według przedmiotu prowadzonej działalności

Przedmiot prowadzonej działalności przedsiębiorstwa	**Zasięg działania przedsiębiorstwa**	**Wielkość**		**Suma końcowa**
		małe	**średnie**	
Produkcja	Lokalny	2	0	2
	Regionalny	2	0	2
	Ogólnopolski	10	10	20
	Międzynarodowy	27	15	42
Suma dla działalności produkcyjnej		**41**	**25**	**66**
Handel	Lokalny	6	0	6
	Regionalny	7	0	7
	Ogólnopolski	17	6	23

	Międzynarodowy	12	0	12
Suma dla działalności handlowej		**42**	**6**	**48**
Usługi	Lokalny	67	0	67
	Regionalny	37	1	38
	Ogólnopolski	45	19	64
	Międzynarodowy	11	6	17
Suma dla działalności usługowej		**160**	**26**	**186**
Mieszany	Lokalny	6	0	6
	Regionalny	4	0	4
	Ogólnopolski	13	6	19
	Międzynarodowy	21	17	38
Suma dla działalności mieszanej		**44**	**23**	**67**
Suma końcowa		**287**	**80**	**367**

Źródło: opracowanie własne

Podczas przeprowadzania badań wszystkie terminy informatyczne, pojawiające się nazwy własne, zagadnienia, sformułowania pytań budzące jakiekolwiek wątpliwości u respondentów były na bieżąco korygowane i tłumaczone. Tym samym wystąpienie potencjalnych błędów spowodowanych niezrozumieniem zadanego pytania było eliminowane w czasie rzeczywistym prowadzonego wywiadu kwestionariuszowego.

Wyniki badań analizowano w kontekście 3 grup respondentów: wyniki tylko dla przedsiębiorstw małych, wyniki tylko dla przedsiębiorstw średnich oraz sumarycznie dla małych i średnich przedsiębiorstw. Takie podejście pozwoliło na bardziej dokładne zobrazowanie poszczególnych zagadnień i możliwość porównania wyników w zależności od wielkości podmiotu gospodarczego.

Analizy statystyczne wyników badań zostały przeprowadzone za pomocą programu IBM SPSS Statistics 25.0. W celu ustalenia zależności między zmiennymi nominalnymi/kategorialnymi przeprowadzono analizę testem chi-kwadrat, względnie testem dokładnym Fishera (jeśli liczebność oczekiwana była mniejsza niż 5). W celu porównania dwóch grup pod względem zmiennej porządkowej wykorzystano test U Manna Whitneya. Jako poziom istotności na potrzeby niniejszych analiz przyjęto $\alpha = 0{,}05$. Wyniki badań w zestawieniach procentowych ukazywano jako liczby dziesiętne z zaokrągleniem do jednego miejsca po przecinku, zgodnie z zaleceniami American Psychological Association (7th ed.)[3] dla miar grupowych.

[3] APA PsycNET (2020), *Publication manual of the American Psychological Association, Seventh Edition*, American Psychological Association, https://psycnet.apa.org/record/2019-59141-000, s. 179, access date: 19.12.2021.

Analiza wyników badań przeprowadzonych w grupie małych i średnich przedsiębiorstw w Polsce pozwoliła na sformułowanie następujących konkluzji:

- w każdym przedsiębiorstwie przetwarzającym informacje w sposób cyfrowy korzysta się z poczty elektronicznej będącej głównym narzędziem cyberprzestępców w atakach z użyciem inżynierii społecznej;
- narzędzia informatyczne najczęściej wykorzystywane w przedsiębiorstwach są podatne na ataki z użyciem socjotechniki;
- rosnąca popularność modelu chmury obliczeniowej wymaga w kwestii bezpieczeństwa informacji większego nacisku w systemie informacyjnym przedsiębiorstwa na odpowiednie wyszkolenie pracowników niż na ochronę zasobów technicznych organizacji;
- poziom świadomości osób odpowiedzialnych za bezpieczeństwo informacji w organizacjach gospodarczych w aspekcie realnego ryzyka kradzieży lub zniszczenia informacji jest niski;
- istnieje potrzeba zwiększania świadomości wszystkich pracowników na wszystkich szczeblach zarządzania informacją w aspekcie istotności inżynierii społecznej w obszarze bezpieczeństwa zasobów informacyjnych;
- istnieje potrzeba opracowywania i budowania systemu ochrony informacji, którego mechanizmy będą funkcjonowały w ramach ciągłego procesu, a nie jednostkowych działań doraźnych;
- wiedza o wpływie czynnika ludzkiego na bezpieczeństwo informacji wśród osób odpowiedzialnych za ten obszar zarządzania zasobami niematerialnymi jest niewystarczająca;
- wpływ aspektów pozatechnicznych w procesie ochrony informacji jest w większości przedsiębiorstw marginalizowany lub pomijany;
- osoby odpowiedzialne za bezpieczeństwo informacji przywiązują obecnie większą wagę do procesów fizycznego zabezpieczania sprzętu programowego niż do odpowiedniego szkolenia pracowników zarządzających informacją;
- w przedsiębiorstwach w sposób niewystarczający stosuje się odpowiednie przepisy i mechanizmy zabraniające praktyk generujących ryzyko zagrożeń powodowanych czynnikami behawioralnymi;
- w przedsiębiorstwach w niewielkim stopniu wykorzystuje się techniki pozwalające monitorować poprawność procesu zarządzania informacją;

- istnieje potrzeba organizowania i prowadzenia szkoleń z zakresu aktualnej wiedzy o bezpieczeństwie informacji i potencjalnych zagrożeniach celem minimalizacji ryzyka wystąpienia incydentów powodowanych czynnikiem ludzkim;
- należy podejmować działania zmierzające do maksymalnej integracji i utożsamiania się pracownika z przedsiębiorstwem, szczególnie na kluczowych dla podmiotu stanowiskach pracy, celem wyeliminowania zagrożeń powodowanych czynnikami bchawioralnymi.

Na podstawie powyższych, elementarnych konkluzji wynikających z odpowiedzi udzielonych przez respondentów sformułowano dwa główne wnioski realizujące część postawionego celu głównego oraz potwierdzające postawioną w monografii hipotezę badawczą:

1) W przedsiębiorstwach małych i średnich nie przywiązuje się należytej uwagi do zagadnień związanych z rolą pozatechnicznych aspektów ochrony informacji (czynnika ludzkiego). Nie zarządza się bezpieczeństwem w sposób skuteczny i kompletny. Nie stosuje się w odpowiednim stopniu zabezpieczeń i narzędzi minimalizujących ryzyko wpływu zachowań pracowników na wystąpienie potencjalnych zagrożeń.
2) Problem wpływu czynnika ludzkiego na bezpieczeństwo informacji powinien być rozpatrywany w każdym przedsiębiorstwie bez względu na jego wielkość i rodzaj wykorzystywanego modelu informatycznego. Tylko odpowiednie działania podejmowane w przedsiębiorstwach, równoważące zaangażowanie środków zarówno technicznych, prawnych, jak i szkoleniowych, są w stanie zapewnić optymalne bezpieczeństwo systemu informacyjnego.

Na podstawie badań zarówno literaturowych, jak i empirycznych stwierdzono, że istniejące w przedsiębiorstwach systemy bezpieczeństwa informacji nacechowane są sposobami ograniczania ryzyka sięgającymi początków popularyzacji cyfrowego przetwarzania zasobów niematerialnych. Metody działania odnoszą się do przełomu lat 90. XX wieku i początków XXI wieku, kiedy faktycznie większość spotykanych zagrożeń miała charakter czysto techniczny. Stosowane obecnie rozwiązania sprzętowe i aplikacyjne są oczywiście nowsze, nieporównywalnie lepsze od swoich protoplastów, posiadające szersze spektrum niwelowania zagrożeń, ale często nieuwzględniające aspektów pozatechnicznych. Do dziś pokutują przyzwyczajenia stawiające na wyższym poziomie zabezpieczenia techniczne niż te związane z działaniem człowieka. Istnieje przekonanie, że odpowiednio skonfigurowany, wyposażony w najnowsze rozwiązania technologiczne system bezpieczeństwa jest w stanie skutecznie

ochronić zasoby informacyjne organizacji gospodarczych. A należy przy tym zwrócić uwagę na fakt, że w przypadku przedsiębiorstw małych i średnich nie zawsze mówimy nawet o zabezpieczeniach technicznych z tzw. „najwyższej półki". Aspekty behawioralne związane z czynnikiem ludzkim odchodzą na plan dalszy. Tymczasem od kilku lat badania prowadzone przez firmy specjalizujące się w branży IT i bezpieczeństwa informatycznego jasno pokazują, że czynnik ludzki jest przyczyną większości współczesnych zagrożeń dla informacji.

W świetle przeprowadzonych badań zarówno empirycznych, jak i literaturowych postawiono i jednocześnie próbowano odpowiedzieć na kluczowe pytania problemowe:

1) Kto powinien zarządzać systemem bezpieczeństwa informacji w przedsiębiorstwach?
2) W jaki sposób identyfikować potencjalne zagrożenia w przedsiębiorstwie związane z czynnikiem ludzkim?
3) Jakie największe potrzeby w zakresie ochrony zasobów niematerialnych można zidentyfikować we współczesnych małych i średnich przedsiębiorstwach?

W przypadku pytania pierwszego, pomijając szczegóły rozważań, które ujęto w monografii, stwierdzono, że właściwym kierunkiem zmian powinno być powoływanie na stanowiska dotyczące bezpieczeństwa informacji osoby, których głównym i jedynym zadaniem będzie ograniczanie i minimalizowanie ryzyka wystąpienia określonych incydentów. Jest to jednak kierunek, który nie zawsze może być spełniony – w szczególności przez przedsiębiorstwa małe, w których ogólna liczba pracowników zarządzających informacją może wynosić od jednej do kilku osób. W tej sytuacji należałoby uwzględnić rozwiązanie, w którym osoba przetwarzająca zasoby informacyjne w ramach obowiązków zawodowych pełniłaby również za dodatkowym wynagrodzeniem funkcję nadzorującą ich bezpieczeństwo. Wspomniano tutaj o dodatkowym wynagrodzeniu, gdyż, biorąc pod uwagę duże znaczenie bezpieczeństwa zasobów informacyjnych dla organizacji gospodarczej, należy dążyć do maksymalnego zaangażowania tych osób w powierzone zadania. Generalnie, warunkiem koniecznym, choć nie zawsze wystarczającym, jest stworzenie dla pracowników zajmujących kluczowe stanowiska w przedsiębiorstwie atrakcyjnych warunków pracy.

Próbując udzielić odpowiedzi na pytanie drugie, stwierdzono, że identyfikacja potencjalnych zagrożeń związanych z czynnikiem ludzkim jest złożona i wymaga wieloaspektowej analizy. Powinna koncentrować się na rozpoznaniu „słabych punktów" systemu informacyjnego, w szczególności działań podejmowanych przez człowieka. Z przeprowadzonych badań można wnioskować, że identyfikację zagrożeń należy realizować poprzez:

- zwracanie szczególnej uwagi na próby oszustwa, wyłudzenia informacji, zniszczenia informacji poprzez pocztę elektroniczną oraz oprogramowanie biurowe jako rozwiązania najczęściej wykorzystywane w przedsiębiorstwach. Najpopularniejsze rozwiązania są najczęściej celem ataku cyberprzestępców, podobnie jak system Windows jest najczęściej atakowanym systemem wśród wszystkich funkcjonujących na rynku gospodarczym, gdyż ma największy w nim udział;
- określenie modelu IT funkcjonującego w przedsiębiorstwie i na tej podstawie oszacowanie potencjalnych zagrożeń;
- określenie skali zjawiska BYOD w przedsiębiorstwie i oszacowanie potencjalnych skutków korzystania z tego rozwiązania;
- określenie skali użycia własnych przenośnych magazynów danych;
- zwracanie uwagi na zachowania pracowników i jeśli to niezbędne wdrożenie technik monitoringu;
- określenie realnego poziomu wiedzy pracowników na temat bezpieczeństwa informacji oraz określenie potrzeb szkoleniowych – badania wskazują, że szkolenia dla pracowników organizowane są w 25,3% przedsiębiorstw, pomimo że aż 79,0% respondentów uważa, że szkolenia powinny być skierowane do każdego pracownika zarządzającego informacją.

Identyfikacja potencjalnych zagrożeń powinna być realizowana również poprzez wnikliwą analizę dotychczasowych naruszeń bezpieczeństwa. Należy ponadto stworzyć odpowiednie mechanizmy skłaniające pracowników do zgłaszania wszelkich nieprawidłowości i w miarę możliwości stworzenia systemu, na podstawie którego każdy pracownik mógłby przesyłać swoje uwagi i pytania do określonej, wyznaczonej do tego celu osoby.

Odpowiedzi respondentów zaprezentowane w wynikach badań ujętych w monografii uwidaczniają w wielu obszarach funkcjonowania przedsiębiorstw określone nieprawidłowości z punktu ochrony informacji. Tym samym mogą stanowić swojego rodzaju „listę" ułatwiającą identyfikację potencjalnych zagrożeń.

Próbując udzielić odpowiedzi na trzecie postawione pytanie, stwierdzono, że identyfikacja potrzeb w zakresie ochrony zasobów niematerialnych, jak też działania zapobiegawcze, minimalizujące zagrożenia dla zasobów informacyjnych powinny ściśle korelować z wynikami uzyskanymi w pytaniu drugim. Na podstawie przeprowadzonych badań można stwierdzić, że powinny one koncentrować się na trzech podstawowych obszarach:

1) stosowaniu odpowiednich przepisów wewnętrznych regulujących użycie urządzeń komputerowych i oprogramowania;
2) zwiększeniu liczby szkoleń dostępnych dla każdego pracownika przetwarzającego informacje;
3) monitorowaniu jak największej ilości obszarów przetwarzania informacji.

Działania powinny być oparte na wiedzy pochodzącej z aktualnych badań z zakresu bezpieczeństwa zasobów informacyjnych: badań, które corocznie publikowane są w postaci raportów zarówno przez jednostki naukowe na całym świecie, jak i największe wywiadownie i organizacje zajmujące się profesjonalnie bezpieczeństwem informacji.

Realizacja skutecznego planu działań w zakresie zwalczania „luk zabezpieczeń" w przedsiębiorstwach może być wspierana cyklicznymi badaniami w formie ankiet przeprowadzanych wśród pracowników. Uzyskane od nich odpowiedzi mogą obnażyć kluczowe obszary wymagające pilnych działań w zakresie niwelowania zagrożeń dla informacji. Kolejnymi narzędziami w procesach identyfikacji potrzeb w zakresie ochrony informacji mogą być również nowoczesne metody zarządzania ryzykiem uwzględniające czynnik ludzki. Stosowanie metod wymaga, niestety, określonej wiedzy na temat narzędzi badawczych, więc nie każda organizacja może je aplikować – chyba że na zasadzie outsourcingu – ale to z kolei podnosi ryzyko ujawnienia „słabych punktów" systemu informacyjnego osobom trzecim.

Reasumując, przeprowadzone i zaprezentowane w rozdziale 4 badania z jednej strony ukazały stan współczesnych zabezpieczeń zasobów informacyjnych w przedsiębiorstwach małych i średnich, obnażając słabości systemów w zakresie nieuwzględniania czynnika ludzkiego, a z drugiej strony wyznaczyły kierunek działań, jaki należy podjąć w zapewnieniu skutecznych zabezpieczeń. Powinny inspirować decydentów organizacji gospodarczych, zarówno osoby odpowiedzialne za określanie odpowiedniego budżctu na ochronę zasobów niematerialnych, jak i osoby decydujące o zabezpieczaniu poszczególnych obszarów minimalizowania ryzyka wystąpienia zagrożeń (w tym obszaru działania człowieka), do działań adekwatnych do istniejących, a jednocześnie ciągle zmieniających się warunków zapewniania bezpieczeństwa informacji.

4.5. Koncepcja Podsystemu Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji

Realizując część celu głównego oraz cele aplikacyjne opracowano koncepcję podsystemu zarządzania bezpieczeństwem informacji z uwzględnieniem czynnika ludzkiego

w przedsiębiorstwach sektora małych i średnich przedsiębiorstw oraz dokonano oceny proponowanego podejścia systemowego.

Definiując pojęcie Podsystemu Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji (Podsystemu ZPABI), należy sprecyzować dwa określenia: podsystemu oraz pozatechnicznych aspektów bezpieczeństwa informacji. Pojęcie podsystemu dotyczy elementu pewnego systemu złożonego z współpracujących i wymieniających ze sobą informacje systemów, subsystemów. Podsystem realizuje założone przez twórcę procesy, które są autonomiczne, ale jednocześnie wpływające na pracę systemu nadrzędnego. Z kolei drugi termin zawiera wszystkie czynności, procesy, decyzje, które dotyczą zarówno posunięć związanych z ochroną zasobów niematerialnych przedsiębiorstw, jak i poczynań powodujących określone zagrożenia dla informacji. Podmiotem inicjującym określone działania jest człowiek. W przypadku przedsiębiorstw jest to pracownik, klient, partner biznesowy, osoba trzecia (np. konkurent, cyberprzestępca). W wybranych przypadkach mogą to być zorganizowane grupy cyberprzestępcze.

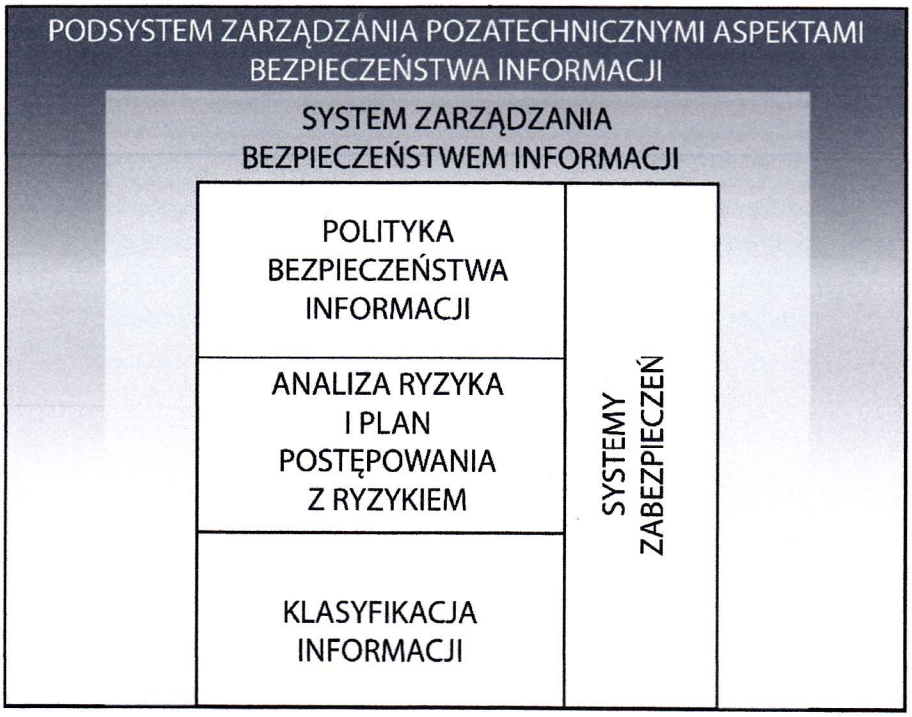
Samo pojęcie „pozatechniczne" w rozumieniu opisywanych aspektów dotyczy wybranego fragmentu działań mających na celu spowodowanie zagrożenia dla informacji lub jej ochrony pozbawionego czynnika, który miałby znamiona awarii, uszkodzenia sprzętu, bazy danych, hurtowni danych lub oprogramowania z przyczyn czysto technicznych. W przypadku przetwarzania informacji w postaci cyfrowej działania pozatechniczne są zazwyczaj częścią większego, bardziej złożonego procesu i często stanowią jego najważniejszy element. Pojęcie określa sam fragment inicjacyjny działania, kontrolę jego przebiegu i zakończenia i nie obejmuje narzędzi, które są rozwiązaniami informatycznymi funkcjonującymi w fizycznych sieciach lokalnych przedsiębiorstw oraz sieci globalnej.

Opracowany Podsystem ZPABI obejmuje zbiór elementów oraz sprzężeń między nimi dotyczących takich obszarów, jak:

- zarządzanie polityką bezpieczeństwa informacji w przedsiębiorstwie w aspekcie czynnika ludzkiego;
- zarządzanie ryzykiem w aspekcie czynnika ludzkiego;
- polityka uświadamiania i podnoszenia wiedzy wśród pracowników;
- monitoring działań we wszystkich obszarach zarządzania informacją.

Podsumowując, pod pojęciem Podsystemu Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji (Podsystemu ZPABI) w niniejszej monografii rozumiana jest realizacja działań i implementacja procedur minimalizujących ryzyko wystąpienia zagrożenia

z powodu tzw. czynnika ludzkiego w ramach Systemu Zarządzania Bezpieczeństwem Informacji w przedsiębiorstwach. Tym samym Podsystem ZPABI jest uzupełnieniem SZBI o elementy dotyczące wpływu człowieka, grup ludzkich na bezpieczeństwo informacji. Umiejscowienie proponowanego podsystemu pokazuje rysunek 2.



Rys. 2. Hierarchiczna struktura bezpieczeństwa informacji z uwzględnieniem Podsystemu ZPABI

Źródło: opracowanie własne na podstawie struktury bezpieczeństwa informacji zaproponowanej przez (Wójcik, 2008, s. 71)

Fundamentem w zarządzaniu bezpieczeństwem informacji w podmiocie gospodarczym jest System Zarządzania Bezpieczeństwem Informacji (SZBI). Jednocześnie aspekty pozatechniczne bezpieczeństwa informacji dotyczące działania człowieka zarówno w zakresie ochrony, jak i powodowania zagrożeń dla zasobów niematerialnych są w obecnych czasach najważniejsze i dotyczą praktycznie każdego obszaru SZBI. Stąd Podsystem ZPABI na rysunku 2 przedstawiony jest jako obejmujący, uzupełniający SZBI a jednocześnie najważniejszy, scalający w jedno wszystkie działania mające na celu minimalizację ryzyka wystąpienia zagrożenia.

Zaproponowany podsystem można rozpatrywać na 3 płaszczyznach:

- w ujęciu funkcjonalnym;
- implementacji i funkcjonowania na płaszczyźnie przedmiotowej;
- implementacji i funkcjonowania na płaszczyźnie podmiotowej.

