# AUTOREFERAT

1. Imię i nazwisko: **Maciej Kiedrowicz**

2. Posiadane stopnie naukowe – z podaniem nazwy, miejsca i roku ich uzyskania oraz tytułu rozprawy doktorskiej.

   **dr inż. – nauki techniczne, informatyka, systemy baz danych,**

   **Wojskowa Akademia Techniczna, Warszawa, 08 lipca 1999r.,**

   Temat: **Metoda wspomagania projektowania rozproszonych baz danych w systemach informatycznych eksploatowanych w warunkach celowego niszczenia elementów sieci komputerowej.**

   Promotor: **dr hab. inż. Tadeusz Nowicki**
   Recenzenci: **prof. dr hab. inż. Juliusz L. Kulikowski**
   **dr hab. inż. Bolesław Szafrański**

   **mgr inż. – cybernetyk, systemy informatyczne, 03 lipca 1987r.**

3. Informacje o dotychczasowym zatrudnieniu w jednostkach naukowych.

   **Wojskowa Akademia Techniczna, Wydział Cybernetyki – adiunkt (2000-obecnie)**

   (funkcje: Kierownik Zakładu Inżynierii Oprogramowania, Z-ca Dyrektora Instytutu Systemów Informatycznych, obecnie: **Prodziekan Wydziału Cybernetyki ds. rozwoju i współpracy**)

   **Uczelnia Warszawska im. Marii Skłodowskiej-Curie – adiunkt (2012-2017)**

   **Wyższa Szkoła Handlu i Prawa im. R. Łazarskiego – adiunkt (2004)**

   **Wojskowa Akademia Techniczna, Wydział Cybernetyki – asystent (1994-2000)**

   **Wojskowy Instytut Informatyki, Filia Nr 2 – programista (1991), st. projektant (1991-1993), st. problemista (1993-1994)**

4. Wskazanie osiągnięcia[1] wynikającego z art. 16 ust. 2 ustawy z dnia 14 marca 2003r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. 2017 r. poz. 1789):
   a) Tytuł osiągnięcia naukowego:

   **Technologie informatyczne w bezpiecznym przetwarzaniu zasobów informacyjnych administracji publicznej**

[1] W przypadku, gdy osiągnięciem tym jest praca/prace wspólne, należy przedstawić oświadczenia wszystkich jej współautorów, określające indywidualny wkład każdego z nich w jej powstanie. W przypadku, gdy praca zbiorowa ma więcej niż pięciu współautorów, habilitant załącza oświadczenie określające jego indywidualny wkład w powstanie tej pracy oraz oświadczenia co najmniej czterech pozostałych współautorów.

b) Publikacje (treści wszystkich publikacji znajdują się w załącznikach):