Ujęcie podsystemu na płaszczyźnie funkcjonalnej można rozpatrywać ogólnie w dwóch wymiarach: przedsiębiorstwo – pracownik oraz przedsiębiorstwo – klienci, partnerzy biznesowi, osoby trzecie. W każdym z tych wymiarów istnieje pewien zakres działań/zadań, które należy podjąć i wykonać, aby zapewnić maksymalne bezpieczeństwo zasobów informacyjnych. Zakres ten powinien być zawarty w ramach funkcjonowania Podsystemu ZPABI.

Wymiar pierwszy obejmuje swoim działaniem wszystkie etapy, okresy, w których pracownik związany jest z przedsiębiorstwem. Są to:

1) okres rekrutacji – przed zatrudnieniem;
2) okres zatrudnienia;
3) okres zakończenia zatrudnienia.

Na przestrzeni wszystkich trzech etapów należy stosować określone środki ostrożności i odpowiednio zarządzać bezpieczeństwem informacji. Kluczowe działania, które powinny być podejmowane w ramach Podsystemu ZPABI w relacji przedsiębiorstwo – pracownik w poszczególnych okresach wyszczególniono w tabeli 4.

Tabela 4. Kluczowe działania minimalizujące zagrożenie informacji z powodu czynnika ludzkiego w podziale na etapy relacji pracownik - przedsiębiorstwo w ramach Podsystemu ZPABI

Etap	Działania
Okres rekrutacji	• Określenie poziomu kompetencji pracowniczych kandydata mających wpływ na bezpieczeństwo zasobów informacyjnych i zestawienie ich z wymaganymi kompetencjami stanowiskowymi. • Określenie wiedzy i doświadczenia w zakresie bezpieczeństwa informacji. • Przeprowadzenie wywiadu odnośnie do oczekiwań w zakresie podejmowanej pracy. Badania literaturowe dowodzą, że osoby, które preferują zatrudnienie na tzw. „umowy śmieciowe" i które nie mają wygórowanych oczekiwań finansowych, szczególnie na bardziej prestiżowe stanowiska pracy, mogą być „narzędziem" tzw. wywiadu gospodarczego. • Ustalenie cech psychofizycznych pracownika, stanu zdrowia, w szczególności identyfikacja zaburzeń psychicznych (zadanie dla psychologa, psychiatry, prawdopodobnie trudne i mogące budzić kontrowersje)*.
Okres zatrudnienia	• Zawarcie z pracownikiem klauzuli poufności w zakresie przetwarzanych informacji zarówno na czas zatrudnienia, jak i po zatrudnieniu. • Określenie zasad przetwarzania informacji na danym stanowisku pracy.

	• Zapoznanie pracownika z wewnętrznymi przepisami i zasadami przetwarzania informacji (poświadczenie zaznajomienia z dokumentami własnoręcznym podpisem przez pracownika). • Szkolenie indywidualne pracownika w zakresie zidentyfikowanego na etapie rekrutacji braku wiedzy z obszaru bezpieczeństwa informacji. • Zapewnienie optymalnych warunków pracy, szczególnie dla pracowników mających dostęp do istotnych z punktu widzenia przedsiębiorstwa zasobów informacyjnych. • Monitorowanie stanowiska pracy. • Monitorowanie procesów przetwarzania informacji przez pracownika. • Ustalenie przejrzystych reguł stosowania kar i nagród (np. w postaci premii lub jej braku) będących następstwem sposobu zarządzania informacją przez pracownika. Reguły powinny być przejrzyste i zaakceptowane uprzednio przez pracownika. • Wprowadzenie systemu motywacyjnego adekwatnie do możliwości przedsiębiorstwa. • Przeprowadzanie ataków kontrolowanych (symulowanych) celem określenia słabych stron pracownika. • Utworzenie systemu pomocy dla pracowników np. poprzez powołanie osoby na stanowisko eksperta bezpieczeństwa informacji lub inne pokrewne (w przypadku przedsiębiorstw małych może to być dodatkowy zakres obowiązków dla określonego pracownika). Ogólnie, pracownik powinien mieć możliwość dostępu do szybkiej pomocy w rozwiązywaniu sytuacji dla niego niejasnych. • Organizacja cyklicznych szkoleń mających na celu utrwalanie dotychczasowej i przekazywanie nowej wiedzy z zakresu bezpieczeństwa informacji.
Okres zakończenia zatrudnienia	• Zapewnienie godziwych warunków odejścia z pracy, szczególnie jeśli zwolnienie następuje z inicjatywy pracodawcy. • Odnowienie (przypomnienie) klauzuli poufności w myśl tekstu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. 1993 nr 47 poz. 211 z późn. zm.), która również dotyczy byłych pracowników i wprowadza ustawowy obowiązek do zachowania tajemnicy przedsiębiorstwa przez 3 lata po ustaniu stosunku pracy[4]. • Monitorowanie w możliwym, dozwolonym prawem zakresie dalszych losów pracownika, w szczególności jego kolejnych miejsc pracy i obserwowanie, czy kluczowe działania przedsiębiorstwa, w którym obecnie pracuje, mogą

[4] Łesak D. (2019), *Klauzula poufności, czyli jak chronić tajemnicę przedsiębiorstwa*, Poradnik Przedsiębiorcy, https://poradnikprzedsiebiorcy.pl/-klauzula-poufnosci-czego-moze-dotyczyc, data dostępu: 21.12.2021 r.

	mieć coś wspólnego z posiadanymi przez pracownika informacjami z racji wcześniejszego zatrudnienia (dotyczy pracowników, którzy posiadali najważniejsze, strategiczne dla przedsiębiorstwa informacje).

*działanie opcjonalne, nieobowiązkowe ze względu na potencjalne trudności w realizacji. Ponadto, jak pisze W. Jedrzejczyk[5], w przedsiębiorstwach raczej nie spotyka się stanowiska psychologa. Działanie jest jednak istotne, szczególnie w sytuacji naboru na stanowiska kluczowe w organizacji gospodarczej

Źródło: opracowanie własne

Drugi wymiar, w którym rozpatruje się podejmowanie działań mających na celu eliminację negatywnych aspektów czynnika ludzkiego w obszarze bezpieczeństwa informacji, dotyczy relacji przedsiębiorstwa z osobami lub grupami osób niebędących pracownikami tego podmiotu gospodarczego. W tabeli 5 zestawiono relacje oraz działania, które powinny być podejmowane w ramach Podsystemu ZPABI.

Tabela 5. Kluczowe działania minimalizujące zagrożenie informacji z powodu czynnika ludzkiego w poszczególnych relacjach w ramach Podsystemu ZPABI

Relacja	Działania
Przedsiębiorstwo – klient	• Zapewnienie określonych warunków przyjmowania klientów, pozwalających na maksymalną izolację od możliwych źródeł pozyskania informacji. • Fizyczne uniemożliwienie dostępu do pomieszczeń, w których przetwarzane są informacje. • Realizacja szkoleń dla osób obsługujących klientów w zakresie bezpieczeństwa informacji.
Przedsiębiorstwo – partner biznesowy	• Zapewnienie określonych warunków przyjmowania partnerów biznesowych, zapewniających maksymalną izolację od możliwych źródeł pozyskania informacji. • Cykliczne szkolenie pracowników z zakresu technik inżynierii społecznej – możliwość działania partnera biznesowego na rzecz konkurencji (tzw. praca na „dwa fronty").
Przedsiębiorstwo – osoby trzecie	• Fizyczne uniemożliwienie dostępu do pomieszczeń, w których przetwarzane są informacje. • Cykliczne szkolenie pracowników z zakresu technik inżynierii społecznej. • Monitorowanie stanowisk pracy, w szczególności wszystkich narzędzi komunikacyjnych (np. telefon, poczta, chat).

Źródło: opracowanie własne

Poziom realizacji wyszczególnionych w tabelach 4 i 5 działań powinien być dostosowany do poziomu funkcjonującego w przedsiębiorstwie Systemu ZBI. Jest oczywiste,

[5] Jędrzejczyk W. (2013), *Intuicja jako kompetencja menedżerska w teorii i praktyce zarządzania przedsiębiorstwem*, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, Toruń, s. 270.

że przedsiębiorstwa małe spełniają zazwyczaj minimalne wymagania odnośnie bezpieczeństwa informacji. Nie należy jednak stosować wymienionych działań wybiórczo, gdyż powoduje to tworzenie „luk" w systemie bezpieczeństwa, a tym samym powoduje jego osłabienie.

Podsystem ZPABI w ujęciu przedmiotowym to wszystkie niematerialne i materialne składniki podsystemu, to wszystkie jego elementy pozwalające minimalizować ryzyko powstania zagrożenia - elementy mające pośredni lub bezpośredni wpływ na czynniki i procesy funkcjonujące w przedsiębiorstwie oraz jego otoczeniu. Są to rozwiązania wspomagające działanie człowieka lub monitorujące jego zachowanie (tab. 6).

Tabela 6. Zestawienie materialnych i niematerialnych składników Podsystemu ZPABI

Rodzaj składnika podsystemu	Składnik podsystemu
Materialne	• bazy wiedzy; • kursy, szkolenia utrwalone na nośnikach informacji (CD, DVD, BR, HDD, SSD, dyski wirtualne etc.); • automatyczne systemy identyfikujące; • automatyczne systemy kontrolujące; • automatyczne systemy raportujące; • systemy kontroli dostępu zdalnego; • systemy wsparcia on-line; • ogólnodostępne nośniki informacji z przepisami i zasadami postępowania w zakresie zarządzania informacją; • oprogramowanie do monitoringu; • sprzęt do monitoringu; • rozwiązania programowe i sprzętowe do blokowania określonych usług; • systemy dla kontrolowanego, celowego przeprowadzania ataków, umożliwiających identyfikację „słabych punktów" pracownika.
Niematerialne	• ustawiczne wsparcie dla pracowników w obszarze bezpieczeństwa informacji; • regularne, ogólne szkolenia dla pracowników; • regularne, specjalistyczne szkolenia dla określonych grup pracowników; • przepisy i zasady postępowania w zakresie zarządzania informacją (wartość merytoryczne bez uwzględniania nośnika informacji); • koncepcje zarządzania ryzykiem z uwzględnieniem czynnika ludzkiego.

Źródło: opracowanie własne

Jednym z podstawowych materialnych składników Podsystemu ZPABI są bazy wiedzy wspomagające identyfikację i rozwiązywanie pojawiających się problemów, umożliwiające gromadzenie aktualnych informacji na temat bezpieczeństwa oraz wspierające procesy dzielenia się wiedzą. Powinny one spełniać następujące warunki:

- dostępność – pracownicy powinni mieć do nich ciągły dostęp, w miarę możliwości również poza godzinami pracy;
- skalowalność – możliwość sprawnego działania bez względu na objętość przetwarzanych informacji oraz liczbę jednoczesnych połączeń;
- przejrzystość – zasoby bazy powinny być przedstawiane użytkownikom w łatwy do nawigowania i zrozumienia sposób;
- łatwość obsługi – baza powinna być wyposażona w mechanizmy pozwalające każdemu pracownikowi na bezproblemowe wyszukiwanie zasobów.

Podsystem Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji na płaszczyźnie przedmiotowej można zdefiniować jako zbiór rozwiązań sprzętowo-programowych realizujących założone cele w zakresie zabezpieczania zasobów informacyjnych organizacji gospodarczej przed zagrożeniami powodowanymi czynnikiem ludzkim. Rozwiązania te w określony sposób ingerują w system informacyjny, minimalizując ryzyko powstania incydentu. Na rysunku 3 przedstawiono schemat powiązań między elementami Podsystemu ZPABI a składnikami systemu informacyjnego. Wymienione składniki można scharakteryzować następująco:

1) Sieć Wewnętrzna Przedsiębiorstwa (SWP) – sieć komputerowa LAN podmiotu gospodarczego, zarówno fizyczna (kablowa) o określonej topologii, jak i bezprzewodowa o określonym standardzie służąca do wymiany danych i informacji.
2) Telefonia Stacjonarna i Komórkowa (TSiK) – wszystkie systemy komunikacji telefonicznej funkcjonujące w podmiocie.
3) Indywidulane Stanowiska Przetwarzania Informacji (ISPI) – wszystkie stanowiska pracy, na których przetwarzane są zasoby informacyjne. Fizycznie mogą to być komputery stacjonarne, laptopy, tablety, smartfony i inne urządzenia, na których przetwarzanie jest możliwe.
4) Zbiorcze Stanowiska Przetwarzania Informacji (ZSPI) – wszystkie stanowiska, które obsługują w określonym zakresie stanowiska indywidualne. Fizycznie mogą to być serwery plików, serwery baz danych, serwery aplikacji, serwery poczty elektronicznej i inne pełniące podobne funkcje.

Powyższe składniki tworzą relacje z elementami Podsystemu ZPABI. Większość relacji (poza połączeniami raportowania) jest dwukierunkowych, ponieważ w każdym przypadku występuje wzajemna wymiana sygnałów, danych lub informacji. Przedstawiają się one następująco:

- Rozwiązania programowe i sprzętowe do blokowania określonych usług działają we współpracy z trzema składnikami: SWP, ISPI oraz ZSPI. W przypadku SWP zbierane są dane o uruchamianych w sieci wewnętrznej usługach lub podpinanych do tej sieci urządzeniach komputerowych. W przypadku ISPI zbierane są dane o uruchamianych aplikacjach, zarówno lokalnych, jak i w chmurze obliczeniowej, oraz podłączanych urządzeniach peryferyjnych (np. do portów USB – Universal Serial Bus). Z kolei w ZSPI element kontroluje uprawnienia użytkowników z korzystania określonych zasobów, monitoruje ich przepływ i sprawdza również podłączane przez pracowników urządzenia zewnętrzne.

  Wykrycie niepożądanych działań ze strony pracowników lub osób trzecich próbujących nielegalnie pozyskać informacje uruchamia mechanizm natychmiastowego ich blokowania. Element ten może działać według dwóch scenariuszy: blokować wcześniej zaprogramowane działania lub, wykorzystując mechanizmy sztucznej inteligencji, samodzielnie „podejmować decyzje" o zezwoleniu lub zablokowaniu usługi. Sztuczna inteligencja może być również rozwiązaniem uzupełniającym, podobnie jak funkcjonuje to w niektórych programach antywirusowych, które mając wbudowane inteligentne mechanizmy, rozpoznają podejrzany kod, mimo że oficjalnie w bazie sygnatur tego kodu nie ma.

  Element ten raportuje swoje działania w automatycznym systemie raportującym.
- Systemy kontroli dostępu zdalnego współpracują tylko z SWP, monitorując w czasie rzeczywistym połączenia między siecią globalną a siecią LAN. Dotyczą przede wszystkim pracowników zdalnych, przydzielając im określone prawa dostępu do zasobów. Blokują jednocześnie nielegalne próby połączeń z siecią przez osoby trzecie. Należy tutaj zaznaczyć, że systemy te nie są rozwiązaniami mającymi na celu blokowanie złośliwego oprogramowania i innych zagrożeń kolportowanych automatycznie przez roboty sieciowe. Są ich uzupełnieniem mającym na celu eliminację niepożądanych celowych lub przypadkowych działań człowieka od strony sieci Internet. Praca składnika jest raportowana.
- Automatyczne systemy kontrolujące współpracują z SWP, ISPI i ZSPI. Mają za zadanie przede wszystkim „pilnować" pracowników w zakresie ustalania prawidłowych zabezpieczeń zasobów informacyjnych. Dotyczy to monitorowania ustalania haseł

urządzeń sieciowych, sieci bezprzewodowych, urządzeń komputerowych, aplikacji lokalnych, dostępu do chmury obliczeniowej lub kontrolowania użytkownika w zakresie otwierania portów komunikacyjnych itp. Wszystkie błędy popełniane przez człowieka są raportowane. Raporty zawierają zarówno sam identyfikator błędu, jak i precyzyjne informacje o osobie, która go popełniła. Tym samym systemy te umożliwiają tworzenie bazy w zakresie potrzeb szkoleniowych.

- Automatyczne systemy identyfikujące współpracują z TSiK oraz ISPI. Są to dwa składniki systemu informacyjnego, które pozwalają na komunikację z przedsiębiorstwem. Systemy identyfikują osoby kontaktujące się z przedsiębiorstwem. Praca składnika jest raportowana w zakresie dozwolonym prawem, szczególnie w myśl przepisów RODO.
- Bazy wiedzy połączone są tylko z ISPI, współpracując jednocześnie z systemami on--line. Współpraca ta ma umożliwić wyszukiwanie w bazie informacji poprzez mechanizmy komunikatora sieciowego, który wyposażony jest w moduł wyszukiwania. Taka synergia pozwala pracownikom używać jednego narzędzia zarówno w kontakcie z osobą zajmującą stanowisko nadzoru nad bezpieczeństwem informacji, jak i z bazą wiedzy. Pozwala również na „odsyłanie" w trakcie rozmowy przez komunikator do określonych dokumentów elektronicznych.
- Systemy dla kontrolowanego, celowego przeprowadzania ataków, umożliwiających identyfikację „słabych punktów" pracownika współpracują z wszystkimi składnikami systemu informacyjnego.

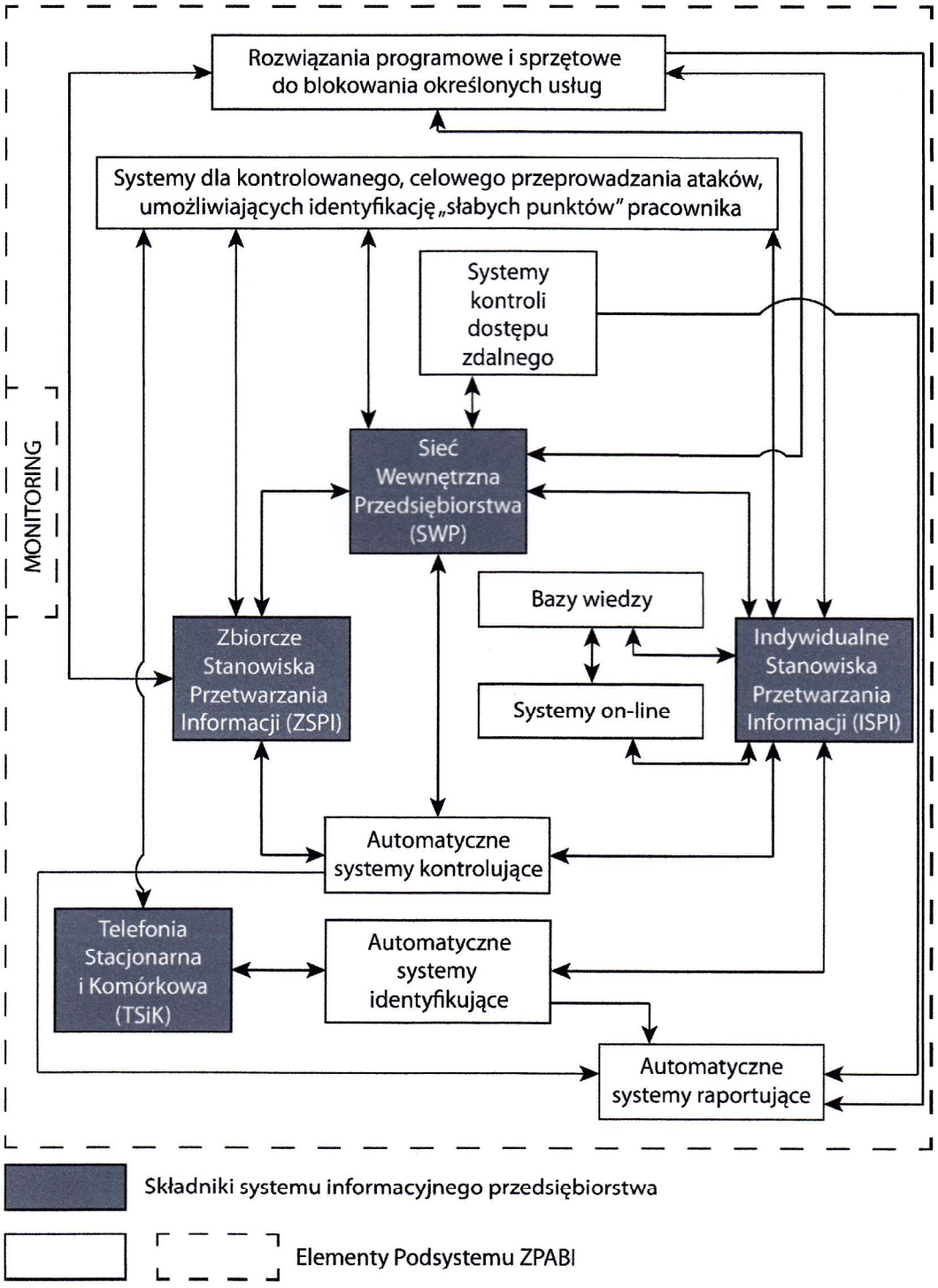
  W przypadku SWP oraz ZSPI umożliwiają symulację, w efekcie której można określić braki wiedzy i doświadczenia pracowników zajmujących się systemem IT przedsiębiorstwa. Pośrednio pozwalają również dokonać sprawdzenia niezawodności innych składników Podsystemu ZPABI realizujących zabezpieczenie SWP i ZSPI.

  W przypadku ISPI i TSiK służą do „testowania" wiedzy i doświadczenia pracowników szczególnie w zakresie technik inżynierii społecznej. Pozwalają nakreślić szczegółową mapę potrzeb szkoleniowych.

Wszystkie elementy, zarówno SI, jak i Podsystemu ZPABI, są monitorowane.

Implementacja podsystemu na płaszczyźnie przedmiotowej wymaga realizacji następujących kroków:

1) analizy wszystkich elementów zastanego systemu informacyjnego;
2) adaptacji elementów Podsystemu ZPABI do zastanej konfiguracji Systemu ZBI;
3) wdrożenia poszczególnych elementów.



Rys. 3. Elementy Podsystemu ZPABI i zależności między składnikami systemu informacyjnego

Źródło: opracowanie własne

Podsystem Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji na płaszczyźnie podmiotowej można zdefiniować jako zbiór powiązań między: elementami niematerialnymi podsystemu a osobami mającymi jakikolwiek wpływ na bezpieczeństwo systemu informacyjnego oraz poszczególnymi osobami, realizujących założone cele w zakresie

zabezpieczania zasobów informacyjnych organizacji gospodarczej przed zagrożeniami powodowanymi czynnikiem ludzkim.