1. [A_6] **M. Kiedrowicz**, J. Stanik, 2018, *Multicriteria optimization used for the information security - ideal and anty-ideal*, w: Conference Proceedings of Geographic Information Systems Conference And Exhibition - "GIS ODYSSEY 2018", 2018, Perugia, Italy, Sep 10-14, 2018, Publisher: Croatian Information Technology Society - GIS Forum, Croatia, pp. 237-251, ISSN: 2623-5714 (Online), 2459-7619 (Print).
2. [A_9] **M. Kiedrowicz**, 2018, *Application possibilities of Advanced Analysis of Public Data Sources in the Fight Against Child Maltreatment*, w: Conference Proceedings of Geographic Information Systems Conference And Exhibition - "GIS ODYSSEY 2018", 2018, Perugia, Italy, Sep 10-14, 2018, Publisher: Croatian Information Technology Society - GIS Forum, Croatia, pp. 204-211, ISSN: 2623-5714 (Online), 2459-7619 (Print).
3. [A_14] **M. Kiedrowicz**, A. Ameljańczyk, 2018, *Multicriteria Methods for Identifying Patterns in the Analysis of the Flow of "Dangerous Financial Documents"*, w: 22nd International Conference on Circuits, Systems, Communications and Computers (CSCC 2018), MATEC Web of Conferences, vol. 210, ISSN: 2261-236X, DOI: 10.1051/matecconf/ 201821004010.
4. [A_29] **M. Kiedrowicz**, 2018, *Metodyka zarządzania ryzykiem w bezpieczeństwie zasobów informacyjnych*, w: Roczniki Kolegium Analiz Ekonomicznych, SGH, Warszawa, nr 49, str. 287-305, ISSN: 1232-4671.
5. [A_40] **M. Kiedrowicz**, 2017, *Multi-faceted methodology of the risk analysis and management referring to the IT system supporting the processing of documents at different levels of sensitivity*, w: 21st International Conference on Circuits, Systems, Communications and Computers (CSCC 2017), MATEC Web of Conferences, vol. 125, ISSN: 2261-236X, DOI: 10.1051/matecconf/ 201712502010
6. [A_42] **M. Kiedrowicz**, J. Stanik, 2017, *Models and method for the risk assessment of an intellectual resource*, w: WSEAS Transactions on Communications, ISSN: 2224-2864, Volume 16, Art. #18, pp. 149-158.
7. [A_44] **M. Kiedrowicz**, 2017, *Generalized data model in distributed registers*, w: Geographic Information Systems Conference and Exhibition "GIS ODYSSEY 2017", 4th to 8th of September 2017, Trento – Vattaro, Italy, Conference proceedings, pp. 171-183.
8. [A_45] **M. Kiedrowicz**, 2017, *Interoperability and globalization of information models*, w: Geographic Information Systems Conference and Exhibition "GIS ODYSSEY 2017", 4th to 8th of September 2017, Trento – Vattaro, Italy, Conference proceedings, pp. 161-170.
9. [A_66] **M. Kiedrowicz**, 2016, *Use of biometric data in identification documents*, w: Zeszyty Naukowe, Maria Skłodowska-Curie Warsaw University, Warsaw, vol. 4(54), pp. 89-102, ISSN: 1897-2500.
10. [A_67] **M. Kiedrowicz**, 2016, *Location with the use of the RFID and GPS technologies - opportunities and threats*, w: Proceedings of Geographic Information Systems Conference And Exhibition - GIS ODYSSEY 2016, 2016, Perugia, Italy, sep 05-09, Publisher: Croatian Information SOC-GIS Forum, Croatia, pp. 122-128, ISBN: 978-953-6129-55-3.
11. [A_68] **M. Kiedrowicz**, 2016, *Objects identification in the information models used by information systems*, w: Proceedings of Geographic Information Systems Conference And Exhibition - GIS ODYSSEY 2016, Perugia, Italy, sep 05-09, Publisher: Croatian Information SOC-GIS Forum, Croatia, pp. 129-136, ISBN: 978-953-6129-55-3.

12. [A_88] **M. Kiedrowicz**, 2015, *Rejestry i zasoby informacyjne wykorzystywane przez organy odpowiedzialne za wykrywanie i przeciwdziałanie przestępczości,* w: Jawność i jej ograniczenia, G. Szpor (red.), Monografie Prawnicze, tom IX, Zadania i kompetencje, B. Szmulik (red.), C.H. Beck, Warszawa, str. 170-264, ISBN: 978-83-255-7664-6.
13. [A_96] **M. Kiedrowicz**, 2014, *The importance of an integration platform within the organisation,* w: Zeszyty Naukowe, Maria Skłodowska-Curie Warsaw University, Warsaw, vol. 4(46), pp.83-94, ISSN: 1897-2500.
14. [A_98] **M. Kiedrowicz**, 2014, *Uogólniony model danych w rozproszonych rejestrach ewidencyjnych,* w: Roczniki Kolegium Analiz Ekonomicznych, SGH, Warszawa, nr 33, str. 209-234, ISSN: 1232-4671.
15. [A_105] **M. Kiedrowicz**, 2011, *Wspomaganie zarządzania - zasoby publiczne w wybranych krajach unijnych,* w: Nowoczesne Systemy Zarządzania, vol. 6, WAT, Warszawa, ISSN: 1896-9380.
16. [A_106] **M. Kiedrowicz**, 2010, *Wspomaganie zarządzania w administracji - podejście procesowe a realizacja usług publicznych,* w: Nowoczesne Systemy Zarządzania, vol. 5, WAT, Warszawa, str. 321-340, ISSN: 1896-9380.
17. [A_114] **M. Kiedrowicz**, 2002, *Mathematical and Simulation Model of Fault Tolerance Distributed Database Systems,* w: ICDM '02 The 2002 IEEE International Conference on Data Mining, International Workshop on Active Mining (AM-2002), pp. 75-79, December 9, Maebashi City, Japan.
18. [P_1] **M. Kiedrowicz**, 2018, *Raport końcowy – sprawozdanie merytoryczne z wykonanych badań naukowych i prac rozwojowych w ramach projektu „Zaawansowane technologie informatyczne wspierające procesy analizy danych (gł. finansowych) w obszarze przestępczości finansowej*" (Projekt IAFEC).
19. [P_2] **M. Kiedrowicz**, 2017, *Raport końcowy – sprawozdanie merytoryczne z wykonanych badań naukowych i prac rozwojowych w ramach projektu „Elektroniczny system zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości*" (Projekt RFID).