Szczegółowy schemat zależności przedstawiono na rysunku 4. Możemy na nim zauważyć dwa rodzaje relacji: między poszczególnymi osobami – oznaczone liniami przerywanymi oraz między elementami podsystemu a osobami – oznaczone liniami ciągłymi.

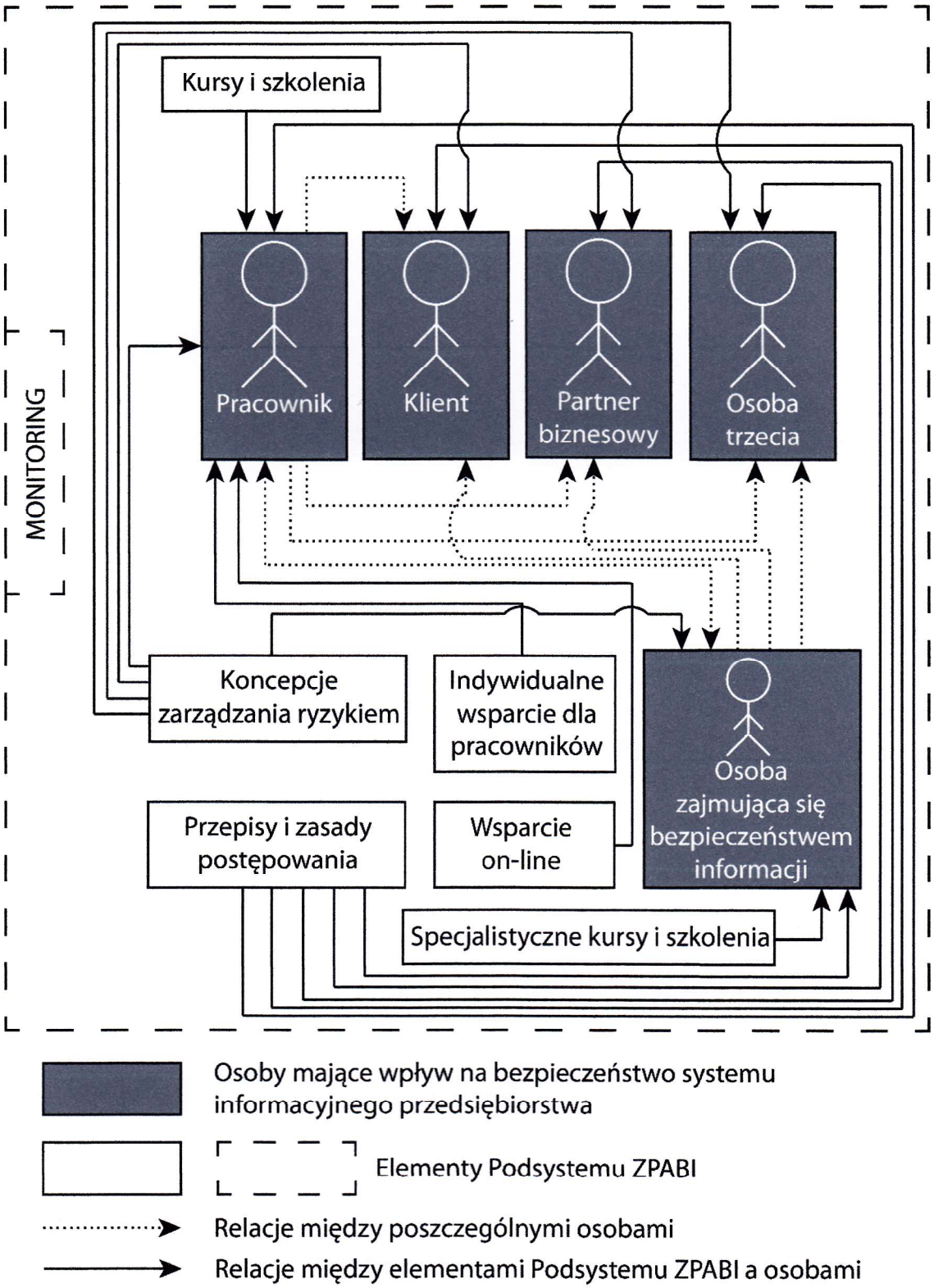
W przypadku relacji międzyludzkich można zdefiniować następujące zależności na płaszczyźnie zapobiegania występowaniu zagrożeń dla zasobów informacyjnych:

- Między osobą zajmującą się bezpieczeństwem informacji a wszystkimi pozostałymi osobami. Mają one następujący charakter:
    - z pracownikiem – dotyczą szeroko rozumianego wsparcia w zakresie bezpieczeństwa przetwarzanych informacji, analizy działań pracownika w aspekcie przestrzegania przepisów i zasad postępowania;
    - z klientem – dotyczą narzucania określonych zasad postępowania w przypadku korzystania przez klienta z systemu przedsiębiorstwa (np. przy zakładaniu konta), przydzielania praw dostępu do systemu informatycznego, określania zasad obsługi klientów, analizy działań klientów w systemie przedsiębiorstwa;
    - z partnerem biznesowym – dotyczą narzucania określonych zasad postępowania w przypadku korzystania przez partnera biznesowego z systemu przedsiębiorstwa (np. przy zakładaniu konta resellera), przydzielania praw dostępu do systemu informatycznego, analizy działań partnerów biznesowych w systemie przedsiębiorstwa;
    - z osobą trzecią – dotyczą określania poziomu zabezpieczeń przed dostępem do systemu informacyjnego, monitorowania prób łamania zabezpieczeń oraz prób wyłudzeń informacji z użyciem socjotechnik.
- Między pracownikiem a wszystkimi pozostałymi osobami. W szczególności:
    - z klientem – dotyczą zachowania określonych standardów obsługi klienta w zakresie eliminowania potencjalnych sytuacji, w których może zaistnieć możliwość celowego lub przypadkowego udostępnienia chronionej informacji, umiejętności przeciwdziałania socjotechnikom;
    - z partnerem biznesowym – dotyczą pracowników wyższego szczebla, odpowiedzialnych za kontakty biznesowe. Zakres relacji analogiczny jak w kontaktach z klientami;
    - z osobą zajmującą się bezpieczeństwem informacji – dotyczą zgłaszania przez pracownika zauważonych nieprawidłowości oraz podejrzanych zachowań

aplikacji i systemu operacyjnego podczas wykonywania powierzonych czynności;

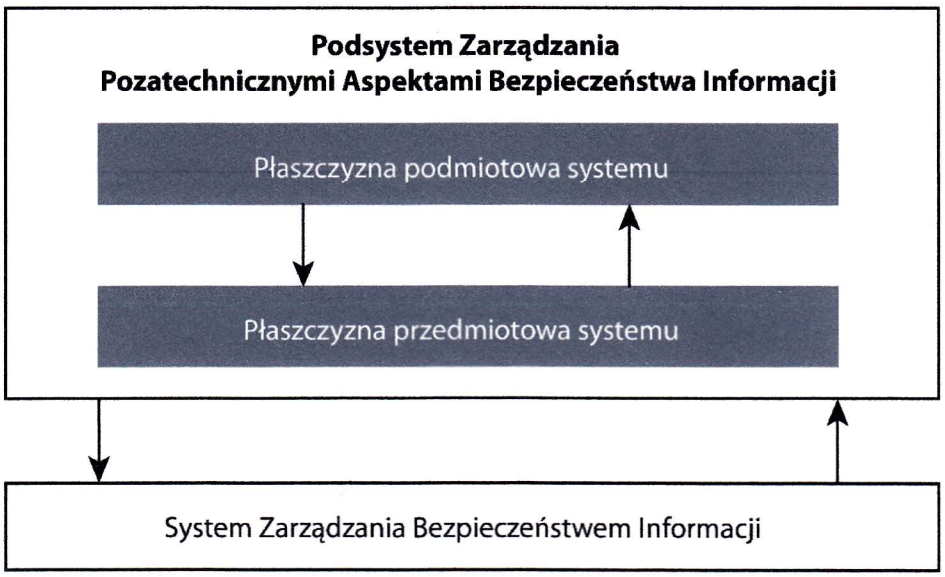
- z osobą trzecią – dotyczą umiejętności dostrzegania sytuacji, w której osoba trzecia używa technik inżynierii społecznej w celu pozyskania informacji, umiejętności przeciwstawienia się tym technikom.

Podsystem ZPABI stanowi w założeniu kompleksowe ujęcie zabezpieczeń przed wszystkimi rodzajami zagrożeń mających swój początek w zachowaniu człowieka. Mając świadomość tempa zmian w procesach zarządzania informacją, zaproponowano podsystem, którego składowe mogą funkcjonować w sposób niezależny. Tym samym podsystem jest rozwiązaniem otwartym, do którego można podłączać kolejne elementy (moduły) chroniące przed zagrożeniami, które być może pojawią się w latach kolejnych. Jedyną, nierozerwalną strukturą jest konieczność współistnienia obu płaszczyzn (rys. 5). Tylko w ten sposób, łącząc ze sobą działania człowieka, składniki materialne i niematerialne przeciwdziałające utracie lub zniszczeniu informacji, można uzyskać kompleksowe rozwiązanie minimalizujące ryzyko zagrożenia dla zasobów niematerialnych.



Rys. 4. Zależności między elementami Podsystemu ZPABI a osobami mającymi wpływ na bezpieczeństwo systemu informacyjnego przedsiębiorstwa

Źródło: opracowanie własne



Rys. 5. Całościowe ujęcie Podsystemu ZPABI na tle relacji z Systemem Zarządzania Bezpieczeństwem Informacji

Źródło: opracowanie własne

Bardzo istotna i również nierozerwalna jest współpraca Podsystemu ZPABI z istniejącym systemem bezpieczeństwa. Pozwala to na kompleksową eliminację potencjalnych incydentów. Ponadto, spektrum współczesnych zagrożeń jest na tyle duże, że poszczególne techniki ataków, prób pozyskania informacji zaczynają wzajemnie się przenikać. Powstające w ten sposób techniki hybrydowe mogą być skutecznie zwalczane tylko poprzez ścisłą współpracę zarówno Podsystemu ZPABI, jak i SZBI.

Opracowana koncepcja Podsystemu ZPABI realizuje pierwszy z postawionych w monografii celów aplikacyjnych.

W pracy dokonano również oceny Podsystemu Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji, która realizuje drugi z postawionych w pracy celów aplikacyjnych.

Oceny Podsystemu ZPABI dokonano na próbie 24 osób odpowiedzialnych za bezpieczeństwo zasobów informacyjnych wśród przedsiębiorstw średnich biorących udział w wywiadzie kwestionariuszowym. Zdecydowano się na przeprowadzenie ankiety dotyczącej oceny podsystemu wśród osób biorących udział w pierwszej części badań, gdyż osoby te były już wprowadzone w pewnym stopniu w problematykę badawczą. Zastosowaną techniką badawczą była ankieta elektroniczna (metoda CAWI – Computer-Assisted Web Interview). Próba badawcza została wyselekcjonowana metodą doboru celowego. Przy wyborze osób biorących w badaniu kierowano się następującymi przesłankami:

- respondenci podczas bezpośredniego wywiadu kwestionariuszowego wykazywali zainteresowanie rozwiązaniami zwiększającymi bezpieczeństwo informacji w ich przedsiębiorstwie;
- udzielane przez respondentów podczas bezpośredniego wywiadu kwestionariuszowego odpowiedzi świadczyły o dużej wiedzy z zakresu bezpieczeństwa informacji;
- osoby te podczas wywiadu kwestionariuszowego wyraziły chęć dalszej współpracy w ramach opracowywania podsystemu.

Pierwszym etapem poprzedzającym działania zmierzające do oceny podsystemu było kompleksowe szkolenie (3-4 – godzinne w zależności od liczby zadawanych pytań) mające na celu opisanie i wytłumaczenie zasady funkcjonowania Podsystemu ZPABI. Ze względu na odległości geograficzne oraz ograniczone zasoby czasowe respondentów odbyło się ono za pośrednictwem multimedialnego komunikatora internetowego w 5 turach kolejno po 3, 4, 3, 8, 6 osób w styczniu-lutym 2020 roku.

Drugim etapem po przeprowadzeniu szkolenia było przesłanie do ww. osób ankiety elektronicznej utworzonej w jednym z narzędzi dostępnych w chmurze obliczeniowej z prośbą o udzielenie odpowiedzi na 4 pytania: 3 zamknięte i 1 otwarte.

Pytania sformułowano następująco:

1. Czy proponowane podejście systemowe może przyczynić się do poprawy bezpieczeństwa informacji?
2. Czy rozwiązanie jest na tyle uniwersalne, że może być wdrożone w każdym małym i średnim przedsiębiorstwie?
3. Czy jeśli byłaby akceptacja zarządu/właściciela przedsiębiorstwa, to czy zdecydowaliby się Państwo wdrożyć Podsystem ZPABI w swoim przedsiębiorstwie?

W pytaniu otwartym poproszono respondentów o wyszczególnienie zauważonych słabych i mocnych stron Podsystemu Zarządzania Pozatechnicznymi Aspektami Bezpieczeństwa Informacji. Udzielone odpowiedzi zunifikowano pod względem znaczeniowym. Do mocnych stron zaliczono:

1) Relatywnie niewielki koszt implementacji podsystemu (w trakcie szkolenia przedstawiono możliwość implementacji podsystemu z wykorzystaniem zarówno komercyjnych komponentów, jak i rozwiązań typu open-source lub rozwiązań w modelu SaaS – np. chat do systemu on-line, struktura bazodanowa dla bazy wiedzy. Ponadto podsystem w dużej mierze opiera się na rozwiązaniach funkcjonujących już w ramach SZBI).

2) Podsystem jest kompleksowy, działa praktycznie na wszystkich obszarach przetwarzania informacji.
3) Możliwość modyfikacji podsystemu, w tym rozbudowy.
4) Relatywnie prosta idea funkcjonowania.

Do słabych stron podsystemu zaliczano:

- Konieczność zatrudniania osoby zajmującej się bezpieczeństwem informacji (mimo że w szkoleniu zaznaczono, iż może to być również osoba, dla której sprawowanie tej funkcji będzie zajęciem dodatkowym).
- Konieczność poświęcania zbyt dużej ilości czasu na realizowanie założeń podsystemu, np. cykliczne szkolenia ogólne i specjalistyczne, kontrolowanie pracy podsystemu, np. raportowania, monitoringu.
- Konieczność wprowadzania zmian, które nie zawsze są „na rękę" właścicielom przedsiębiorstw, np. zakazu używania swoich urządzeń komputerowych w pracy.
- Możliwe niezadowolenie pracowników z implementacji monitoringu.

Uzyskane wyniki dotyczące oceny podsystemu można uznać za satysfakcjonujące, pomimo że bazują one tylko na przekazanej respondentom wiedzy oraz opisaniu podczas przeprowadzanego szkolenia struktury i funkcjonowania podsystemu a nie na doświadczeniach z jego użytkowania. Należy więc zadać pytanie: czy po wdrożeniu i użytkowaniu podsystemu przez określony czas (minimum 2 lat, aby np. zrealizować przynajmniej 2 cykle szkoleń, przeanalizować poszczególne systemy w realnym przeciwdziałaniu określonym zagrożeniom) odpowiedzi respondentów pokrywałyby się z obecnie uzyskanymi?

Trudno jednoznacznie na to pytanie odpowiedzieć. Obserwując wdrożenia różnego rodzaju systemów w praktyce gospodarczej czy też funkcjonowanie nowych rozwiązań informatycznych nawet największych firm na świecie, można zauważyć, że nie zawsze oczekiwania są zgodne z realną eksploatacją tych produktów. Jako bezpośredni przykład można podać najbardziej popularny na świecie system operacyjny, do którego w każdym miesiącu publikowane są nowe aktualizacje eliminujące występujące w nim błędy. Podobnie jest z wieloma innymi produktami i systemami o mniej lub bardziej skomplikowanej architekturze. Stąd też należy przyjąć, ze w trakcie eksploatacji mogą pojawić się problemy które trudno przewidzieć na etapie projektowania. Przyjmując jednak założenie, że Podsystem ZPABI w dużej mierze opiera się na funkcjonujących już w przedsiębiorstwach systemach

bezpieczeństwa informacji, praca tego podsystemu nie powinna zbytnio odbiegać od jego teoretycznych założeń.

W pracy zaproponowano również autorski model oceny dojrzałości bezpieczeństwa informacji w aspekcie funkcjonowania Podsystemu ZPABI bazujący na wybranych założeniach modelu CMMI (Capability Maturity Model Integration). Podjęto również rozważania naukowe dotyczące wybranych aspektów opłacalności implementacji Podsystemu ZPABI.

Analizując zagadnienia i aspekty ochrony zasobów niematerialnych, w monografii odnoszono się do założeń norm serii ISO 27000 oraz modelu CMMI (Capability Maturity Model Integration) jako najbardziej, zdaniem autora, przystających do obszarów tematycznych niniejszej monografii. Problematyka poruszana w książce może nasuwać również myśl o związkach z takimi zbiorami dobrych praktyk, wskazówek jak chociażby COBIT (Control Objectives for Information and related Technology) czy ITIL (Information Technology Infrastructure Library), ale po rozważeniu stwierdzono, że te kwestie zostaną pominięte, gdyż nie dotyczą takiego ujęcia problemu, jak zaprezentowane w publikacji. Praktyki COBIT koncentrują się bardziej na kontroli, a mniej na procesach implementacji, a obszary będące w zainteresowaniu niniejszej monografii i tak w dużej mierze pokrywają się z normami ISO 27000. W przypadku ITIL i innych norm oraz zbiorów praktyk jest analogicznie.

4.6. Wkład pracy w rozwój nauk o zarządzaniu i jakości

Ochrona zasobów informacyjnych organizacji gospodarczej to obecnie przede wszystkim wyszkolona kadra pracownicza, skuteczne systemy eliminujące zarówno zagrożenia ze strony technicznej, jak i zagrożenia płynące z tzw. czynnika ludzkiego. Niezbędna jest synergia tych dwóch obszarów. Stworzenie spójnej struktury bezpieczeństwa informacji stanowi jedyną drogę do minimalizacji ryzyka potencjalnych zagrożeń.

Bezpieczeństwo uwzględniające aspekty pozatechniczne jest obecnie jeszcze często ignorowane. Osoby odpowiedzialne za ochronę informacji zbyt duże zaufanie pokładają w posiadanych zabezpieczeniach programowych i sprzętowych, ignorując często czynniki zwiększające ryzyko zniszczenia lub utraty informacji powodowane przez samych pracowników. Badania publikowane zarówno w literaturze naukowej, jak i w raportach publikowanych przez największe firmy na świecie zajmujące się cyberbezpieczeństwem pokazują, że większość współcześnie obserwowanych zagrożeń informacyjnych ma podłoże związane z czynnikiem ludzkim. Działania za pomocą technik inżynierii społecznej są

odnotowywane w większości przedsiębiorstw na świecie, a ich skuteczność jest niepokojąco wysoka.

Aby poprawić bezpieczeństwo zasobów informacyjnych, konieczne jest wdrożenie odpowiednich mechanizmów eliminujących lub minimalizujących działania w zakresie prób nielegalnego pozyskania informacji. Niezbędna jest zmiana nastawienia osób zajmujących się bezpieczeństwem informacji w przedsiębiorstwach. Konieczne w procesie ochrony zasobów jest uwzględnianie człowieka jako „elementu" najbardziej narażonego na błędy, zaniedbania, celowe działania sabotażowe itd. Działania podejmowane przez pracowników mają charakter nieprzewidywalny, nie da się ich „zaprogramować", a liczba możliwych zachowań w określonych sytuacjach przetwarzania informacji jest praktycznie nieograniczona. Stwarza to bardzo trudne warunki dla zapewnienia bezpieczeństwa, a jednocześnie otwiera szereg możliwości działania ze strony osób chcących nielegalnie pozyskać lub zniszczyć informacje. Konieczne są rozwiązania systemowe, ciągle udoskonalane, wyposażone w procesy bezpieczeństwa funkcjonujące równolegle z innymi procesami zarządzania informacją. Nie oznacza to oczywiście, że dotychczasowe zabezpieczenia powinny przestać funkcjonować – takie działanie doprowadziłoby prawdopodobnie do „powrotu" zagrożeń, które dominowały w latach poprzednich (i są w określonym, ale mniejszym stopniu również dziś). Niezbędne jest działanie kompleksowe, uwzględniające wszystkie możliwe przejawy zagrożenia zasobów niematerialnych.

Przyjęta struktura monografii łączy najistotniejsze aspekty, obszary, w których informacja i jej bezpieczeństwo występują. Kolejne rozdziały miały na celu przybliżyć samą istotę informacji i jej znaczenia zarówno teoretycznego, jak i praktycznego we współczesnej gospodarce, rozwiązania aplikacyjne, systemy, sieci komputerowe, które dla informacji w jej współczesnym kształcie stanowią naturalne środowisko zarządzania, a jednocześnie nakreślają mapę słabych i mocnych punktów bezpieczeństwa systemu informacyjnego. Monografia miała na celu zdefiniować współczesne środowisko bezpieczeństwa informacji, zarówno w kształcie organizacyjnym, jak i technicznym. Myślą przewodnią i inspiracją do napisania tej książki było przede wszystkim zarządzanie bezpieczeństwem zasobów informacyjnych ze szczególnym uwzględnieniem czynnika ludzkiego.

Zarządzanie czynnikiem ludzkim w aspekcie jego wpływu na bezpieczeństwo informacji nie jest łatwe. Trudność wynika z faktu, że jest to zjawisko relatywnie nowe (biorąc pod uwagę jego obecny rozmiar) i brak jest wypracowanych wzorców zarówno na płaszczyźnie postępowań wobec osób zarządzających informacją, jak i wobec samego zjawiska, które obejmuje całe spektrum manier, zachowań i wiedzy pracowników oraz innych osób mających

wpływ na bezpieczeństwo informacji. Brak jest również sprawdzonych metod zarządzania ryzykiem uwzględniających czynnik ludzki w bezpieczeństwie informacji, które to metody są podstawą dla efektywnego zarządzania bezpieczeństwem informacji. Wiele opracowywanych metod można uznać za pionierskie (np. HEART-IS), a ich mechanizmy próbuje się dopiero adaptować z metod rozwijanych dla innych obszarów działalności człowieka, w których błędy ludzkie mogą wpłynąć na życie i zdrowie innych ludzi, np. energetyka jądrowa, lotnictwo, żegluga morska, programy kosmiczne.