c) Omówienie celu naukowego ww. prac i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania – strony 4 – 31.

5. Omówienie pozostałych osiągnięć naukowo - badawczych – strony 32 – 33.

## Wprowadzenie

Osiągnięcie naukowe pt. „**Technologie informatyczne w bezpiecznym przetwarzaniu zasobów informacyjnych administracji publicznej**” obejmuje zrealizowane osiągnięcia technologiczne opisane w [P_1] i [P_2]:

1. Projekt IAFEC[2] (przestępstwa gospodarcze i finansowe, pranie brudnych pieniędzy).
2. Projekt RFID[3] (przetwarzanie dokumentów wrażliwych, bezpieczne udostępnianie).

oraz cykl publikacji (wymienionych w punkcie 4.b) podzielonych tematycznie na trzy obszary:

I. Uogólniony i dziedzinowe modele danych w odniesieniu do repozytoriów i rejestrów administracji publicznej; zasoby informacyjne administracji publicznej.
II. Wybrane aspekty bezpieczeństwa w przetwarzaniu zasobów informacyjnych administracji publicznej; podejście zorientowane procesowo i oparte na analizie ryzyka.
III. Wykorzystanie zaproponowanych modeli do zwalczenia przestępstw gospodarczych i finansowych; uwarunkowania legislacyjne.

Dla bardziej przejrzystego układu prezentowanych publikacji, obszary badań i wykorzystane technologie przedstawiono w tabeli 1.

**UWAGA**: Publikacje wchodzące w skład osiągnięcia naukowego oznaczone są **[A_xxx]**, publikacje które uzupełniają osiągnięcie naukowe oznaczone są **[B_xxx]**, pozostałe publikacje mają oznaczenie **[C_xxx]**. Publikacje dotyczące projektów oznaczono **[P_xxx]**. Numeracja wynika z chronologii pojawiania się publikacji (im wyższy numer tym starsza publikacja).

| | **I** | **II** | **III** |
|---|---|---|---|
| badania / technologia | Zasoby danych<br>Repozytoria, rejestry<br>Modele | Bezpieczeństwo<br>Procesy<br>Ryzyko | Zwalczanie przestępstw<br>Legislacja |
| 1. Projekt IAFEC | A: 44, 45, 98<br>B: 61, 89, 108, 109 | A: 6, 29, 40, 106<br>B: 1, 5, 7, 11, 12, 15, 16, 41, 94, 111 | A: 9, 14, 66, 88<br>B: 3, 8, 10, 17, 38, 39, 60, 110 |
| 2. Projekt RFID | B: 108, 109 | A: 106<br>B: 19, 41, 81, 111 | A: 9, 67, 68<br>B: 10 |
| Inne | A: 105, 114<br>B: 112, 113, 115 | A: 42, 96<br>B: 28, 35, 93, 107 | |

Tabela 1. Przypisanie publikacji wchodzących w skład dzieła naukowego (A) oraz publikacji uzupełniających (B) do obszarów badań w kontekście technologii.