Przedstawione w monografii badania pokazują, że w bezpieczeństwie informacji nie uwzględnia się należycie czynnika ludzkiego. Zarówno w przedsiębiorstwach małych, jak i średnich pokutuje przekonanie, że to aspekty techniczne zabezpieczeń stanowią główny element systemu bezpieczeństwa informacji. Zachowania pracowników, ich wiedzę, doświadczenie, kompetencje nie przekłada się dostatecznie na potencjalne skutki zarządzania informacją. Zjawiska i czynniki te w wielu istniejących systemach bezpieczeństwa wydają się nieobecne.

Przeprowadzone w monografii badania nakreśliły swoistą mapę poziomów bezpieczeństwa informacji na płaszczyźnie przedsiębiorstw małych i średnich w Polsce. Ukazały słabe i mocne strony systemów bezpieczeństwa, przedstawiając jednocześnie zbiór niezbędnych działań, jakie należy podjąć w celu minimalizacji ryzyka w procesach zarządzania informacją.

Przyjęty cel badawczy: 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, został osiągnięty.

Przeprowadzone studia literaturowe, a także zrealizowane badania empiryczne wśród małych i średnich przedsiębiorstw wykazały, że zarządzanie bezpieczeństwem nie ewaluowało wraz z nowymi metodami nielegalnego pozyskiwania informacji. Większość przedsiębiorstw nie dostrzega ryzyka w zachowaniu swoich pracowników, nie widzi potrzeby ich szkolenia, pozwala korzystać z narzędzi i urządzeń, które obecnie uchodzą za najbardziej narażone na ataki z użyciem technik inżynierii społecznej.

Organizacjami stanowiącymi podstawę zarówno do badań literaturowych, jak i własnych badań empirycznych, opracowania podsystemu były małe i średnie przedsiębiorstwa. Jednakże uzyskane wyniki uprawniają do hipotezy, że zaproponowana koncepcja ma zastosowanie również w przypadku innych rodzajów organizacji, np. administracji publicznej, trzeciego sektora, a weryfikacja tej hipotezy jest zagadnieniem do dalszych badań i rozważań naukowych.

Prezentowana monografia systematyzuje zagadnienia dotyczące współczesnych aspektów ochrony informacji w małych i średnich przedsiębiorstwach. Opracowane w części teoretycznej modele, schematy, zestawienia, struktury mogą stanowić podstawę do stworzenia kolejnych koncepcji związanych z ochroną zasobów niematerialnych. Przedstawiona autorska definicja czynnika ludzkiego w bezpieczeństwie informacji ukazuje syntetyczne ujęcie rozpatrywanej problematyki w zarządzaniu informacją.

Przeprowadzone na terenie Polski badania związane z zarządzaniem informacją, bezpieczeństwem informacji z uwzględnieniem czynnika ludzkiego stanowią relatywnie nowe podejście w kwestii zarządzania bezpieczeństwem informacji. Kwestię te zauważył również recenzent wydawniczy, Prof. Mirosław Kwieciński, który pisze: *„(...) prezentowana problematyka badawcza stanowi w polskim piśmiennictwie nadal istotne novum. Szczególnie daje się zauważyć brak polskich ujęć teoretycznych oraz badań dotyczących roli zarządzania bezpieczeństwem zasobów informacji w przedsiębiorstwach sektora MŚP w kontekście roli czynnika ludzkiego. (...)*". Podobnie zagadnienia poruszane w monografii ujął drugi z recenzentów wydawniczych, Prof. Janusz Zawiła-Niedźwiecki, który, podkreślając oryginalność pracy, pisze: *„Warto docenić oryginalność ujęcia tytułowej kwestii przez Autora monografii. Wykazuje on, że teoria zarządzania bezpieczeństwem informacji niewiele wykroczyła poza sformułowania, że człowiek jest najsłabszym elementem zasobów organizacji z punktu widzenia zapewniania bezpieczeństwa. Tym samym organizacje są narażone na wsobne niebezpieczeństwa związane z niewłaściwym uwzględnianiem czynnika ludzkiego w bezpiecznym organizowaniu swojej działalności. Przy tym stopień tych niebezpieczeństw jest wyższy w mniejszych przedsiębiorstwach, gdyż ich potencjał budowania zabezpieczeń jest mniejszy niż dużych organizacji czy korporacji, które dysponują większą liczbą specjalistów od tych wyzwań i budują własne dobre praktyki. Małe i średnie przedsiębiorstwa potrzebują wsparcia metodycznego, które powinna dostarczyć nauka. Pierwszy krok ku temu dostarcza recenzowana monografia*".

Opracowany na podstawie badań literaturowych oraz własnych, empirycznych Podsystem ZPABI jest rozwiązaniem scalającym obszary techniczne i pozatechniczne bezpieczeństwa informacji i stanowi jednocześnie pionierskie ujęcie tej tematyki w formie kompleksowego rozwiązania systemowego w zakresie zarządzania informacją, wpisując się jednocześnie w rozwój nauk o zarządzaniu.

Problematyka bezpieczeństwa informacji oraz wpływu czynnika ludzkiego na to bezpieczeństwo jest aktualna i nic nie wskazuje na to, aby w najbliższej przyszłości mogło dojść do jakiegokolwiek przewartościowania tego zjawiska. Wymaga ona jednocześnie

dalszych analiz, zarówno na płaszczyźnie rozpoznawania kolejnych zagrożeń dla procesu zarządzania informacją, jak i na płaszczyźnie metod przeciwdziałania tym zagrożeniom.

5. Pozostałe osiągnięcia naukowo-badawcze

5.1. Osiągnięcia przed uzyskaniem stopnia doktora

Pracę zawodową rozpocząłem w 2001 roku – po ukończeniu studiów wyższych na Wydziale Elektrycznym Politechniki Częstochowskiej na kierunku Elektrotechnika w zakresie Informatyki w Elektroenergetyce. Już w okresie studiów moje zainteresowania naukowe oscylowały wokół zagadnień związanych z informatyką i zarządzaniem informacją, ze szczególnym uwzględnieniem rozwiązań aplikacyjnych w funkcjonowaniu przedsiębiorstw. Temat mojej pracy magisterskiej, który brzmiał: „*Analiza inwestycji w zakresie ograniczenia emisji pyłu w elektrowniach*", pozwolił mi na połączenie zagadnień ze studiowanym kierunkiem oraz zagadnień związanych z informatyką i zarządzaniem. Aspekt informatyczny pojawił się w części empirycznej pracy przy opracowaniu autorskiej aplikacji komputerowej napisanej w języku Delphi, analizującej opłacalność inwestycji w kwestii instalacji filtrów wraz z ich doborem. W trakcie studiów ukończyłem również Fakultatywne Studia Pedagogiczne w Międzywydziałowym Studium Kształcenia Nauczycieli Przedmiotów Technicznych, mając duże przekonanie co do wyboru kierunku mojej drogi zawodowej.

Chęć pogłębiania swojej wiedzy w zakresie zarządzania informacją w przedsiębiorstwach z użyciem narzędzi informatycznych oraz chęć pracy naukowej w tym obszarze skłoniło mnie do podjęcia pracy w Katedrze Informatycznych Systemów Zarządzania (obecnie Katedry Informacyjnych Systemów Zarządzania) na Wydziale Zarządzania Politechniki Częstochowskiej pod opieką naukową Prof. Leszka Kiełtyki. W tym samym czasie podjąłem dalsze kształcenie na Wydziale Zarządzania Politechniki Częstochowskiej na kierunku „Zarządzanie i Marketing" w ramach studiów wyższych magisterskich uzupełniających w zakresie „Przedsiębiorczości i rozwoju przedsiębiorstw" ukończone w 2003 roku pracą pt. „*Nowoczesne technologie informatyczne w procesie usprawniania wymiany informacji w przedsiębiorstwie*".

Moje główne zainteresowania naukowe od początku pracy na uczelni obejmowały dwa obszary zarządzania informacją:

- przetwarzanie i wymiana informacji w podmiotach gospodarczych;
- bezpieczeństwo zasobów informacyjnych w podmiotach gospodarczych ze szczególnym uwzględnieniem wpływu czynnika ludzkiego.

Obszar pierwszy dominował w pierwszym okresie mojej pracy naukowej (szczególnie przed uzyskaniem stopnia doktora). Zainteresowania naukowe obszarem drugim pojawiły się po uzyskaniu stopnia naukowego doktora.

W trakcie realizacji studiów uzupełniających, w pracy zawodowej jako asystent, prowadziłem swoje pierwsze badania naukowe, które skoncentrowane były w obszarze zarządzania informacją w przedsiębiorstwach przy wykorzystaniu potencjału sieci Internet[6]. Obejmowały one takie zagadnienia, jak:

- Wymiana informacji poprzez globalną sieć Internet w relacjach B2B i B2C.
- Wirtualizacja podmiotów gospodarczych.
- Tworzenie wizerunku podmiotu gospodarczego w sieci Internet.
- Komunikacja w sieci Internet ze szczególnym uwzględnieniem multimediów.

Od samego początku pracy naukowej zarządzanie informacją w podmiotach gospodarczych stanowiło główny nurt moich zainteresowań. Były one relatywnie szerokie i dotyczyły praktycznie większości obszarów, gdzie informacja jest w jakikolwiek sposób przetwarzana i przechowywana. Efekt tak szerokiego spektrum dociekań naukowych można dostrzec w moich publikacjach, w których poruszałem zarówno poziom aplikacyjny zarządzania informacją[7], sposoby gromadzenia zasobów niematerialnych[8], jak i metody wymiany informacji poprzez nowoczesne środki transmisji sieciowej. Obszar moich zainteresowań naukowych dotyczył sposobów wymiany informacji między pracownikami, partnerami biznesowymi jak też biznesem i klientami podmiotów gospodarczych. Szczególny nacisk położyłem na efektywność wymiany informacji z użyciem transmisji grupowej podczas połączeń multimedialnych: wideokonferencji[9]. Ciekawość naukową dodatkowo aktywizowała cyklicznie organizowana Konferencja Naukowa „Multimedia w Biznesie", której do chwili obecnej jestem współorganizatorem, a podczas jej XII edycji byłem sekretarzem naukowym.

---

[6] **Kobis P.** (2001), *Rola Internetu w rozwoju małych i średnich przedsiębiorstw*, [w:] B. Plawgo (red.), *Małe i średnie przedsiębiorstwa w gospodarce regionu*, Wydawnictwo Uniwersytetu w Białymstoku, Białystok, s. 198-204, ISBN 83-89031-04-3.

[7] **Kobis P.** (2002), *Zastosowanie prognozowania do wspomagania decyzji finansowych w przedsiębiorstwach z użyciem arkusza kalkulacyjnego MS Excel*, [w:] L. Kiełtyka (red.), *Multimedia w zarządzaniu*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa, s. 404-413, ISBN 83-88469-01-0.

[8] **Kobis P.** (2002), *Cooperation of the decision support systems and data warehouses in the companies*, Zborník prednášok 4 medzinárodnej vedeckej konferencie Využívanie nových poznatkov v strojárskej praxi TRANSFER 2002, 2 Diel, Trenčín, s. 351-356, ISBN 80-88914-75-2.

[9] Kiełtyka L., **Kobis P.** (2002), *Nowe technologie przesyłania danych w przedsiębiorstwie*, [w:] R. Borowiecki, A. Jaki (red.), *Restrukturyzacja a procesy rozwoju i kreowania wartości przedsiębiorstw*, Wydawnictwo Katedry Ekonomiki i Organizacji Przedsiębiorstw Akademii Ekonomicznej w Krakowie. Warszawa-Kraków, s.246-250, ISBN 83-907047-1-4.
Kobis P. (2002), *Zastosowanie wideokonferencji w nowoczesnym zarządzaniu*, „Współczesne Zarządzanie. Kwartalnik środowisk naukowych i liderów biznesu", Nr 4, s. 88-94, ISSN 1643-5494.
Kiełtyka L., **Kobis P.** (2002), *Transmisja danych z wykorzystaniem technologii IP Multicast*, „Informatyka Teoretyczna i Stosowana", Nr 3, s. 155-162, ISSN 1643-2355.

Analiza poszczególnych rozwiązań w zakresie zarządzania informacją w przedsiębiorstwach w latach 2001-2003 mojej pracy ugruntowała moje zainteresowania naukowe w obszarze przetwarzania zasobów niematerialnych w organizacjach gospodarczych. Głównym nurtem badawczym stała się wymiana informacji w sieci Internet z użyciem nowych technologii ze szczególnym uwzględnieniem transmisji grupowej. Komunikacja poprzez sieci teleinformatyczne, rozpatrywana zarówno na płaszczyźnie gospodarczej, jak i naukowej w pierwszej dekadzie XXI wieku była zagadnieniem, które w niezwykle dynamiczny sposób zmieniało podejście organizacji gospodarczych w aspekcie wymiany informacji. Rozwój sieci szerokopasmowych, technologii IP Multicast, multimediów, sposobów kompresji obrazu i dźwięku nakreślało ogromne możliwości do rozwoju pracy zdalnej, spotkań wirtualnych na różnych szczeblach pracowniczych na niespotykaną na ówczesne czasy skalę.

Rozważane aspekty teoretyczne związane z zarządzaniem informacją postanowiłem skonfrontować z praktyką. W tym celu, chcąc pogłębić własną wiedzę praktyczną w zakresie zarzadzania informacją oraz wykorzystywania technik i technologii informatycznych, w okresie od 01.02.2003 r. do 31.07.2003 r. odbyłem staż przemysłowy w przedsiębiorstwie produkcyjno-handlowym Linex w Częstochowie. Staż wzbogacił mój zasób wiedzy praktycznej, przyczyniając się jednocześnie do odkrycia określonych subobszarów w zakresie zarządzania informacją, co z kolei wzbogaciło moje dalsze rozważania naukowe w kolejnych publikacjach.

W latach kolejnych, w okresie od 2004 do 2010 roku (do uzyskania stopnia doktora), kontynuowałem swoje badania, czego efektem był cykl publikacji, które dotyczyły wybranych aspektów wymiany informacji.

Szczególnym obszarem wymiany informacji z punktu badawczego były dla mnie spotkania Rad Nadzorczych (RN) spółek oraz komunikacja między akcjonariuszami podczas Walnych Zgromadzeń Akcjonariuszy (WZA). Celem badań było opracowanie koncepcji spotkań wirtualnych z użyciem dostępnych wówczas rozwiązań aplikacyjnych i komunikacji sieciowej. Dodatkową inspirację stanowił fakt, iż na gruncie gospodarczym podejmowano pierwsze próby realizacji tego typu spotkań. Polska Grupa Farmaceutyczna S.A. jako pierwsza spółka w Polsce zdecydowała się na transmitowanie przebiegu Walnego Zgromadzenia Akcjonariuszy przez Internet[10].

[10] **Kobis P.** (2004), *Technologie informatyczne umożliwiające komunikację w korporacjach na szczeblach rad nadzorczych*, [w:] A. Nowicki, D. Jelonek, J. Goliński (red.), *Informatyka ekonomiczna. Aspekty naukowe i dydaktyczne*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, s.83-90, ISBN 83-88469-62-2.

Moje badania koncentrowały się na obszarach technologii wspomagających wymianę informacji, technologiach transmisji danych, sposobów wymiany informacji w zależności od modelu nadzoru korporacyjnego i systemach multimedialnych w podmiotach gospodarczych. W świetle wirtualnych spotkań RN i WZA podejmowałem badania naukowe w zakresie adaptacji środowisk pracy grupowej na płaszczyźnie aplikacyjnej i komunikacyjnej w dużych przedsiębiorstwach[11]. Swoje przemyślenia naukowe publikowałem i wygłaszałem w Polsce i za granicą: 7. Medzinárodna Vedecka Konferencia „Využívanie nových poznatkov v strojárskej praxi" TRANSFER 2005, Trenčín, Slovak Republik, V Międzynarodowa Konferencja „Multimedia w Biznesie i Edukacji", Częstochowa, Konferencja Naukowa „Technologie informatyczne i prognozowanie w zarządzaniu", Hołny Mejera, VIII Międzynarodowa Konferencja „Multimedia w Biznesie i Zarządzaniu", Częstochowa.

Tematami rozważań naukowych w mojej pracy z badanego obszaru wymiany informacji były również technologie multimedialne oraz rozważania na temat efektywności inwestycji w zakresie implementacji rozwiązań technik i technologii komunikacyjnych. Aspekt szeroko rozumianej efektywności inwestycji zdefiniowany został w moich rozważaniach jako relacja efektów uzyskanych w wyniku poniesienia określonych nakładów inwestycyjnych do wartości tych nakładów[12]. Na podstawie tak zdefiniowanego problemu podejmowałem rozważania naukowe dotyczące poszczególnych aspektów implementacji systemów pracy grupowej, konfrontując je z tradycyjnymi, funkcjonującymi w podmiotach gospodarczych stacjonarnymi formami spotkań[13].

W moich rozważaniach naukowych dotyczących aspektu technologii multimedialnych szczególne miejsce zajmowała wymiana informacji w czasie rzeczywistym z użyciem wideokonferencji, transmisji strumieniowych obrazu i dźwięku przy użyciu transmisji grupowej (IP Multicast). Celem poparcia moich rozważań naukowych w kwestii

---

[11] **Kobis P.** (2005), *The Modern Information Technologies Supporting Groupware in Big Companies*, TRANSFER 2005, Vyuzivanie novych poznatkov v strojarskej praxi, Zbornik prednasok 7. medzinarodnej vedeckej konferencie, 2 diel, Trencin, s. 308-311, ISBN 80-8075-070-X.
Kobis P. (2005), *Wymiana informacji z użyciem oprogramowania na platformie systemowej GNU/LINUX*, [w:] L. Kiełtyka (red.), *Multimedia w biznesie i edukacji*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa, s. 113-117, ISBN 83-88469-28-2.
Kobis P. (2006), *Aspekty organizacyjne dotyczące implementacji systemów pracy grupowej w dużych przedsiębiorstwach*, [w:] L. Kiełtyka, J. Nazarko (red.), *Metody i procesy usprawniania zarządzania przedsiębiorstwem. Wybrane zagadnienia*, Wyd. Menedżerskie PTM, Warszawa, s. 243-248, ISBN 83-914212-2-8.
Kobis P. (2008), *Wspomaganie procesów produkcyjnych poprzez wdrażanie systemów pracy grupowej*, [w:] J. Nazarko, L. Kiełtyka (red.), *Narzędzia informatyczne w zarządzaniu i inżynierii produkcji*, Wyd. DIFIN, Warszawa, s. 143-152, ISBN 978-83-7251-920-7.
Kobis P. (2010), *Multimedialne technologie komunikacyjne w procesach nadzoru korporacyjnego*, [w:] A. Dura (red.), *Współczesne koncepcje zarządzania w teorii i praktyce*, Wydawnictwo AGH, Kraków, ISBN 978-83-7464-369-6.
[12] Pabianiak P. (2003), *Ocena efektywności inwestycji*, e-BizCom, Szczecin, s. 9.
[13] **Kobis P.** (2007), *Ocena efektywności inwestycji w procesie wdrażania technologii informatycznych w dużych przedsiębiorstwach*, [w:] L. Kiełtyka (red.), *IT w organizacjach gospodarczych*, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, s. 137-147, Toruń, ISBN 978-83-7285-355-4.

analizowanych technologii prowadziłem badania wśród dużych przedsiębiorstw, dotyczące po pierwsze oczekiwań w zakresie wymiany informacji i usług aplikacyjnych, a po drugie aktualnego stanu posiadania w zakresie rozwiązań teleinformatycznych. Wyniki publikowałem i wygłaszałem na konferencjach naukowych, m.in. VI Międzynarodowej Konferencji „Multimedia w Biznesie" w Kielcach[14], I Konferencji Naukowej „Zarządzanie przepływem i ochroną informacji w państwie i przedsiębiorstwie. Problemy teorii i praktyki" w Krakowie[15], XII Międzynarodowej Konferencji Naukowej „Zarządzanie przedsiębiorstwem – teoria i praktyka" w Krakowie.

Moje zainteresowania budziły również futurystyczne w owym okresie rozwiązania komunikacji multimedialnej. Przykładem może być teleimersja, która, wedle twórców koncepcji, miała stanowić ostateczną syntezę technologii sieciowej oraz medialnej, zapewniając optymalne warunki pracy. Była to koncepcja promowana w obszarze naukowym przez takie ośrodki naukowe, jak: University of North Carolina w Chapel Hill czy University of Pensylwania w Stanach Zjednoczonych. Próby podjęcia opracowania naukowej koncepcji wykorzystania tego typu narzędzi w dużych przedsiębiorstwach przedstawiłem na łamach Kwartalnika Środowisk Naukowych i Liderów Biznesu „Współczesne Zarządzanie"[16] oraz VII Międzynarodowej Konferencji „Multimedia w Biznesie"[17].

Zdobywaną wiedzę i koncepcje teoretyczne weryfikuję empirycznie. W 2005 roku zostałem członkiem Towarzystwa Naukowego Organizacji i Kierownictwa (nr legitymacji członkowskiej 5/2005). W ramach członkostwa starałem się konfrontować własne przemyślenia i badania naukowe w środowisku biznesu poprzez aktywny udział w organizowanych spotkaniach oddziału częstochowskiego TNOiK z lokalnymi przedstawicielami biznesu oraz realizowanych szkoleniach dla sektora gospodarczego. Osobiście również przeprowadzałem szkolenia pod egidą TNOiK z zakresu zarządzania informacją w przedsiębiorstwie, m.in. dla francuskiej firmy Leroy Merlin, oddziału w Poczesnej koło Częstochowy. Moja praca w Towarzystwie Naukowym Organizacji i Kierownictwa została doceniona i 14.09.2010 roku zostałem odznaczony srebrną odznaką honorową Towarzystwa (nr legitymacji 4294).

---

[14] **Kobis P.** (2006), *Wybrane technologie wspierające wymianę informacji w dużych przedsiębiorstwach w Polsce*, [w:] L. Kiełtyka (red.), *Multimedia w organizacjach gospodarczych i edukacji*, Wyd. DIFIN, s. 278-287, Warszawa, ISBN 83-7251-673-1.

[15] **Kobis P.** (2007), *Technologie multimedialne wspierające wymianę informacji w przedsiębiorstwach*, [w:] M. Kwieciński (red.), *Zarządzanie przepływem i ochroną informacji*, Wydawnictwo Krakowskiej Szkoły Wyższej, Kraków, s. 40-46, ISBN 978-83-89823-19-9.

[16] **Kobis P.** (2004), *Zastosowanie nowoczesnych technik komunikacyjnych w dużych przedsiębiorstwach*, „Współczesne Zarządzanie. Kwartalnik środowisk naukowych i liderów biznesu", Nr 4, s.83-91, ISSN 1643-5494.

[17] **Kobis P.** (2008), *Multimedia sieciowe we współczesnym biznesie*, [w:] L. Kiełtyka (red.), *Technologie i systemy komunikacji oraz zarządzania informacją i wiedzą*, Wyd. DIFIN, Warszawa, s. 84-91, ISBN 978-83-7251-882-8.

Dalsze badania, przemyślenia naukowe zaowocowały przydzieleniem mojej osobie w roku 2008 ministerialnego własnego grantu naukowego pt. „*Model zarządzania informacją w aspekcie implementacji systemów pracy grupowej w instytucjach*", zarejestrowanego pod numerem N N115 134334. Projekt realizowany był w sieci lokalnej Politechniki Częstochowskiej z użyciem głównie wideokonferencyjnego systemu grupowego oraz sześciu systemów desktopowych i oprogramowania do pracy grupowej. W projekcie podjąłem badania parametrów transmisji audio-wideo-dane z użyciem technologii interaktywnego multicastu, dostosowania ich do istniejących warunków wymiany informacji na podstawie wykonanych analiz. Przedmiotem projektu była analiza jakościowa i ilościowa dotycząca wewnętrznego potencjału instytucji z punktu widzenia istniejących systemów informatycznych z ukierunkowaniem na systemy pracy grupowej. Dokonałem analizy zasobów informacji, informatyzacji poszczególnych szczebli zarządzania oraz składników systemu zarządzania, sprzyjających implementacji systemów informatycznych wspomagających grupowe podejmowanie decyzji. Analizie poddałem stopnień wykorzystania nowoczesnych technik wymiany informacji ze szczególnym naciskiem na systemy wideokonferencyjne i aplikacje wspierające komunikację w czasie rzeczywistym (tryb synchroniczny pracy grupowej). Efektem wymiernym było zbudowanie modelu pomocnego do wdrażania i wykorzystania systemów pracy grupowej w dowolnej instytucji wykorzystującej sieć intranetową z podłączeniem do sieci Internet.

Moje 9-letnie badania naukowe związane z zarządzaniem informacją w sieciach teleinformatycznych, systemami multimedialnymi, systemami grupowymi pozwoliły na opracowanie koncepcji, napisanie i obronienie pracy doktorskiej na Wydziale Zarządzania Akademii Górniczo-Hutniczej w Krakowie pod tytułem: „*Wpływ Grupowych Systemów Wspomagania Decyzji na usprawnianie zarządzania dużymi przedsiębiorstwami*". Głównym motywem podjęcia tematu pracy była konieczność usprawnienia systemów wspomagania wymiany informacji w przedsiębiorstwach ze szczególnym uwzględnieniem grupowego podejmowania decyzji na szczeblach Rad Nadzorczych, jak też szczeblach kierowniczych. Wybór przedsiębiorstw podlegających badaniu wynikał z faktu możliwości powoływania przez te spółki organów Rad Nadzorczych, zarządu i Walnego Zgromadzenia Akcjonariuszy. Rady Nadzorcze spółki stanowiły w mojej ocenie najważniejszą grupę docelową objętą zakresem badań pracy. Komunikacja na szczeblach Rad Nadzorczych, zarządów spółek oraz pomiędzy akcjonariuszami podczas walnych zgromadzeń była kluczowa z punktu podejmowania decyzji strategicznych i taktycznych. Najistotniejszymi problemami naukowymi poruszanymi w pracy doktorskiej były:

- brak sprawnego, ekonomicznego i nowoczesnego sposobu wymiany informacji (wymiana dokumentów, spotkania wirtualne – audio- i wideokonferencje);
- zbyt powolne implementowanie usprawnień technologicznych, wynikających z wprowadzanych na rynek nowych rozwiązań informatycznych;
- brak możliwości szybkiego i efektywnego szkolenia pracowników;
- wysokie koszty nieuniknionych spotkań zarządów korporacji (w tym spotkania konferencyjne);
- brak szybkiej i sprawnej wymiany danych z pracownikami w przypadku stosowania telepracy.

W kolejnych rozdziałach pracy dokonałem:

- badań literaturowych;
- wyboru obiektów badawczych spełniających wstępne kryteria do przeprowadzania badań;
- przeprowadzenia badań;
- przeprowadzenia oceny efektywności inwestycji;
- opracowania algorytmu postępowania przy wdrażaniu systemu wspomagania grupowego podejmowania decyzji;
- oceny i weryfikacji opracowanego algorytmu i określenia wpływu wdrożonych technologii informatycznych na zarządzanie dużymi przedsiębiorstwami.

Wybór tematu pracy, jej koncepcji poprzedziłem badaniami i dyskusjami naukowymi na konferencjach naukowych, m.in. na:

- Konferencji Naukowej i Letniej Szkole Zarządzania w 2008 roku[18], gdzie przedstawiłem również przeprowadzone wspólnie i pod kierunkiem Prof. Leszka Kiełtyki badania nt. „Nowoczesnych technologii informacyjnych wspierających wymianę informacji w dużych przedsiębiorstwach w Polsce" wśród menedżerów odpowiedzialnych za stan infrastruktury informatycznej oraz wymianę informacji w podmiotach gospodarczych,
- VIII Międzynarodowej Konferencji „Multimedia w Biznesie i Zarządzaniu" w 2009 roku[19] oraz

[18] Kiełtyka L., **Kobis P.** (2008), *Wymiana informacji w dużych przedsiębiorstwach przy użyciu nowoczesnych rozwiązań multimedialnych*, [w:] M.J. Stankiewicz (red.), *Zarządzanie organizacjami w gospodarce opartej na wiedzy. Wyzwania strategiczne wobec organizacji*, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, Toruń, s. 333-342, ISBN 978-83-7285-404-9.

[19] **Kobis P.** (2009), *Obszary zastosowań systemów informatycznych w aspekcie wymiany informacji w dużych przedsiębiorstwach w Polsce*, [w:] L. Kiełtyka (red.), *Multimedia w biznesie i zarządzaniu*, Wyd. DIFIN, Warszawa, s. 115-122, ISBN 978-83-7641-129-3.

- Konferencji Naukowej „International Conference on Engineering Optimization" w 2008 roku w Rio de Janeiro w Brazylii, gdzie przyjęto i opublikowano moją wstępną koncepcję algorytmu w artykule pt. „The Corporate Network Optimization in Implementation of Computer Supported Collaborative Work"[20]. Mój udział w dyskusji, jak również samej konferencji został doceniony powołaniem mnie, już jako doktora, do International Scientific Committee, kolejnej, trzeciej organizowanej w dniach 1-5 lipca 2012 roku w Rio de Janeiro konferencji „International Conference on Engineering Optimization".

5.2. Osiągnięcia po uzyskaniu stopnia doktora

Po uzyskaniu stopnia doktora dalej rozwijałem swoje zainteresowania naukowe w zakresie zarządzania informacją. W dalszym ciągu prowadziłem badania skoncentrowane wokół zagadnień wymiany informacji, pracy grupowej i technik multimedialnych.

Poruszane w badaniach kwestie dotyczyły implementacji określonych rozwiązań multimedialnych w środowisku systemów operacyjnych[21] z zachowaniem obowiązujących międzynarodowych standardów transmisji obrazu i dźwięku H.323, G.711, G.723. Podejmowałem próby opracowania modelu pozwalającego na funkcjonowanie systemów pracy grupowej w organizacjach gospodarczych[22]. Opracowany model badałem również empirycznie w sieci lokalnej Wydziału Zarządzania Politechniki Częstochowskiej z użyciem aktualnych w owym czasie aplikacji do komunikacji multimedialnej.

W latach 2010-2011 wspólnie z Prof. Waldemarem Jędrzejczykiem prowadziłem badania dotyczące pracy grupowej w kontekście tworzenia efektywnych zespołów, efektywności funkcjonowania przedsiębiorstw oraz orientacji na pracę zespołową[23] oraz badania z zakresu

---

[20] **Kobis P.** (2008), *The Corporate Network Optimization in Implementation of Computer Supported Collaborative Work*, EngOpt 2008. International Conference on Engineering Optimization, Rio de Janeiro, Brazil, ISBN 978-85-7650156-5.

[21] **Kobis P.** (2011), *Poziom informatyzacji dużych przedsiębiorstw w Polsce w aspekcie wykorzystania grupowych systemów wspomagania decyzji oraz technik multimedialnych*, [w:] M. Pańkowska (red.), *Wiedza i komunikacja w innowacyjnych organizacjac. Komunikacja elektroniczna*, Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice, s. 208-226, ISBN 978-83-7246-683-9.

[22] **Kobis P.** (2010), *Procesy implementacji rozwiązań multimedialnych wspomagających wymianę informacji w organizacjach*, [w:] L. Kiełtyka, R. Kucęba, W. Jędrzejczyk (red.), *IT w organizacjach gospodarczych. Wybrane zagadnienia*, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, Toruń, s. 109-118, ISBN 978-83-7285-534-3.

Kobis P., Dudek D. (2010), *Information and Communication Technology in the Processes of Control and Corporate Governance*, Dnesne Trendy Inovacii. Zbornik prispevkov z medzinarodnej vedeckej konferencie. Trencin, Trencin, pp. 129-135, ISBN 978-80-89400-12-6.

[23] Jędrzejczyk W., **Kobis P.** (2011), *Aspects of Group Work*, [in:] L. Kiełtyka (ed.), *IT Tools in Knowledge Management in Organizations. Selected Problems*, Wydawnictwo PCz, Częstochowa, pp. 60-76, ISBN 978-83-7193-507-7.

Kobis P., Jędrzejczyk W. (2011), *Preferences for Group Work in the Light of Empirical Studies*, [in:] L. Varkoly (ed.), Present Day Trends of Innovations, Publish MiF, Dubnica nad Vahom, pp. 230-241, ISBN 978-80-89400-26-3.

Kobis P., Jędrzejczyk W. (2011), *Zalety i wady pracy grupowej w świetle badań empirycznych*, [w:] L. Kiełtyka (red.), *Narzędzia informatyczne w zarządzaniu. Wybrane zagadnienia*, Wydawnictwo PCz, Częstochowa, s. 153-171, ISBN 978-83-7193-510-7.

kapitału ludzkiego mające na celu określenie zdolności umysłowych i postaw psychologicznych, istotnych z punktu widzenia kluczowych kompetencji osobowych[24]. W badaniach dotyczących zagadnienia pracy grupowej rozpatrywałem następujące problemy badawcze:

- preferencje osobowe do pracy grupowej,
- organizacja pracy grupowej,
- mocne i słabe strony pracy grupowej,
- rola lidera w grupie zadaniowej,
- rozwiązywanie problemów decyzyjnych oraz konfliktów w grupie zadaniowej,
- diagnozy typów postaw osobowych, predestynujących do określonego trybu pracy/ nauki;
- rozpoznania preferowanego trybu pracy;
- zależności pomiędzy wyznaczonymi za pomocą testu psychologicznego typami postaw a własną oceną preferowanego trybu pracy/ nauki.

W badaniach dotyczących kapitału ludzkiego rozpatrywałem następujące problemy badawcze:

- diagnozy poziomu zdolności intuicyjnych;
- samooceny zdolności intuicyjnych;
- diagnozy typu postaw psychologicznych;
- samooceny preferowanego trybu pracy;
- zależności pomiędzy własną oceną preferencji a wskaźnikami określonymi za pomocą testów psychologicznych.

Wyniki badań przedstawiłem na konferencjach w kraju i za granicą: IX Międzynarodowej Konferencji „Multimedia w Biznesie i Zarządzaniu" w Wiśle w 2001 roku, International Scientific Conference „Present Day Trends of Innovations" DTI 2011 w Dubnica nad Váhom na Słowacji.

Badania w obszarze kapitału ludzkiego stały się impulsem i stanowiły przyczynek do dalszych moich dociekań naukowych związanych w okresie późniejszym z badaniem wpływu czynnika ludzkiego na zarządzanie bezpieczeństwem informacji. Stanowiły one dla mnie naturalną konsekwencję/kontynuację badań w zakresie pracy grupowej, w której dostrzegłem, że jednym z ważniejszych czynników warunkujących sprawne zarządzanie zasobami informacyjnymi jest bezpieczeństwo informacji i człowiek.

---

[24] Jędrzejczyk W., **Kobis P.** (2011), *Mental Abilities and Psychological Attitudes as Competencies in the Light of Empirical Studies*, [in:] L. Varkoly (ed.), Present Day Trends of Innovations, Publish MiF, Dubnica nad Vahom, pp. 104-109, ISBN 978-80-89400-26-3.

Behawioralny aspekt zarządzania przyczynił się również do mojego współorganizowania wraz z Prof. Waldemarem Jędrzejczykiem kolejnych trzech ogólnokrajowych spotkań naukowych na cyklicznej konferencji pt. „Behawioralizm w teorii i praktyce zarządzania współczesnymi organizacjami". Konferencje odbyły się w latach 2015, 2016 i 2018 z udziałem kilkudziesięciu ośrodków naukowych w Polsce. W każdej z konferencji pełniłem funkcję sekretarza naukowego i byłem współredaktorem naukowym 5 monografii naukowych:

1. Kiełtyka L., Jędrzejczyk W., **Kobis P.** (red.): Wyzwania współczesnego zarządzania. Tendencje w zachowaniach organizacyjnych, Dom Organizatora, Towarzystwo Naukowe Organizacji i Kierownictwa, Toruń 2015.
2. Jędrzejczyk W., **Kobis P.**, Kucęba R. (red.): Behawioralizm w teorii i praktyce zarządzania. Społeczny wymiar zarządzania zasobami ludzkimi, Monografia, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa 2016.
3. Kiełtyka L., Jędrzejczyk W., **Kobis P.** (red.): Wyzwania współczesnego zarządzania. Kreowanie kapitału intelektualnego organizacji, Monografia, Towarzystwo Naukowe Organizacji i Kierownictwa, 2016.
4. Jędrzejczyk W., **Kobis P.**, Kucęba R. (red.): Behawioralizm w teorii i praktyce zarządzania. Kreowanie kapitału ludzkiego, strukturalnego i społecznego organizacji, Monografia, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa 2017.
5. Kiełtyka L., Jędrzejczyk W., **Kobis P.** (red.): Wyzwania współczesnego zarządzania. Nowe technologie, innowacyjność, kompetencje, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, Toruń, 2018.

Od roku 2013 kontynuacja moich badań naukowych w aspekcie zarządzania informacją w przedsiębiorstwach dotyczyła dwóch wzajemnie przenikających się obszarów. Pierwszy z obszarów stanowił kontynuację moich dotychczasowych rozważań na temat pracy grupowej, wymiany i przetwarzania informacji między pracownikami. Został jednak wzbogacony o aspekty związane z wykorzystaniem chmury obliczeniowej w przetwarzaniu zasobów niematerialnych. Chmura obliczeniowa stanowiła naturalny rozwój w obszarze zarządzania informacją ze szczególnym uwzględnieniem pracy grupowej. Rozwój modelu SaaS (Software on a Service) stanął u podstaw przetwarzania informacji w grupach pracowniczych, rozwijając jednocześnie możliwości w aspekcie pracy mobilnej i pracy zdalnej. Zakres moich badań dotyczył mikro, małych i średnich podmiotów gospodarczych (MSP). Ta grupa przedsiębiorstw jest w kręgu moich zainteresowań naukowych do chwili obecnej. Wynika to z kilku czynników.

Przede wszystkim przedsiębiorstwa MSP w przeważającej liczbie przypadków nie mają własnych działów IT, a przez to nie mają własnych wypracowanych praktyk zarządzania informacją, wewnętrznych polityk w aspekcie pracy grupowej oraz zarządzania bezpieczeństwem informacji. Sytuacja ta stwarza duże pole do badań i wypracowywania naukowych podstaw w postaci systemów, modeli, algorytmów, które mogą znaleźć zastosowanie w praktyce. Podmioty z sektora MSP, według moich obserwacji, są również bardzicj „otwarte" na współpracę z badaczami, przez co istnieje możliwość pozyskania większej ilości niezbędnych do badań danych i informacji. Powyższe wnioski wysuwam na podstawie porównania ze swoimi wcześniejszymi doświadczeniami podczas badań przedsiębiorstw dużych, również przy realizacji swojej pracy doktorskiej. Przedsiębiorstwa z sektora MSP są ponadto o wiele bardziej zróżnicowane, zarówno pod względem poziomu zarządzania zasobami informacyjnymi w wielu aspektach, jak i pod względem organizacyjnym (np. firmy rodzinne). Jest to dodatkowy w moim odczuciu pozytywny aspekt wpływający na poziom „ciekawości" naukowej.

Jak wspomniałem wcześniej, moje badania od roku 2013 dotyczyły dwóch wzajemnie przenikających się obszarów zarządzania informacją. W związku z tym trudno jest jednoznacznie przydzielić grupę publikacji do danego obszaru, ponieważ zawarte w nich rozważania często dotyczą dwóch obszarów mimo, w zależności od pozycji, dominacji jednego z nich. Mogę stwierdzić jednak, że moje zainteresowania w obszarze zarządzania bezpieczeństwem informacji były coraz intensywniejsze.

Chcąc jednak dokonać podziału między ww. obszarami z wyraźnym zaznaczeniem przenikania poszczególnych aspektów w publikacjach, mogę stwierdzić, że w ramach obszaru zarządzania informacją w aspekcie jej wymiany i przetwarzania, również z użyciem chmury obliczeniowej opublikowałem łącznie 23 publikacje.

W moich rozważaniach naukowych podejmowałem problematykę związaną z efektywnością wykorzystywania chmur obliczeniowych w podmiotach gospodarczych[25]. Analizując efektywność wdrożeń cloud computingu (CC) w przedsiębiorstwach, bazowałem na ogólnie przyjętym w literaturze przedmiotu podejściu określającym efektywność jako rezultat podjętych działań, opisany relacją uzyskanych efektów do poniesionych nakładów, przy szacowaniu efektywności jako wykorzystania cząstkowych, syntetycznych wskaźników

[25] **Kobis P.** (2013), *Efektywność działalności firm z sektora MŚP przy wykorzystaniu rozwiązań cloud computingu*, [w:] O. Seroka-Stolka (red.), *Współczesne problemy zarządzania małym i średnim przedsiębiorstwem*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa, s. 222-231, ISBN 978-83-63500-39-9.

produktywności wykorzystania zasobów (pracy, kapitału)[26]. Rozważania teoretyczne konfrontowałem również z badaniami największych wywiadowni na świecie oraz danymi publikowanymi przez największe firmy świadczące usługi modelu cloud computing. Wykorzystując najbardziej aktualne wówczas opracowania literatury polskiej i światowej, podejmowałem próby określenia ekonomicznych aspektów implementacji rozwiązań CC w podmiotach gospodarczych. Analizując wymianę danych i informacji w przedsiębiorstwach w swoich badaniach, brałem pod uwagę każdy rodzaj chmury obliczeniowej z jednoczesnym określaniem powiązań z poszczególnymi usługami. Wynikało to ze specyfiki działalności przedsiębiorstw, które przetwarzają zarówno dane i informacje powszechnie uznawane za ogólnodostępne, jak i dane i informacje wymagające szczególnej ochrony oraz sensytywne chronione określonymi przepisami prawa. Szerokie spektrum zarządzanych informacji wymaga stosowania chmur publicznych, prywatnych, hybrydowych. Model współpracy chmur między sobą i przedsiębiorstwem przedstawiłem wraz z Prof. L. Kiełtyką na łamach „Przeglądu Organizacji" w 2013 roku[27].

Systematyczne, wedle badań literaturowych, zainteresowanie cloud computingiem na początku drugiej dekady XXI wieku przekładające się na fizyczne implementacje tych rozwiązań w podmiotach gospodarczych skutkowało stopniowym zmniejszaniem wśród przedsiębiorstw własnych działów IT. Zarządzanie zasobami informatycznymi zostało delegowane w dużej mierze poza obręb przedsiębiorstw do dostawców CC. Funkcjonowanie fizycznych serwerów w przedsiębiorstwach przestało być celowe, przez co i obsługa tych urządzeń stawała się zbędna. Wzbudzało to dość intensywną dyskusję naukową dotyczącą zagadnienia redukcji i fluktuacji miejsc pracy. Temu tematowi również poświęciłem publikację pt. „Fluktuacja miejsc pracy w aspekcie popularyzacji technologii cloud computingu"[28].

W kolejnych publikacjach naukowych z zakresu zarządzania informacją z użyciem nowych technologii oraz wykorzystywania nowego modelu zarządzania informacją, jakim jest cloud computing, podejmowałem takie tematy badawcze, jak:

- Bezpieczeństwo wykorzystywania chmur obliczeniowych[29].

---

[26] J. Adamczyk, A. Nehring (1995), *Efektywność przedsiębiorstw sprywatyzowanych*, Wydawnictwo Akademii Ekonomicznej w Krakowie, Kraków, s. 33.

[27] Kiełtyka L., **Kobis P.** (2013), *Ekonomiczne aspekty wirtualizacji zasobów informatycznych przedsiębiorstw*, „Przegląd Organizacji", Nr 4 (879), s. 13-19, ISSN 0137-7221.

[28] **Kobis P.** (2013), *Fluktuacja miejsc pracy w aspekcie popularyzacji technologii cloud computingu*, [w:] B. Ziółkowska (red.), *Wybrane problemy z teorii i praktyki zarządzania wartością w przedsiębiorstwie*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa, s. 156-165, ISBN 978-83-63500-42-9.

[29] **Kobis P.** (2013), *Czynniki warunkujące bezpieczne i efektywne wykorzystywanie cloud computingu w przedsiębiorstwach*, [w:] H. Howaniec, I. Szewczyk, W. Waszkielewicz (red.), *Informacje i marketing w działalności organizacji*, Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, Bielsko Biała, s. 93-105, ISBN 978-83-63713-42-3.