Przedstawiony do oceny materiał obejmuje istotne, z punktu widzenia procesu dostosowywania administracji do zmieniającego się otoczenia, aspekty związane z przetwarzaniem zasobów danych. Równie ważnym zagadnieniem, które zostało opisane w publikacjach, jest konieczność uwzględnienia

[2] Projekt pt. „Zaawansowane technologie informatyczne wspierające procesy analizy danych (gł. finansowych) w obszarze przestępczości finansowej" – dalej zwany „Projekt IAFEC” lub „IAFEC”.
[3] Projekt pt. „Elektroniczny system zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości” – dalej zwany „Projekt RFID” lub „Projekt kancelarii RFID”.

zależności pomiędzy różnymi obszarami funkcjonowania administracji, w szczególności związane z otoczeniem prawnym. Otoczenie systemu zarządzania zasobami danych jest bardzo złożone i zmienne. Z jednej strony mamy do czynienia ze stale rozwijającą się technologią teleinformatyczną oraz zmiennym otoczeniem prawnym (krajowym i unijnym), z drugiej zaś – z względnie stałymi przyzwyczajeniami użytkowników systemów informatycznych, którzy starają się nadążać za zmieniającym się otoczeniem. Istotnym problemem, który często jest pomijany, jest konieczność rozwoju istniejących już lub projektowanie nowych systemów teleinformatycznych, mających wspomagać wszystkich interesariuszy zmieniającego się otoczenia, w kontekście nowych obszarów, które podlegają „informatyzacji". Czas realizacji poszczególnych etapów cyklu życia oprogramowania powoduje niejednokrotnie, że już w trakcie ich realizacji stają się one nieaktualne. O ile problemy wynikające z samego procesu wytwarzania oprogramowania zostały rozwiązane (wykorzystywanie standardów, budowa modułowa, zastosowanie zwinnych metodyk projektowania, etc.), o tyle kwestie dotyczące implementacji ciągłych zmian w otoczeniu, nie zostały jeszcze rozwiązane. Dotyczy to m.in. **konieczności dostosowywania systemów informatycznych do zmieniających się uwarunkowań prawnych**, w szczególności w związku ze zmieniającymi się definicjami i zakresami zasobów danych, które są w tych systemach wykorzystywane. Bardzo istotnym elementem tego dostosowywania jest konieczność **zachowania bezpieczeństwa** wynikającego z dostępu do coraz większego wolumenu danych. Bezpieczeństwa rozumianego z jednej strony, jako ochrona przed nieuprawnionym dostępem do danych wrażliwych, z drugiej zaś – jako pełna rozliczalność z faktu udostępnienia określonych danych.

Pojęcie zasobów informacyjnych (zasobów danych) administracji publicznej jest szerokie i obejmuje wszystkie zasoby danych, którymi dysponuje administracja publiczna (rządowa i samorządowa). Zasoby te są przetwarzane w sposób tradycyjny oraz z wykorzystaniem technologii teleinformatycznych. Sposób ich zbierania, przetwarzania oraz udostępniania jest regulowany stosownymi przepisami prawa. Ciągły rozwój technologii teleinformatycznych wymusza również konieczność bieżącego dostosowywania całego aparatu administracyjnego, który odpowiada za zarządzanie tymi zasobami. Ogromnych problemów przysparza również konieczność uwzględnienia przyzwyczajeń potencjalnych użytkowników tych systemów, którzy w wielu przypadkach chcieliby zachować tradycyjne (niejednokrotnie „papierowe") sposoby dostępu do nich.

Autorska **propozycja stworzenia uogólnionego modelu danych**, opartego na możliwie najszerszym (obejmującym największy wolumen danych i zawierającym najszerszy ich zakres) zasobie danych, pozwala na właściwe wykorzystanie technologii informatycznych do jego zarządzania. Zaproponowane podejście obejmuje również charakterystykę odpowiednich działań, które zostały wykonane przed opracowaniem takiego modelu oraz charakterystykę sposobu wykorzystania istniejących rozwiązań teleinformatycznych. Istotnym elementem jest także wskazanie możliwości późniejszego wykorzystania zaproponowanego modelu. W szczególności dotyczącego zastosowań w zaawansowanej analizie danych w wybranych obszarach życia praktycznego. Jedną z głównych zalet takiego podejścia jest większe **„uniezależnienie się" od zmian w otoczeniu**, które zachodzą w coraz szybszym stopniu. Innymi słowy, takie podejście daje możliwość nadążania z tworzeniem (modyfikacją) systemów informatycznych do zmieniających się wymagań rzeczywistych i potencjalnych interesariuszy tych systemów.