- Szanse i zagrożenia w procesie wykorzystywania cloud computingu[30].
- Konkurencyjność przedsiębiorstw w aspekcie wykorzystania cloud computingu[31].
- Korzyści z wykorzystywania modelu SaaS w podmiotach gospodarczych[32].
- Czynniki warunkujące rozwój i wybór chmur obliczeniowych w przedsiębiorstwach[33].
- Formy wykorzystywania aplikacji informatycznych w podmiotach gospodarczych do zarządzania zasobami informacyjnymi[34].
- Zarządzanie procesami biznesowymi z użyciem technik i technologii informatycznych[35].
- Aspekty zrównoważonego rozwoju przedsiębiorstw w świetle wykorzystania chmury obliczeniowej[36].
- Technologie mobilne w procesie zarządzania informacją w przedsiębiorstwach[37].
- Aspekt jakościowy wirtualizacji spotkań grup roboczych i przetwarzania informacji[38].

---

[30] **Kobis P.** (2013), *Istota cloud computing oraz szanse i zagrożenia związane z wykorzystaniem chmury obliczeniowej*, [w:] L. Kiełtyka (red.), *Technologie informacyjne w funkcjonowaniu organizacji. Zarządzanie z wykorzystaniem multimediów*, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, Toruń, s. 213-222, ISBN 978-83-7285-692-0.
Kobis P. (2013), *Korzyści i wydatki finansowe wynikające z implementacji elementów Cloud Computing w małych firmach*, [w:] L. Kiełtyka (red.), *Technologie informacyjne w funkcjonowaniu organizacji. Zarządzanie z wykorzystaniem multimediów*, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, Toruń, s. 223-234, ISBN 978-83-7285-692-0.
Kobis P. (2015), *Zarządzanie zasobami informacyjnymi przedsiębiorstw z wykorzystaniem chmur obliczeniowych*, Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie, s. 91-100, ISSN 2083-1560.

[31] **Kobis P.** (2013), *Konkurencyjność przedsiębiorstw sektora MSP w aspekcie implementacji rozwiązań z zakresu cloud computingu*, [w:] Z.E. Zieliński (red.), *Rola informatyki w naukach ekonomicznych i społecznych. Innowacje i implikacje interdyscyplinarne*, t. 1, Wydawnictwo Wyższej Szkoły Handlowej, Kielce, s. 11-20, ISBN 978-83-89274-80-9.
Kobis P. (2016), *Employee Mobility in Light of Cloud Computing Model*, „Przedsiębiorczość i Zarządzanie", t.17, cz.1, z.7, s. 159-172, ISSN 1733-2486.

[32] **Kobis P.**, Chmielarz G. (2017), *The Barriers and Benefits of Implementing Cloud Computing in Economic Organizations*, „Informatyka Ekonomiczna", Nr 3(45), s. 66-79, ISSN 1507-3858.

[33] **Kobis P.** (2017), *Czynniki kształtujące wybór informatycznego modelu zarządzania informacją*, „Marketing i Rynek", Nr 7, s. 327-340, ISSN 1231-7853.
Kobis P., Wrzalik A. (2017), *Narzędzia e-marketing wspierające prosumpcję w sektorze MSP*, [w:] J. Popczyk, R. Kucęba, K. Dębowski, W. Jędrzejczyk (red.), *Energetyka prosumencka. Konsolidacja problematyki społecznej, ekonomicznej i technicznej w aspekcie transformacji polskiego rynku energii elektrycznej*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa, s. 227-236, ISBN 978-83-65951-16-8.

[34] **Kobis P.** (2013), *Nowe formy organizacji zasobów informatycznych w przedsiębiorstwach*, Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie, Nr 10, s. 7-18, ISSN 2083-1560.
Kobis P. (2016), *Prosumpcja w rozwoju platform e-commerce*, [w:] J. Popczyk, R. Kucęba, K. Dębowski, W. Jędrzejczyk (red.), *Energetyka prosumencka. Próba konsolidacji w aspektach: przyrodniczym, społecznym, ekonomicznym i technicznym*, Wydawnictwo Politechniki Śląskiej, Gliwice, s. 290-300, ISBN 978-83-7880-407-9.

[35] Dudek D., **Kobis P.** (2013), *The Concept of the Intelligent Enterprise Management System*, [in:] L. Varkoly (ed.), Present Day Trends of Innovations 3, Publish MiF, Dubnica nad Vahom, pp. 34-41, ISBN 978-80-89400-59-1.

[36] **Kobis P.** (2014), *Nowe formy zarządzania informacją wspierające zrównoważony rozwój przedsiębiorstw*, [w:] I.K. Hejduk (red.), *Koncepcja sustainability wyzwaniem współczesnego zarządzania*, Oficyna Wydawnicza Szkoła Główna Handlowa w Warszawie, Warszawa, s. 93-103, ISBN 978-83-7378-929-6.
Kobis P. (2014), *Ochrona środowiska w aspekcie stosowania nowych rozwiązań z zakresu technologii informacyjnych*, [w:] W. Bajdur (red.), *Światowy Dzień Bezpieczeństwa i Ochrony Zdrowia w Pracy. Chemiczne zagrożenia środowiskowe. Aspekty teoretyczne i praktyczne*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa, s. 155-162, ISBN 978-83-65179-11-1.

[37] **Kobis P.** (2015), *Zastosowanie technologii mobilnych w biznesie*, [w:] L. Kiełtyka, W. Jędrzejczyk (red.), *Wykorzystanie potencjału współczesnych technologii informacyjnych w zarządzaniu organizacjami*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa, s. 69-79, ISBN 978-83-7193-627-2.

[38] **Kobis P.** (2014), *Wirtualizacja spotkań grup roboczych w przedsiębiorstwach – aspekt jakościowy*, [w:] M. Dudek, A. Madyda, D. Sala, W. Waszkielewicz (red.), *Metodyczno-instrumentalne aspekty inżynierii produkcji*, Wydawnictwa AGH, Kraków, s. 197-207, ISBN 978-83-7464-705-2.

Publikacje naukowe opracowane w ramach powyższej tematyki powstały m.in. w wyniku krytycznej analizy bibliograficznej, zarówno polskiej, jak i światowej. W ramach mojej pracy naukowej śledziłem na przestrzeni lat badania, raporty publikowane przez największe wywiadownie na świecie oraz firmy, takie jak: Microsoft, IBM, Google, Cisco. Przegląd badań, ich porównanie, analiza związana ze sposobem doboru prób badawczych, modelu badań umożliwiła mi wypracowanie własnych praktyk i przeniesienie ich na grunt lokalny, czego efektem były realizowane przeze mnie badania na terenie województwa śląskiego. Badania te prowadziłem dwukrotnie, w roku 2013 (podmioty duże i sektor MSP) oraz w roku 2015 (sektor MSP). Zakres badań obejmował takie aspekty, jak:

- Praca mobilna pracowników przedsiębiorstw.
- Zdalne wykorzystywania zasobów informacyjnych podmiotów gospodarczych.
- Świadomość menedżerów przedsiębiorstw w zakresie możliwości wykorzystywania cloud computingu.
- Poziom wykorzystania modelu cloud computing w przedsiębiorstwach.
- Analiza oprogramowania używanego do zarządzania zasobami informacyjnymi.

Wyniki badań zostały przedstawione i opublikowane w ramach projektu „PITWIN – Portal Innowacyjnego Transferu Wiedzy w Nauce" współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Społecznego[39], publikacji w Zeszytach Naukowych Politechniki Częstochowskiej[40] oraz IV Kongresu Zarządzania w Warszawie w 2016 roku[41].

Jak wspomniałem wcześniej, od 2013 roku coraz silniej moje zainteresowania naukowe wzbudzały aspekty bezpieczeństwa zarządzania informacją, które w literaturze naukowej były również poruszane w coraz większym zakresie. Pojawiały się one praktycznie w każdym analizowanym obszarze badań. Analizowana przeze mnie naukowo wcześniej wymiana i przetwarzanie informacji w ramach pracy grupowej, używanie nowych technik i technologii multimedialnych, modelu cloud computing pozwoliła mi na inne spojrzenie w aspekcie zarządzania informacją. Powszechnie wykorzystywane systemy, technologie oraz modele

---

Kobis P. (2014), *Wpływ nowych technologii przetwarzania informacji na kompleksowe zarządzanie jakością*, [w:] E. Kulej-Dudek, P. Pypłacz, K. Smoląg (red.), *Rozwój i doskonalenie funkcjonowania organizacji - aspekty teoretyczne i praktyczne*, Wydawnictwo PCz, Częstochowa, s. 129-137, ISBN 978-83-7193-613-5.

Kobis P. (2014), *Zjawisko prosumpcji w aspekcie wykorzystywania rozwiązań informatycznych*, [w:] J. Popczyk, R. Kucęba, K. Dębowski, W. Jędrzejczyk (red.), *Energetyka prosumencka. Pierwsza próba konsolidacji*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa, s. 156-163, ISBN 978-83-63500-92-4.

Kobis P. (2015), *Wirtualizacja zasobów informacyjnych organizacji gospodarczych – era chmury obliczeniowej*, „Przegląd Organizacji", Nr 2 (901), s. 34-42, ISSN 0137-7221.

[39] **Kobis P.** (2013), *Konkurencyjność przedsiębiorstw sektora MSP*... (op. cit)

[40] **Kobis P.** (2013), *Nowe formy organizacji zasobów informatycznych*... (op. cit)

41 **Kobis P.** (2016), *Świadomość i zakres wykorzystania przez firmy polskiego sektora MŚP rozwiązań chmurowych*, [w:] W. Sroka (red.), *Zarządzanie współczesnym przedsiębiorstwem. Uwarunkowania, trendy, perspektywy*, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, Toruń, s. 415-428, ISBN 978-83-7285-797-2.

rozwiązań teleinformatycznych służące zarządzaniu informacją jawiły mi się już nie tylko jako przestrzeń do wymiany i przetwarzania zasobów niematerialnych, ale również jako przestrzeń do walki konkurencyjnej na rynku gospodarczym oraz przestrzeń, w której nader często dochodzi do zjawisk cyberprzestępczości. W kolejnych moich publikacjach podejmowałem tematykę bezpiecznego zarządzania informacją w przedsiębiorstwach z naciskiem na bezpieczną wymianę informacji poprzez sieci lokalne i globalną, jej przetwarzanie z użyciem nowych systemów stacjonarnych i mobilnych oraz magazynowanie na serwerach lokalnych i w chmurze obliczeniowej. Analiza bibliograficzna, szczególnie anglojęzyczna, studiowanie aktualnych raportów publikowanych przez międzynarodowe stowarzyszenia bezpieczeństwa informacji (np. ISACA, ISSA, AISA), kolejne badania w zakresie systemów bezpieczeństwa informacji doprowadziły do sprecyzowania moich zainteresowań w zakresie cyberbezpieczeństwa, a mianowicie do bezpieczeństwa informacji z uwzględnieniem czynnika ludzkiego. Od wielu lat można zaobserwować wzrost znaczenia błędów popełnianych przez człowieka w ogólnym zestawieniu odnotowywanych na świecie próbach nielegalnego pozyskania lub zniszczenia informacji.

Chciałbym nadmienić, iż obszar bezpieczeństwa informacji nie był również dla moich dotychczasowych rozważań obszarem obcym, gdyż pojawiał się w moich poprzednich opracowaniach naukowych. Podczas moich badań przed uzyskaniem stopnia doktora, w obszarze zarządzania informacją moje zainteresowanie naukowe wzbudził obszar technicznego bezpieczeństwa zasobów informacyjnych[42]. Dotyczył on zagadnień, takich jak:

- Oszustwa finansowe w obszarze elektronicznej wymiany informacji w instytucjach finansowych;
- Włamania do systemów informacyjnych przedsiębiorstw poprzez sieć Internet;
- Niszczenie danych i informacji;
- Sabotaż ze strony niezadowolonych pracowników (najczęściej z działów IT);
- Podsłuchy transmisji w sieciach komputerowych;

---

[42] **Kobis P.** (2003), *Responsibility and Threats Connected with Modern Technologies Implementation*, 5-th European Conference of Young Research and Science Workers in Transport and Telecommunications, TRANSCOM 2003, Section 3, Information Technologies Communication Systems and their Control,, Žilina, Slovak Republic, Published by University of Žilina, Žilina, s. 53-56, ISBN 80-8070-081-8.
Kobis P. (2005), *The Modern Information Technologies Supporting Groupware in Big Companies*, TRANSFER 2005, Vyuzivanie novych poznatkov v strojarskej praxi, Zbornik prednasok 7. medzinarodnej vedeckej konferencie, 2 diel, Trencin, s. 308-311, ISBN 80-8075-070-X.
Kobis P. (2005), *Wymiana informacji z użyciem oprogramowania na platformie systemowej GNU/LINUX*, [w:] L. Kiełtyka (red.), *Multimedia w biznesie i edukacji*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa, s. 113-117, ISBN 83-88469-28-2.
Kobis P. (2009), *Przechowywanie i archiwizacja danych z użyciem nowoczesnych technik informatycznych*, [w:] L. Kiełtyka (red.), *Techniki informatyczne w podmiotach gospodarczych. Wybrane zagadnienia*, Wydawnictwo PCz, Częstochowa, s. 62-71, ISBN 978-83-7193-449-0.

- Bezpieczeństwa podczas pracy grupowej;
- Bezpieczeństwa systemów operacyjnych;
- Przechowywania i archiwizacji danych.

Były to więc aspekty, które w wymiarze merytorycznym są aktualne do dnia dzisiejszego. Zmianie uległy techniczne sposoby nielegalnego pozyskiwania informacji oraz znaczny wzrost czynnika ludzkiego będącego w pewnym stopniu pochodną inżynierii społecznej, socjotechnik wykorzystywanych przez cyberprzestępców. Wykorzystanie czynnika ludzkiego do cyberprzestępczości wynikało i wynika nadal z faktu, że poziom zaawansowania współczesnych technik i technologii informatycznych służących zabezpieczaniu danych i informacji jest tak wysoce zaawansowany, iż wykorzystywanie błędów popełnianych przez pracowników, nakłanianie ich do określonych zachowań poprzez stosowanie socjotechnik stało się dużo łatwiejszym sposobem na nielegalne pozyskiwanie informacji.

Wracając do mojej pracy naukowej, po uzyskaniu stopnia doktora pierwszymi publikacjami dotyczącymi bezpieczeństwa informacji były opracowania poruszające kwestie bezpieczeństwa chmury obliczeniowej. Dotyczyły one zagadnień związanych z poziomem bezpieczeństwa przesyłanych i przechowywanych danych w poszczególnych krajach na świecie, walki z cyberprzestępczością oraz poziomem ochrony własności intelektualnej[43]. Powyższe aspekty rozpatrywałem w kontekście transgranicznej wymiany informacji wynikającej z istoty funkcjonowania cloud computingu. Przenosząc bowiem zasoby niematerialne przedsiębiorstwa do chmury obliczeniowej, należy mieć na uwadze zarówno poziom zabezpieczeń oferowanych przez firmy hostujące dane i informacje, jak i poziom prawodawstwa w poszczególnych krajach, które są siedzibami tych firm lub na terytorium których znajdują się infrastruktury teletechniczne. W moich opracowaniach pojawił się również aspekt bezpieczeństwa chmur publicznych. Dane umieszczone w publicznej chmurze obliczeniowej są dostępne z każdego komputera podłączonego do sieci. Znajdują się razem z danymi innych klientów. Wprawdzie każdy z użytkowników ma swoje kanały dostępowe uniemożliwiające podglądanie danych innych usługobiorców, ale sam fakt przechowywania danych w tej samej infrastrukturze może budzić niepokój. Zaniepokojenie może również wynikać z faktu, że powierzamy swoje zasoby obcej firmie, która, co prawda, gwarantuje i zapewnia maksymalny poziom bezpieczeństwa, ale przed użytkownikami zewnętrznymi. Sama, jeśli zechce, może bez problemu przeglądać nasze dane. Aspekt ten poruszył nawet Richard Stallman, założyciel i prezes Free Software Foundation. W wywiadzie dla dziennika

[43] **Kobis P.** (2013), *Czynniki warunkujące bezpieczne i efektywne* ... (op.cit.)

„The Guardian" wręcz ostrzega przed masowym wykorzystywaniem chmur, jednoznacznie twierdząc, że jest to po prostu pułapka. Jego zdaniem prywatne dane użytkowników nie powinny być powierzane zewnętrznym firmom, bo to oznacza, że chcą mieć do nich dostęp. Zdaniem Stallmana, uzależniamy się od zamkniętych rozwiązań opracowanych przez ludzi, na których pracę nie mamy żadnego wpływu. Wypowiedź prezesa Free Software Foundation może być nieco przesadzona, lecz wywołuje jednocześnie w pewnym stopniu niepokój i trudno w całości się z nią nie zgodzić. Należy jednak zaznaczyć, że dane, które mogą stanowić zainteresowanie osób trzecich, nie są zazwyczaj przetrzymywane w publicznych chmurach, lecz w chmurach prywatnych, które ww. niedogodności są pozbawione[44].

Kolejne moje badania z zakresu zarządzania bezpieczeństwem informacji dotyczyły wybranych problemów związanych z odpowiednim zabezpieczeniem informacji przetwarzanych w podmiotach gospodarczych. W obszarze moich zainteresowań pojawiły się zagadnienia związane z obowiązującymi zapisami prawnymi dotyczącymi bezpieczeństwa informacji oraz regulującymi sposoby jej magazynowania i przetwarzania[45]. Na podstawie badań literaturowych przedstawiałem możliwe do implementacji poziomy zabezpieczeń minimalizujące ryzyko utraty informacji oraz minimalizujące wpływ czynnika ludzkiego na bezpieczeństwo zasobów informacyjnych. Zestawiałem klasyczne cyberzagrożenia, których pojawienie się związane było z użyciem specjalnie spreparowanego szkodliwego oprogramowania z zagrożeniami bezpośrednio powodowanymi przez pracowników (np. z braku kompetencji, niezadowolenia z pracy, przekupienia przez konkurencję), grupy wspierane przez podmioty zewnętrzne. Przedstawiałem aktualnie obowiązujące zapisy legislacyjne w obszarze ochrony danych, zestawiając je z analizą przypadków naruszenia bezpieczeństwa ze szczególnym uwzględnieniem sieci Internet. Podejmowałem próby określenia zagrożeń wpływających na ryzyko utraty informacji, analizując dostępne, najnowsze w danym okresie badania i raporty największych światowych wywiadowni zestawiając je z podejmowanymi przez organizacje gospodarcze działaniami w celu zabezpieczenia posiadanych informacji[46].

---

[44] **Kobis P.** (2013), *Istota cloud computing oraz szanse i zagrożenia* ... (op.cit.)

[45] Chmielarz G., **Kobis P.** (2018): *Analiza przypadków naruszenia bezpieczeństwa danych osobowych oraz zmian legislacyjnych zachodzących w obszarze zarządzania ochroną danych osobowych*, „Marketing i Rynek", Nr 9, s. 120-137, ISSN 1231-7853.
Kobis P., Kisiołek A. (2018), *Zarządzanie bezpieczeństwem danych w przedsiębiorstwach MSP z uwzględnieniem czynnika ludzkiego - wyniki badań*, „Przegląd Organizacji", Nr 8, s. 44-52, ISSN 0137-7221.

[46] **Kobis P.** (2016), *Wybrane aspekty bezpieczeństwa danych elektronicznych w podmiotach gospodarczych*, [w:] P. Pypłacz, D. Dudek (red.), *Rozwój i doskonalenie funkcjonowania organizacji. Determinanty rozwoju współczesnych organizacji*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa, s. 89-98, ISBN 978-83-65179-48-7.

Przetwarzanie informacji wymaga obecnie stosowania coraz szybszych urządzeń komputerowych wyposażonych w zaawansowane oprogramowanie służące do agregacji, klasyfikacji, unifikacji, katalogowania i wyszukiwania danych. Ponadto, odrębne systemy pozwalają na generowanie nowych informacji z posiadanych już danych, porównując je i syntetyzując. Również specjalne aplikacje służą do wizualizacji magazynowanych danych, tworząc tym samym odrębny zestaw danych multimedialnych. Pliki multimedialne są generowane również z różnych aplikacji służących do komunikacji sieciowej lub też z wydarzeń typu: szkolenia, kampania reklamowa itp. Wszystkie wymienione zasoby wymagają stosowania określonych działań:

- magazynowania;
- utworzenia kanałów dostępowych;
- ochrony przed szkodliwym oprogramowaniem;
- tworzenia kopii bezpieczeństwa.

Biorąc pod uwagę powyższe czynniki, moje rozważania naukowe oscylowały również wokół bezpiecznych systemów określanych mianem Network-Attached Storage (NAS), nazywanych również w literaturze przedmiotu osobistą chmurą obliczeniową. Podejmowałem teoretyczne próby integracji NAS z chmurami publicznymi w zakresie niezbędnym dla bezpiecznego zarządzania informacją w podmiotach gospodarczych. Wynikiem badań było opracowanie sposobu implementacji i wykorzystywania tego typu urządzeń w przedsiębiorstwach. Swoje wyniki opublikowałem na International Scientific Conference & International Workshop „Present Day Trends of Innovations" w 2017 roku[47].

Opracowanie skutecznego systemu bezpieczeństwa informacyjnego w przedsiębiorstwie jest kluczowe dla ochrony wartości niematerialnych. Niemniej istotną kwestią jest jednak świadomość w zakresie potrzeby implementacji tego typu rozwiązań wśród menedżerów odpowiedzialnych za zasoby informacyjne. Poziom świadomości menedżerów w aspekcie ochrony danych i informacji opisałem w publikacji, której założenia przedstawiłem na XII Konferencji Naukowej „Multimedia w Biznesie i Zarządzaniu" w Koszęcinie w 2017 roku[48]. Zagadnienia związane ze świadomością menedżerów w zakresie konieczności implementacji odpowiednich zabezpieczeń, stosowania odpowiednich polityk bezpieczeństwa

47 **Kobis P.**, Chmielarz G. (2017), *Information Management in SME Sector Enterprises with the Use of NAS Storage Systems*, [in:] L. Varkoly, M. Zabovsky, R. Szczebiot (eds.), *Present Day Trends of Innovations 7*, Printing House of Lomza State University of Applied Sciences, Łomża, pp. 136-146, ISBN 978-83-60571-49-1.