Wykazano, że **zaproponowane sposoby projektowania modeli danych umożliwiają ich praktyczne wykorzystanie** w projektowaniu systemów informatycznych i umożliwiają ich pełniejsze wykorzystanie – zgodnie z wymaganiami użytkowników oraz przy spełnieniu rygorystycznych uwarunkowań wynikających z zachowania przepisów prawa, **ze szczególnym uwzględnieniem bezpieczeństwa danych**, a co tym idzie, również **bezpieczeństwa informacji**.

Analiza dostępnej literatury (publikowanej tradycyjnie – w formie papierowej, jak i w postaci elektronicznej) pokazuje, że brak jest pozycji, które by tak kompleksowo opisywały zagadnienia będące

przedmiotem zainteresowania habilitanta. Bibliografie przedstawione w poszczególnych pozycjach osiągnięcia naukowego obejmują najczęściej publikacje dotyczące pojedynczych pojęć lub zagadnień, które zostały opisane w literaturze przedmiotu. Należy również zauważyć, że tematyka oraz liczba wystąpień na konferencjach międzynarodowych potwierdza duże zainteresowanie opisywanymi zagadnieniami.

Ponadto brak jest publikacji związanych z wynikami badań (zarówno w języku polskim, jak i angielskim), które byłyby prowadzonych we wskazanych obszarach. Może to wynikać również z tego powodu, że opisywane badania obejmują na ogół zasoby różnorodnych repozytoriów i ewidencji. Wynika to również z faktu, iż w wielu przypadkach, przywoływane zasoby dotyczą danych wrażliwych (obejmujących np. dane osobowe) lub danych stanowiących różnego rodzaju tajemnice (np. tajemnicę handlową, tajemnicę finansową lub bankową). Prezentowane spojrzenie, obejmujące kompleksowe podejście do wielu obszarów badań, pozwala przyjąć, że wyniki tych badań stanowią istotny rozwój dyscypliny i mogą być przyczynkiem do dalszego zastosowania technologii teleinformatycznych w obszarach, w których do tej pory nie były stosowane.

Bardzo istotnym uzupełnieniem publikacji z zakresu tematyki będącej przedmiotem autoreferatu, są wyniki prac badawczo-rozwojowych prowadzonych przez habilitanta. Dotyczy to przede wszystkim dwóch projektów, którymi kierował, a które były wynikiem rozstrzygnięcia konkursów ogłaszanych przez Narodowe Centrum Badań i Rozwoju. Pierwszym z nich był projekt pt.: „Zaawansowane technologie informatyczne wspierające procesy analizy danych (gł. finansowych) w obszarze przestępczości finansowej", opisany w [P_1]. Drugi projekt ma tytuł „Elektroniczny system zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości" i został scharakteryzowany w [P_2]. Oba projekty były realizowane w ramach obszaru „Bezpieczeństwo i obronność państwa".

## I. Uogólniony i dziedzinowe modele danych w odniesieniu do repozytoriów i rejestrów administracji publicznej; zasoby informacyjne administracji publicznej

Charakterystyka istniejących repozytoriów, rejestrów i ewidencji została przedstawiona w pracach [A_44, A_45, A_98, A_105, A_114]. Publikacje [B_61, B_89, B_108, B_109, B_110, B_112, B_113, B_115] są ich rozszerzeniem i uszczegóławiają wybrane kwestie związane z modelami dziedzinowymi i zakresem przetwarzanych danych. Począwszy od rozważań ogólnych, związanych z funkcjonowaniem scentralizowanych i rozproszonych baz danych [A_114, B_115, B_110, B_108, B_109], poprzez kwestie związane z różnorodnością samych systemów baz danych (systemy heterogeniczne i homogeniczne) oraz różnorodnością funkcjonujących systemów informatycznych [A_45, B_61, B_110], poprzez obszary, w których są wykorzystywane [A_44, A_98, B_112, B_113], a skończywszy na analizie porównawczej zasobów informacyjnych nie tylko w Polsce, ale również w krajach Unii Europejskiej [A_105, B_110].