48 **Kobis P.**, Dudek D. (2017), *Poziom świadomości menedżerów w aspekcie ochrony danych elektronicznych w przedsiębiorstwach*, [w:] L. Kiełtyka, A. Sokołowski (red.), *Techniki i technologie wspomagające funkcjonowanie przedsiębiorstw*, Wydawnictwo PCz, Częstochowa, s. 11-20, ISBN 978-83-7193-659-3.

informacji, organizowania cyklicznych szkoleń w tym zakresie, kończąc na konieczności systematycznego podnoszenia kompetencji pracowników przedsiębiorstw oraz odpowiedniego nadzorowania postepowania osób mających największe uprawnienia w zakresie przetwarzania informacji, wpisywały się w nurt moich rozważań w temacie wpływu czynnika ludzkiego na bezpieczeństwo informacji.

W roku 2016 przeprowadziłem badania w województwie śląskim wśród przedsiębiorstw sektora MSP. Badaniu poddałem wówczas 153 przedsiębiorstwa wybrane metodą doboru losowego prostego. Celem badań było określenie poziomu świadomości menedżerów IT lub osób odpowiedzialnych w organizacjach za bezpieczeństwo zarządzania informacją oraz ich opinii nt. bezpiecznego przetwarzania informacji. Wyniki badań przedstawiłem na:

- konferencji naukowej „Perspektywy rozwoju przedsiębiorczości i zarządzania w gospodarce cyfrowej" w Tomaszowie Mazowieckim w 2017 roku, a następnie opublikowałem w czasopiśmie „Przegląd Nauk Ekonomicznych"[49].
- X Międzynarodowej Konferencji „Współczesne problemy zarządzania przedsiębiorstwem" w Szczyrku w 2017 roku, a następnie opublikowałem w Zeszytach Naukowych Wyższej Szkoły Humanitas, seria Zarządzanie w 2018 roku[50];
- Miesięczniku „Przegląd Organizacji" w 2018 roku[51].

W ramach przeprowadzonych badań opracowałem również model ochrony danych w tradycyjnym dziale IT oraz model ochrony danych w organizacjach wykorzystujących wszystkie aplikacje w chmurze obliczeniowej.

W obszarze rozważań naukowych na temat bezpieczeństwa zasobów informacyjnych pojawiły się również aspekty związane z outsourcingiem usług informatycznych. Rozważania były wynikiem analizowania możliwości zmniejszenia zagrożeń w podmiotach gospodarczych, które z różnych względów nie posiadały potencjału pozwalającego na skuteczną ochronę zasobów niematerialnych. Wśród zalet tego typu rozwiązań analizowałem zagadnienia w zakresie optymalizacji kosztów pracy, kontroli wydatków, dostępu do wykwalifikowanej kadry specjalistów, łatwiejszego wypełnienia luk kompetencyjnych oraz możliwości koncentracji przedsiębiorstw na głównym profilu działalności[52]. Wyniki moich przemyśleń

[49] **Kobis P.** (2017), *Zarządzanie w zakresie bezpieczeństwa informacji w małych i średnich przedsiębiorstwach*, „Przegląd Nauk Ekonomicznych", Nr 27, s. 187-196, ISSN 2544-221X.
[50] **Kobis P.** (2018), *Chosen Aspects of IT Resources Security in SME Sector Enterprises - Results of the Research*, Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie, Nr 2, t. 19, s. 211-229, ISSN 1899-8658.
[51] **Kobis P.**, Kisiołek A. (2018), *Zarządzanie bezpieczeństwem danych w przedsiębiorstwach MSP z uwzględnieniem czynnika ludzkiego - wyniki badań*, „Przegląd Organizacji", Nr 8, s. 44-52, ISSN 0137-7221.
[52] **Kobis P.** (2018), *Outsourcing IT w aspekcie bezpieczeństwa danych w organizacjach gospodarczych*, [w:] L. Kiełtyka, K. Smoląg (red.), *Współczesne wyzwania przedsiębiorstw - przegląd wybranych koncepcji zarządzania przedsiębiorstwem*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa, s. 61-71, ISBN 978-83-65951-34-2.

naukowych w tym zakresie przedstawiłem m.in. na XIII Konferencji Naukowej „Multimedia w Biznesie i Administracji" w Częstochowie w 2018 roku.

W każdym z rozpatrywanych, badanych przeze mnie obszarów zarządzania bezpieczeństwem informacji jako główny czynnik zwiększający ryzyko wystąpienia zagrożenia jawił się człowiek. Aspekt ten dotyczył wymiany informacji w środowisku pracowniczym, podczas pracy zdalnej, pracy w zespołach wirtualnych, podczas kontaktów z klientami podmiotu gospodarczego oraz osób trzecich, które z różnych, analizowanych później przeze mnie pobudek dążyły do nielegalnego pozyskania lub zniszczenia zasobów niematerialnych. Aspekt czynnika ludzkiego, działań socjotechnicznych wynikających z inżynierii społecznej stał się dla mnie najbardziej ciekawym naukowo obszarem badań związanych z ochroną informacji. Dodatkowym motywem w podjęciu kolejnych badań w aspekcie czynnika ludzkiego był fakt, że w literaturze przedmiotu właśnie ten czynnik jawił się jako najważniejszy, przeważający w procesach ochrony zasobów niematerialnych. Praktycznie wszystkie kolejne moje opracowania naukowe związane były z obszarem, w którym głównymi elementami były błędy popełniane przez człowieka, podatność na działania osób trzecich (socjotechnika), brak odpowiednich kompetencji w zakresie bezpieczeństwa informacji oraz inne czynniki, takie jak: zmęczenie, pośpiech, stres, przesadne zaufanie do osób trzecich, niezadowolenie z szeroko rozumianych warunków pracy, szpiegostwo gospodarcze, monotonia w procesie wykonywanych obowiązków.

Rozpatrywane przeze mnie zagadnienia naukowe można sklasyfikować jako:

- Rola czynnika ludzkiego w bezpieczeństwie wymiany informacji podczas spotkań wirtualnych, w tym: przekazywania informacji poprzez sieć Internet, zdalnego wykorzystywania zasobów informacyjnych przechowywanych w sieci lokalnej podmiotu, korzystania z informacji przechowywanej w chmurze obliczeniowej;
- Czynniki zależące od pracowników w zakresie bezpieczeństwa zasobów informacyjnych;
- Analiza dostępnych metod szacowania ryzyka w zakresie potencjalnego zniszczenia lub utraty informacji na rzecz osób/podmiotów nieupoważnionych, np. CRAMM, COBRA, MARION, FMEA, OCTAVE, MEHARI, ze szczególnym uwzględnieniem norm ISO;
- Elementy organizacyjno-proceduralne bezpieczeństwa informacji w aspekcie czynnika ludzkiego uwzględniające pojęcia związane z cyberhigieną;
- Aspekty czynnika ludzkiego w kontekście bezpieczeństwa informacji zarządzanej z użyciem tradycyjnego modelu IT i modelu cloud computing;

- Bezpieczeństwo zasobów informacyjnych podczas obsługi popularnych aplikacji komputerowych w aspekcie czynnika ludzkiego przy jednoczesnym wyszczególnieniu cech psychofizycznych i kompetencji pracowniczych powodujących potencjalne zagrożenia dla zasobów niematerialnych;
- Wpływ pandemii Covid-19 ma bezpieczeństwo informacji w aspekcie pracy zdalnej z uwzględnieniem czynnika ludzkiego.

W zakresie bezpieczeństwa informacji z uwzględnieniem czynnika ludzkiego prowadziłem badania naukowe obejmujące swoim zasięgiem zarówno obszar Polski, jak i badania obejmujące teren województwa śląskiego. Główne moje badania opublikowałem w mojej monografii naukowej pt. „Zarządzanie bezpieczeństwem informacji w systemach informacyjnych małych i średnich przedsiębiorstw z uwzględnieniem czynnika ludzkiego", która ukazała się w 2021 roku nakładem wydawnictwa Stowarzyszenie Wyższej Użyteczności „Dom Organizatora" w Toruniu.

Część badań opracowywałem wspólnie z innymi pracownikami naukowymi, w tym z Prof. Olehem Karyy z Uniwersytetu Naukowego „Politechnika Lwowska", z którym to Uniwersytetem współpracuję naukowo od 2018 roku. Wyniki badań zostały wygłoszone i opublikowane w ramach XI Międzynarodowej Konferencji Naukowej „Przemysł 4.0 – wyzwania i rozwiązania dla marketingu i zarządzania" w Szczyrku[53], 28-30 listopada 2019 roku, 35th International Business Information Management Association Conference, która odbyła się 1-2 kwietnia 2020 roku w Seville w Hiszpanii[54] (indeksowana w bazach Web of Science) oraz opublikowane w czasopismach: „Operations Research and Decisions"[55] (indeksowane w bazach Scopus i Web of Science) i „Przegląd Organizacji" (indeksowany w bazie ERIH Plus)[56].

Podczas mojej współpracy z Katedrą Zarządzania Organizacjami Narodowego Uniwersytetu „Politechnika Lwowska" oraz Wielkopolską Wyższą Szkołą Społeczno-Ekonomiczną w Środzie Wlkp. w 2021 roku uruchomiony został międzynarodowy, interdyscyplinarny projekt naukowy pt. „Transformacja cyfrowa marketingu szkół wyższych" realizowany na terenie Polski, Ukrainy, Białorusi i Czech (https://edu-marketing.eu). Angażując się

[53] **Kobis P.** (2021), *Human Factor Aspects in Information Security Management in the Traditional IT and Cloud Computing Models*, „Operations Research and Decisions", No 1, vol. 31, pp. 61-76, ISSN 2081-8858.
[54] **Kobis P.** (2020), *Technological, Behavioral, and Organizational-Procedural Aspects of Management of Safety Information in Companies*, [in:] K.S. Soliman (ed.), *Education Excellence and Innovation Management: a 2025 Vision to Sustain Economic Development during Global Challenges*, International Business Information Management Association (IBIMA), Norristown, pp. 2405-2415, ISBN 978-0-9998551-4-1.
[55] **Kobis P.** (2021), *Human Factor Aspects…* (op. cit.)
[56] **Kobis P.**, Kisiołek A., Karyy O., Chmielarz G. (2021), *Threats to Information Security Driven by Human Factor in the Perception of Persons in Charge of Intangible Resources Management*, „Przegląd Organizacji", No 5, pp. 19-27, ISSN 0137-7221.

w projekt, będąc jego wykonawcą, autorem elektronicznej platformy oraz głównym koordynatorem w części dotyczącej bezpieczeństwa informacji z uwzględnieniem czynnika ludzkiego, prowadzę badania dotyczące wpływu czynnika ludzkiego na bezpieczeństwo informacji w uczelniach wyższych wymienionych krajów. Tym samym w moich rozważaniach naukowych postanowiłem wyjść poza obszar samych przedsiębiorstw i badać wpływ czynnika ludzkiego na bezpieczeństwo zasobów informacyjnych również w innych obszarach zarządzania informacją. Stanowi to dla mnie obszar kolejnych wyzwań naukowych, w których planuję badania w zakresie bezpieczeństwa zasobów niematerialnych w przyszłości.

Analizując mój dorobek w zakresie artykułów naukowych dotyczących zagadnień z zakresu zarządzania bezpieczeństwem zasobów informacyjnych, mogę wymienić 10 najbardziej, moim zdaniem, znaczących pozycji:

1. **Kobis P.**, Chmielarz G. (2017), *Information Management in SME Sector Enterprises with the Use of NAS Storage Systems*, [in:] L. Varkoly, M. Zabovsky, R. Szczebiot (eds.), *Present Day Trends of Innovations 7*, Printing House of Lomza State University of Applied Sciences, Łomża, pp. 136-146, ISBN 978-83-60571-49-1.
2. **Kobis P.** (2017), *Zarządzanie w zakresie bezpieczeństwa informacji w małych i średnich przedsiębiorstwach*, „Przegląd Nauk Ekonomicznych", Nr 27, s. 187-196, ISSN 2544-221X.
3. **Kobis P.** (2018), *Chosen Aspects of IT Resources Security in SME Sector Enterprises - Results of the Research*, Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie, Nr 2, t. 19, s. 211-229, ISSN 1899-8658.
4. **Kobis P.** (2019), *Człowiek w zespołach wirtualnych a bezpieczeństwo w zarządzaniu informacją*, „Przegląd Organizacji", Nr 7, s. 57-64, ISSN 0137-7221.
5. **Kobis P.** (2019), *Human Factor in the Aspect of Digital Information in Business Enterprises*, [in:] A. Dunay (ed.), *People, Planet and Profit: Sustainable Business and Society*, Vol.2, Szent Istvan University Publishing, Godollo, pp. 35-42, ISBN 978-963-269-882-3.
6. **Kobis P.** (2020), *Information Risk Management in SME Sector Enterprises*, „International Scientific Journal INDUSTRY 4.0", Vol. 5, Iss. 2, 2020, pp. 79-83, ISSN 2543-8582.
7. **Kobis P.** (2020), *Technological, Behavioral, and Organizational-Procedural Aspects of Management of Safety Information in Companies*, [in:] K.S. Soliman (ed.), *Education Excellence and Innovation Management: a 2025 Vision to Sustain Economic Development during Global Challenges*, International Business Information Management Association (IBIMA), Norristown, pp. 2405-2415, ISBN 978-0-9998551-4-1.

8. **Kobis P.** (2021), *Human Factor Aspects in Information Security Management in the Traditional IT and Cloud Computing Models*, „Operations Research and Decisions", No 1, vol. 31, pp. 61-76, ISSN 2081-8858.
9. **Kobis P.**, Kisiołek A., Karyy O., Chmielarz G. (2021), *Threats to Information Security Driven by Human Factor in the Perception of Persons in Charge of Intangible Resources Management*, „Przegląd Organizacji", No 5, pp. 19-27, ISSN 0137-7221.
10. **Kobis P.** (2021), *Impact of the human factor on the security of information resources of enterprises during the Covid-19 pandemic*, The 5th International MultiConference of Management Science 2021 (IMMS 2021), 29 July, Bangkok, Thailand, pp. 143-155.

Na dzień 17.12.2021 r. w druku są moje kolejne publikacje wygłoszone na konferencjach krajowych w 2021 roku: „Rola czynnika ludzkiego w procesach zarządzania bezpieczeństwem zasobów informacyjnych przedsiębiorstw" oraz „Wpływ pandemii COVID-19 na bezpieczeństwo zasobów informacyjnych organizacji gospodarczych", które ukażą się jako rozdziały w monografiach naukowych.

Pozytywne recenzje otrzymała również praca naukowa pt. „Impact of the human factor on the security of information resources of enterprises during the Covid-19 pandemic", którą opracowałem we współpracy z Prof. Olehem Karyy, a która wydana zostanie w czasopiśmie „Polish Journal of Management Studies" (indeksowana w Web of Science, SCOPUS), stanowiąca rozwinięcie moich przemyśleń i badań naukowych wygłoszonych na konferencji IMMS 5th International MultiConference of Management Science, która odbyła się w lipcu 2021 roku w Bangkoku w Tajlandii.

6. Informacja o wykazywaniu się istotną aktywnością naukową w więcej niż jednej uczelni, instytucji naukowej lub instytucji kultury, w szczególności zagranicznej

6.1. Współpraca z Uniwersytetem Narodowym „Politechnika Lwowska"

W mojej pracy naukowej od roku 2018 podjąłem współpracę z Katedrą Zarządzania Organizacjami Narodowego Uniwersytetu „Politechnika Lwowska". Efektem współpracy są następujące publikacje:

1) Kisiołek A., Karyy O., **Kobis P.**, Prokopenko O. (2018), *Internet as a Communication Tool at the Service of a Higher Education Institution – a Respective for the Education Markets of Poland and Ukraine*, Visnik Nacional'nogo Universitetu „L'vivs'ka Politechnika", No. 899, pp. 91-99, ISSN 0321-0499.
2) Kisiołek A., Karyy O., **Kobis P.** (2021), *Marketing of Higher Education Institutions in the Digital Economy Era*, [in:] L. Kiełtyka, K. Smoląg (eds.), *Wybrane uwarunkowania i determinanty rozwoju współczesnych przedsiębiorstw*, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, Toruń, pp. 15-34, ISBN 978-83-7285-981-5.
3) Dzyubina A., Karyy O., Kisiołek A., **Kobis P.** (2021), *Current Trends in E-Commerce: Global and Ukrainian Directions*, [in:] L. Kiełtyka, K. Smoląg (eds.), Wybrane uwarunkowania i determinanty rozwoju współczesnych przedsiębiorstw, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, Toruń, pp. 35-47, ISBN 978-83-7285-981-5.
4) **Kobis P.**, Kisiołek A., Karyy O., Chmielarz G. (2021), *Threats to Information Security Driven by Human Factor in the Perception of Persons in Charge of Intangible Resources Management*, „Przegląd Organizacji", No 5, pp. 19-27, ISSN 0137-7221.
5) Artykuł przyjęty do druku, po pozytywnych recenzjach: **Kobis P.**, Karyy O., *Impact of the Human Factor on the Security of Information Resources of Enterprises During the Covid-19 Pandemic*, Polish Journal of Management Studies.

W roku 2021 przy współpracy z Uniwersytetem Narodowym „Politechnika Lwowska" oraz Wydziałem Ekonomicznym Wielkopolskiej Wyższej Szkoły Społeczno-Ekonomicznej w Środzie Wlkp. uruchomiony został międzynarodowy projekt badawczy pt. „*Transformacja*

cyfrowa marketingu szkół wyższych". Prace nad projektem trwały od 2020 roku. Projekt ma charakter interdyscyplinarny, który łączy zagadnienia z zakresu marketingu internetowego szkół wyższych z zagadnieniami dotyczącymi bezpieczeństwa informacji zarządzanych przez badane uczelnie przy uwzględnieniu czynnika ludzkiego. Badania obejmują 4 kraje: Polskę, Ukrainę, Białoruś i Czechy i są skierowane do uczelni publicznych i niepublicznych w badanych krajach.

Jestem współautorem projektu, autorem platformy internetowej oraz głównym koordynatorem w części badań dotyczących bezpieczeństwa informacji z uwzględnieniem czynnika ludzkiego.

Projekt jest uruchomiony pod adresem internetowym: https://edu-marketing.eu. W przygotowaniu jest monografia, której część empiryczną stanowić będą badania z tego projektu.

W ramach współpracy z Uniwersytetem Narodowym „Politechnika Lwowska" należę również do zespołu recenzentów czasopisma „Journal of Lviv Polytechnic National University. Series of Economics and Management Issues", ISSN 2522-1639 (print), 2663-0257 (online). Strona internetowa czasopisma: https://science.lpnu.ua/semi.

Załączniki (umieszczone w części „Pozostałe dokumenty" w punkcie „Zaświadczenia, certyfikaty oraz inne dokumenty potwierdzające aktywności"):

- ***Zaświadczenie o współpracy (autorzy: Prof. dr hab. Nataliya Chukhray, Prorektor ds. Edukacji i współpracy międzynarodowej Narodowego Uniwersytetu „Politechnika Lwowska" oraz Prof. dr hab. Oleh Karyy, kierownik Katedry Zarządzania Organizacjami Narodowego Uniwersytetu „Politechnika Lwowska")***

6.2. Współpraca z Wielkopolską Wyższą Szkołą Społeczno-Ekonomiczną w Środzie Wielkopolskiej

W ramach współpracy naukowej z Wielkopolską Wyższą Szkołą Społeczno-Ekonomiczną w Środzie Wielkopolskiej w latach 2018-2019 byłem członkiem Advisory Committee, cyklicznej publikacji naukowej pt. „Studies of economic and social processes".

W roku 2020 byłem członkiem Editorial Board monografii naukowej: J. Babiak, A, Kisiołek, K. Urbaniak (red.) „*Socio-Economic Inequalities. Poland, Europe, World*", Bogucki Wydawnictwo Naukowe, Poznań, Środa Wielkopolska, 2020.

W roku obecnym (2021) jestem członkiem Editorial Board monografii naukowej: Babiak J., Kisiołek A., „*The world during and after the pandemic*", The Great Poland University of Social and Economics in Środa Wlkp. & Bogucki Wydawnictwo Naukowe, Poznań–Środa Wielkopolska 2021. Wydanie monografii planowane jest w pierwszym kwartale 2022 roku.

Załączniki (umieszczone w części „Pozostałe dokumenty" w punkcie „Zaświadczenia, certyfikaty oraz inne dokumenty potwierdzające aktywności"):

- ***Zaświadczenie o współpracy nr 1 (autor: Prof. dr hab. Ireneusz Kubiaczyk, Rektor Wielkopolskiej Wyższej Szkoły Społeczno-Ekonomicznej)***
- ***Zaświadczenie o współpracy nr 2 (autor: Prof. dr hab. Ireneusz Kubiaczyk, Rektor Wielkopolskiej Wyższej Szkoły Społeczno-Ekonomicznej)***

6.3. Członkostwo w Towarzystwie Naukowym Organizacji i Kierownictwa

Od roku 2005 jestem członkiem Towarzystwa Naukowego Organizacji i Kierownictwa w Częstochowie, uhonorowanym w 2010 roku Srebrną Odznaką Honorową Towarzystwa.

W kadencji 2013-2017 oraz 2017 – nadal, jestem członkiem Zarządu TNOiK Oddział w Częstochowie.

Jako członek byłem współwykonawcą projektu realizowanego wraz z Narodowym Funduszem Ochrony Środowiska i Gospodarki Wodnej (umowa nr 564/2015/Wn50/EE-se/D) pt. „Zanim udusi nas SMOG – Społecznościowa Platforma Transferu Wiedzy (SPTW)". Celem projektu było uświadamianie i kształcenie społeczności lokalnej w obszarze ochrony środowiska i zrównoważonego rozwoju w aspekcie przeciwdziałania niskiej emisji. Istotne w tym zakresie było również propagowanie sposobów redukcji niskiej emisji oraz uświadomienie odbiorców odnośnie zagrożeń i następstw zdrowotnych powstających na skutek spalania odpadów, jak również ogrzewania budynków paliwami niskiej jakości. Projekt był realizowany przez oddział TNOiK w Częstochowie od kwietnia 2015 r. do sierpnia 2017 r. Przeszkolono następującą liczbę uczestników: 795 mieszkańców, 105 przedsiębiorców, 167 nauczycieli i 35 lokalnych liderów. W ramach projektu byłem również autorem i wykonawcą internetowej Społecznościowej Platformy Transferu Wiedzy, pełniąc funkcję administratora platformy w zakresie odpowiedzialności w obszarze zarządzania przetwarzanymi i przechowywanymi informacjami oraz bezpieczeństwa platformy.

Załączniki (umieszczone w części „Pozostałe dokumenty" w punkcie „Zaświadczenia, certyfikaty oraz inne dokumenty potwierdzające aktywności"):

- *Karta aplikacji produktu, będącego wynikiem badań naukowych lub prac rozwojowych prowadzonych w Politechnice Częstochowskiej*

7. Informacja o osiągnięciach organizacyjnych, dydaktycznych oraz popularyzujących naukę

W trakcie mojej pracy naukowej byłem współorganizatorem łącznie 21 Międzynarodowych i Krajowych Konferencji Naukowych (6 przed uzyskaniem stopnia doktora i 15 po uzyskaniu stopnia doktora), w których pełniłem funkcje sekretarza naukowego i członka komitetu organizacyjnego. Szczegółowy wykaz konferencji i pełnionych funkcji został ujęty w części wniosku pt. „Wykaz osiągnięć naukowych albo artystycznych, stanowiących znaczny wkład w rozwój określonej dyscypliny".

Efektem wymiernym mojej pracy podczas organizowanych konferencji jest:

1) Współredakcja 7 monografii naukowych:

1. Kiełtyka L., Jędrzejczyk W., **Kobis P.** (red.) (2015), *Wyzwania współczesnego zarządzania. Tendencje w zachowaniach organizacyjnych*, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, Toruń, ISBN 978-83-7285-791-0.
2. Jędrzejczyk W., **Kobis P.**, Kucęba R. (red.) (2016), *Behawioralizm w teorii i praktyce zarządzania. Społeczny wymiar zarządzania zasobami ludzkimi*, Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa, ISBN 978-83-65179-59-3.
3. Kiełtyka L., Jędrzejczyk W., **Kobis P.** (red.) (2016), *Wyzwania współczesnego zarządzania. Kreowanie kapitału intelektualnego organizacji*, Towarzystwo Naukowe Organizacji i Kierownictwa, Warszawa, ISBN 978-83-7285-815-3.
4. Kulej-Dudek E., **Kobis P.** (red.) (2016), *Rozwój i doskonalenie funkcjonowania organizacji. Przedsiębiorstwa w erze nowych technologii, działań innowacyjnych i społecznie odpowiedzialnych*, Wydawnictwo PCz, Częstochowa, ISBN 978-83-7193-645-6.
5. Kiełtyka L., **Kobis P.** (red.) (2017), *Wybrane zagadnienia zarządzania współczesnymi przedsiębiorstwami*, Wydawnictwo PCz, Częstochowa, ISBN 978-83-7193-660-9.
6. Jędrzejczyk W., **Kobis P.**, Kucęba R. (red.) (2017), *Behawioralizm w teorii i praktyce zarządzania. Kreowanie kapitału ludzkiego, strukturalnego i społecznego organizacji*,

Wydawnictwo Wydziału Zarządzania Politechniki Częstochowskiej, Częstochowa, ISBN 978-83-65951-10-6.

7. Kiełtyka L., Jędrzejczyk W., **Kobis P.** (red.) (2018), *Wyzwania współczesnego zarządzania. Nowe technologie, innowacyjność, kompetencje*, Towarzystwo Naukowe Organizacji i Kierownictwa. Dom Organizatora, Toruń, ISBN 978-83-7285-855-9.

2) Uczestnictwo w sesji panelowej „Paradoksy funkcjonowania współczesnych organizacji" w ramach III Ogólnopolskiej Konferencji naukowej „Rozwój i doskonalenie funkcjonowania organizacji" która odbyła się w Częstochowie w dniu 22 czerwca 2016 roku.
3) Przewodniczenie sesji naukowej „Aspekty zarządzania i doskonalenia działalności przedsiębiorstw" w ramach XII Konferencji Naukowej „Multimedia w Biznesie i Zarządzaniu", która odbyła się w Koszęcinie w dniach 22-24 marca 2017 roku.
4) Przewodniczenie sesjom biznesowym:
    a. W ramach XII Konferencji Naukowej „Multimedia w Biznesie i Zarządzaniu", która odbyła się w Koszęcinie w dniach 22-24 marca 2017 roku.
    Firmy i tematy sesji: Kaspersky Lab Polska: Kaspersky DDoS Protection (KDP); BMF Centrum Specjalistycznego Sprzętu Mobilnego: "Technologie mobilne o zwiększonej wytrzymałości" – zastosowanie; GH Cranes: Inteligentne suwnice - innowacja oparta na technologii informacyjnej.
    b. W ramach XIV Konferencji Naukowej „Multimedia w Biznesie i Administracji. Technologie ICT we współczesnym zarządzaniu", która odbyła się w Częstochowie 25-26 marca 2021 roku.
    Firmy i tematy sesji: Sophos: Holistyczne podejście do bezpieczeństwa sieciowego. Jedna platforma, jeden producent, kilka rozwiązań; Synology: Data security, czyli jak zabezpieczyć dane, by były rzeczywiście bezpieczne.

Załączniki (umieszczone w części „Pozostałe dokumenty" w punkcie „Certyfikaty potwierdzające pełnienie określonych funkcji podczas konferencji naukowych"):

- ***Certyfikat zaświadczający o pełnieniu funkcji Sekretarza Naukowego podczas III Ogólnopolskiej Konferencji Naukowej „Rozwój i doskonalenie funkcjonowania organizacji" (autorzy: Przewodnicząca Konferencji: dr inż. Klaudia Smoląg, Przewodniczący Komitetu Naukowego: Prof. dr hab. inż. Leszek Kiełtyka);***

- *Certyfikat zaświadczający o uczestniczeniu w Sesji Panelowej pt. „Paradoksy funkcjonowania współczesnych organizacji" podczas III Ogólnopolskiej Konferencji Naukowej „Rozwój i doskonalenie funkcjonowania organizacji" (autorzy: Przewodnicząca Konferencji: dr inż. Klaudia Smoląg, Przewodnicząca Sesji Panelowej: Dr hab. Iwona Chomiak-Orsa, prof. UE, Przewodniczący Komitetu Naukowego: Prof. dr hab. inż. Leszek Kiełtyka);*

- *Certyfikat zaświadczający o pełnieniu funkcji Sekretarza Naukowego podczas XII Konferencji Naukowej „Multimedia w Biznesie i Zarządzaniu" (autorzy: Przewodniczący Komitetu Naukowego: Prof. dr hab. inż. Krzysztof Zieliński, Przewodniczący Konferencji: Prof. dr hab. inż. Leszek Kiełtyka);*

- *Certyfikat zaświadczający o przewodniczeniu Sesji Biznesowej podczas XII Konferencji Naukowej „Multimedia w Biznesie i Zarządzaniu" (autorzy: Przewodniczący Komitetu Naukowego: Prof. dr hab. inż. Krzysztof Zieliński, Przewodniczący Konferencji: Prof. dr hab. inż. Leszek Kiełtyka);*

- *Certyfikat zaświadczający o przewodniczeniu Sesji Naukowej pt. „Aspekty zarządzania i doskonalenia działalności przedsiębiorstw" podczas XII Konferencji Naukowej „Multimedia w Biznesie i Zarządzaniu" (autorzy: Przewodniczący Komitetu Naukowego: Prof. dr hab. inż. Krzysztof Zieliński, Przewodniczący Konferencji: Prof. dr hab. inż. Leszek Kiełtyka);*

- *Certyfikat zaświadczający o przewodniczeniu Sesji Biznesowej podczas XIV Konferencji Naukowej „Multimedia w Biznesie i Administracji" (autorzy: Przewodnicząca Rady Programowej: dr inż. Edyta Kulej-Dudek, Przewodniczący Konferencji: Prof. dr hab. inż. Leszek Kiełtyka);*

Popularyzacja przeze mnie nauki miała również swój wyraz w organizowaniu ogólnopolskiego projektu edukacyjno-badawczego „VIII Olimpiada Przedsiębiorczości i Zarządzania" dla uczniów szkół średnich z całej Polski na Wydziale Zarządzania Politechniki Częstochowskiej w roku 2020 w roli członka Komitetu Głównego olimpiady.

Załączniki (umieszczone w części „Pozostałe dokumenty" w punkcie „Zaświadczenia, certyfikaty oraz inne dokumenty potwierdzające aktywności"):

- *Zaświadczenie nr 01/KG/VIII/2020 o członkostwie w Komitecie Głównym ogólnopolskiego projektu edukacyjno-badawczego „VIII Olimpiada Przedsiębiorczości i Zarządzania" (autor: dr hab. Andrzej Brzeziński, prof. PCz)*

Od 2015 roku biorę udział w pracach Zespołu Redakcyjnego czasopisma „Przegląd Organizacji", w którym od początku pełnię redaktora opracowania elektronicznego (pierwotnie nazwa funkcji: redaktor wydania elektronicznego) miesięcznika. W ramach pracy

w „Przeglądzie Organizacji" brałem czynny udział w projektach mających na celu popularyzację czasopisma w środowisku naukowym oraz podnoszenie rangi czasopisma poprzez umieszczenie w uznanych bazach indeksujących, liście czasopism punktowanych według wykazu ministerialnego oraz podnoszenie jego punktacji. Wykaz projektów:

Typ projektu	**Nr rej.**	**Rok złożenia wniosku**	**Pełniona funkcja**
Działalność upowszechniająca naukę - podmiotowy - Działalność wydawnicza	624/P-DUN/2018	2017	Redaktor pomocniczy, wykonawca
Wsparcie dla Czasopism Naukowych	424945	2018	Redaktor pomocniczy, wykonawca
Wniosek o finansowanie w ramach programu Rozwój Czasopism Naukowych	Wniosek złożony	2021	Redaktor pomocniczy

Będąc członkiem zespołu redakcyjnego czasopisma brałem również udział w przygotowywaniu zadań związanych z:

- opracowaniem numerów archiwalnych czasopisma od 1990 roku do postaci przyjętej w świecie nauki za standard;
- przygotowaniem i udostępnieniem na stronie internetowej oprogramowania pozwalającego na wyszukiwanie interesujących treści w oparciu o metadane;
- zarejestrowaniem i oznaczeniem udostępnianych artykułów numerami DOI;
- opracowaniem koncepcji budowy nowej platformy wymiany i przechowywania informacji dla „Przeglądu Organizacji" w obszarach dwustronnych relacji autor – redakcja, recenzent -redakcja.

W mojej bieżącej pracy na rzecz „Przeglądu Organizacji", pełniąc funkcję redaktora opracowania elektronicznego, podejmuję ciągłe działania na rzecz udoskonalania formy cyfrowej czasopisma, strony internetowej czasopisma, redakcji kolejnych numerów, umieszczania czasopisma w przynależnych bazach.

Załączniki (umieszczone w części „Pozostałe dokumenty" w punkcie „Zaświadczenia, certyfikaty oraz inne dokumenty potwierdzające aktywności"):

- ***Działania dr inż. Pawła Kobisa na rzecz „Przeglądu Organizacji" (autor: Prof. dr hab. Stanisław Brzeziński, Redaktor Naczelny „Przeglądu Organizacji")***

Jestem obecnie również promotorem pomocniczym otwartego w 2019 roku przewodu doktorskiego pt. „*Kompetencje pracownicze w zarządzaniu bezpieczeństwem informacji w małych przedsiębiorstwach*". Przewód doktorski otwarty jest na Wydziale Zarządzania Politechniki Częstochowskiej.

Byłem autorem recenzji artykułów naukowych i brałem czynny udział w Komitetach Konferencji Międzynarodowych, w tym:

1) 3rd International Conference on Engeneering Optimization, EngOpt 2012, Rio dc Janciro, Brazylia, 1-5 lipiec 2012 r. (International Scientific Committee);
2) 35th IBIMA International Conference, Seville, Hiszpania, 1-2 kwiecień 2020 r. (Program Committee);
3) 36th IBIMA International Conference, Granada, Hiszpania, 4-5 listopad 2020 r. (Program Committee);
4) 37th IBIMA International Conference, Cordoba, Hiszpania, 30-31 maj 2021 r. (Program Committee, Excellent Constructive Review Certyficate);
5) 38th IBIMA International Conference, Seville, Hiszpania, listopad 2021 r. (Program Committee).

Pełny spis udziału i pełnionych funkcji w Komitetach Konferencji Naukowych znajduje się w części wniosku pt. „Wykaz osiągnięć naukowych albo artystycznych, stanowiących znaczny wkład w rozwój określonej dyscypliny".

W zakresie pracy organizacyjnej na Wydziale Zarządzania Politechniki Częstochowskiej brałem czynny udział w:

- Wydziałowej Komisji Rekrutacyjnej (dwukrotnie);
- Komisji ds. przeprowadzania ankiety oceniającej nauczycieli akademickich wśród studentów (trzykrotnie);
- Komisji ds. Internetowej Komunikacji Wydziału Zarządzania z otoczeniem.

W zakresie pracy dydaktycznej prowadziłem i prowadzę zajęcia na studiach stacjonarnych i niestacjonarnych w firmie wykładów, ćwiczeń, laboratoriów i projektu. Zajęcia realizowałem i realizuję na kierunkach:

- Zarządzanie;
- Zarządzanie i Inżynieria Produkcji;
- Zarządzanie Jakością i Produkcją;
- Quality and Production Management;
- Bezpieczeństwo i Higiena Pracy;
- Finanse i Rachunkowość;
- Finanse i Rachunkowość w Biznesie;
- Logistyka;
- Logistyka Inżynierska;
- Zarządzanie w Turystyce i Sporcie.

Od 2011 roku posiadam uprawnienia w zakresie prowadzenia zajęć w trybie e-learningowym (od 2014 na poziomie zaawansowanym), udokumentowane certyfikatem ukończenia kursu e-learning, wystawionego przez Ośrodek Kształcenia na Odległość Politechniki Częstochowskiej. Tym samym w każdym roku akademickim realizuję przedmioty również w trybie e-learningowym, w zakresie dopuszczonym obowiązującymi przepisami, stosując wszystkie dostępne narzędzia nauki na odległość oferowane przez uczelnianą platformę Moodle.

Wykaz wybranych prowadzonych przedmiotów w formie stacjonarnej oraz poprzez system e-learningowy:

- Komunikacja w zarządzaniu (*wykład, realizacja materiałów dydaktycznych również na platformę e-learningową Politechniki Częstochowskiej*);
- Finanse i rachunkowość w chmurze obliczeniowej (*wykład, laboratorium, realizacja materiałów dydaktycznych również na platformę e-learningową Politechniki Częstochowskiej*);
- Technologie informacyjno-komunikacyjne w logistyce (*laboratorium*);
- Systemy finansowo-księgowe w modelu cloud computing (*wykład, laboratorium*)
- Systemy informatyczne w turystyce i rekreacji (*wykład, laboratorium, realizacja materiałów dydaktycznych również na platformę e-learningową Politechniki Częstochowskiej*);
- Informatyczne systemy finansowo-księgowe (*wykład, ćwiczenia, realizacja materiałów dydaktycznych również na platformę e-learningową Politechniki Częstochowskiej*);

- Metody i obszary modelowania procesów produkcyjnych (*wykład, ćwiczenia, realizacja materiałów dydaktycznych również na platformę e-learningową Politechniki Częstochowskiej*);
- Arkusze kalkulacyjne w analizie finansowej (*ćwiczenia*);
- Informatyka (*wykład, laboratorium, realizacja materiałów dydaktycznych również na platformę e-learningową Politechniki Częstochowskiej*);
- Information Technology (*wykład, laboratorium, realizacja materiałów dydaktycznych również na platformę e-learningową Politechniki Częstochowskiej*)
- Projekt inżynierski (*projekt, realizacja materiałów dydaktycznych również na platformę e-learningową Politechniki Częstochowskiej*);
- Nowoczesne technologie w turystyce, hotelarstwie i gastronomii (*wykład, ćwiczenia, realizacja materiałów dydaktycznych również na platformę e-learningową Politechniki Częstochowskiej*);
- Technologia Informacyjna (*ćwiczenia*);
- Makroekonomia (*wykład, ćwiczenia, realizacja materiałów dydaktycznych również na platformę e-learningową Politechniki Częstochowskiej*).

Załączniki (umieszczone w części „Pozostałe dokumenty" w punkcie „Zaświadczenia, certyfikaty oraz inne dokumenty potwierdzające aktywności"):

- ***Zaświadczenie o ukończeniu szkolenia dla pracowników Politechniki częstochowskiej „e-nauczanie w praktyce szkoły wyższej" (autorzy: Pełnomocnik Rektora ds. e-learningu: dr hab. Krzysztof Cpałka, prof.PCz, , prowadzący szkolenie: Anna Stanisławska-Mischke, Dorota Morawska-Walasek, Przemysław Stencel.***

- ***Certyfikat ukończenia szkolenia dla pracowników Politechniki Częstochowskiej „Doskonalenie umiejętności nauczycieli akademickich w prowadzeniu e-zajęć" (autor: Przewodnicząca Zespołu ds. e-learningu w Politechnice Częstochowskiej, Dr hab. Dorota Jelonek, prof. PCz)***

Jestem promotorem oraz recenzentem łącznie kilkudziesięciu prac inżynierskich, licencjackich oraz magisterskich, których tematyka związana była z zagadnieniami prowadzonych przeze mnie przedmiotów dydaktycznych oraz zainteresowaniami naukowymi związanymi z zarządzaniem informacją i bezpieczeństwem informacji. Promotorem i recenzentem prac inżynierskich i magisterskich byłem również poza uczelnią macierzystą

w ramach dodatkowego miejsca pracy w Wyższej Szkole Ekonomii i Prawa im. Prof. Edwarda Lipińskiego w Kielcach.

W trakcie mojej pracy naukowo-dydaktycznej na Wydziale Zarządzania Politechniki Częstochowskiej otrzymałem następujące odznaczenia:

- Medal 20-lecia Wydziału Zarządzania Politechniki Częstochowskiej, rok 2017.
- Medal Brązowy za Długoletnią Służbę nadany przez Prezydenta Rzeczypospolitej Polskiej, postanowieniem z dnia 5 czerwca 2018 roku, nr legitymacji: 158-2018-51.
- Medal Komisji Edukacji Narodowej, nadany przez Ministra Edukacji i Nauki za szczególne zasługi dla oświaty i wychowania, postanowieniem z dnia 11 sierpnia 2021 roku, nr legitymacji 175612.

Za zasługi w pracy naukowej i organizacyjnej otrzymałem łącznie 18 Nagród Rektora Politechniki Częstochowskiej, w tym nagrody zespołowe I, II i III stopnia.

Lp.	Rodzaj nagrody	Rok
1	Nagroda Rektora Politechniki Częstochowskiej zespołowa I stopnia za cykl publikacji z zakresu multimediów w zarządzaniu	2003
2	Nagroda Rektora Politechniki Częstochowskiej zespołowa I stopnia za cykl publikacji z zakresu informatycznych systemów zarządzania	2004
3	Nagroda Rektora Politechniki Częstochowskiej zespołowa II stopnia za cykl publikacji w dziedzinie technik informatycznych wykorzystywanych w zarządzaniu	2005
4	Nagroda Rektora Politechniki Częstochowskiej zespołowa I stopnia za zorganizowanie międzynarodowej konferencji naukowej nt. „Multimedia w Biznesie i Edukacji"	2006
5	Nagroda Rektora Politechniki Częstochowskiej zespołowa III stopnia za organizację VI Międzynarodowej Konferencji „Multimedia w Biznesie"	2007
6	Nagroda Rektora Politechniki Częstochowskiej zespołowa II stopnia za całokształt osiągnięć naukowych i dydaktycznych	2008
7	Nagroda Rektora Politechniki Częstochowskiej zespołowa stopnia III za cykl publikacji z zakresu informatycznych systemów zarządzania	2009
8	Nagroda Rektora Politechniki Częstochowskiej zespołowa stopnia III za zorganizowanie VII Międzynarodowej Konferencji „Multimedia w biznesie"	2009
9	Nagroda Rektora Politechniki Częstochowskiej zespołowa III stopnia za zorganizowanie VIII Międzynarodowej Konferencji pt. „Multimedia w Biznesie i Zarządzaniu".	2010
10	Nagroda Rektora Politechniki Częstochowskiej zespołowa II stopnia za działalność organizacyjną	2012
11	Nagroda Rektora Politechniki Częstochowskiej zespołowa II stopnia za działalność organizacyjną	2013
12	Nagroda Rektora Politechniki Częstochowskiej zespołowa II stopnia za zorganizowanie X Jubileuszowej Międzynarodowej Konferencji pt. „Multimedia w Biznesie i Zarządzaniu".	2014

13	Nagroda Rektora Politechniki Częstochowskiej zespołowa I stopnia za cykl publikacji	2014
14	Nagroda Rektora Politechniki Częstochowskiej zespołowa III stopnia za organizację XI Konferencji „Multimedia w Biznesie i Zarządzaniu", Częstochowa 26-27 marca 2015 r.	2016
15	Nagroda Rektora Politechniki Częstochowskiej zespołowa III stopnia za cykl publikacji	2016
16	Nagroda Rektora Politechniki Częstochowskiej zespołowa II stopnia za organizację Interdyscyplinarnej Konferencji Środowisk Naukowych Biznesowych i Samorządowych nt. „Energetyka prosumencka w wymiarach zrównoważonego rozwoju" oraz seminarium nt. „Zarządzanie energetyką prosumencką".	2016
17	Nagroda Rektora Politechniki Częstochowskiej zespołowa II stopnia za osiągnięcia w zakresie wdrażania i propagowania nowych metod nauczania w PCz	2016
18	Nagroda Rektora Politechniki Częstochowskiej zespołowa III stopnia za organizację konferencji: „Behawioralizm w teorii i praktyce zarządzania współczesnymi organizacjami", 4-5.11.2015 r., Częstochowa.	2017

Załączniki (umieszczone w części „Pozostałe dokumenty" w punkcie „Nagrody Rektora Politechniki Częstochowskiej"):

- ***Dyplomy dokumentujące otrzymane Nagrody Rektora Politechniki Częstochowskiej***