Osiągnięcie przedstawione w [A_44, A_45, A_98] to propozycja uogólnienia zawartości zasobów danych wykorzystywanych w systemach informatycznych. Rozważania zostały oparte przede wszystkim na analizie rozwiązań już istniejących, ale również w oparciu o zastosowania, które mogą (lub powinny) się pojawić w najbliższej przyszłości. Wynika to nie tylko z naturalnego rozwoju technologii informatycznych, ale również z już istniejących i planowanych uregulowań prawnych [A_98, B_112, B_113]. Jest to o tyle istotne, że niektóre z przyszłych zmian prawnych są wymuszone już wprowadzonymi (lub zapowiedzianymi) zmianami na poziomie unijnym.

Dużą zaletą prezentowanych propozycji uogólnienia modeli danych jest to, że przeprowadzone analizy zawartości danych dotyczą nie tylko ich struktur formalnych (wynikających z zastosowanych

technologii informatycznych), ale również uwzględniają semantykę danych. Takie rozwiązanie pozwala zakładać, że przedstawione rozwiązania są na tyle uniwersalne, że będą mogły znaleźć zastosowania nie tylko w krajowych rozwiązaniach, ale również na poziomie co najmniej europejskim. Przedstawione propozycje zawartości modeli informacyjnych obejmują zarówno dane dotyczące osób fizycznych, jak również dane dotyczące podmiotów prawnych. Ze względu na niejednoznaczność wielu pojęć z tego zakresu oraz rozbieżności w rozumieniu tych samych pojęć, konieczne było przyjęcie pewnych założeń, które dawały możliwość uwzględnienia ich w jednym modelu [A_98]. Analizę przeprowadzono w oparciu o rozwiązania krajowe oraz unijne.

Opracowane technologie (przedstawione w [P_1] i [P_2]) obejmowały konieczność rozwiązania serii problemów badawczych, które w dalszej kolejności były weryfikowane w trakcie opracowywania publikacji.

Przedstawione w [A_44, A_45, A_98, A_105, A_114] charakterystyki rejestrów i ewidencji publicznych zasobów danych obejmują bazy danych wykorzystywane przez administrację publiczną. Prowadzone badania dotyczyły rejestrów i ewidencji, których istnienie jest wymuszane uregulowaniami legislacyjnymi na obszarze Polski, ale badania obejmowały również zasoby danych funkcjonujące w krajach unijnych. Podejście takie wynikało m.in. z potrzeby uwzględnienia rozwiązań występujących w innych krajach w kontekście współpracy pomiędzy państwami członkowskimi Unii Europejskiej. Zbieranie, przetwarzanie i udostępnianie danych występujących w analizowanych rejestrach wynika z uregulowań prawnych (zarówno szczebla krajowego, jak i unijnego).

Opracowanie [A_98] dotyczy poszerzonego spojrzenia na zasoby danych, przetwarzanych w systemach informatycznych, a których zakres oraz przetwarzanie są ściśle związane z koniecznością zadośćuczynienia wymogom formalno-prawnym. Analiza obejmuje wszelkiego rodzaju dane, które związane są z informacjami na temat osób fizycznych i prawnych oraz podmiotów nieposiadających osobowości prawnej. Analiza dotyczy także próby stworzenia uogólnionego modelu środowiska homogenicznego, który dawałby możliwość wykorzystania klasycznych metod i narzędzi teleinformatycznych przy uwzględnieniu istniejących i aktualnie tworzonych norm prawnych w tym zakresie. Przedstawiona analiza obejmuje także potencjalne efekty, które mogą się pojawić w konsekwencji zmian w sposobie i trybie przetwarzania danych jako skutek zmian uregulowań prawnych.

W pierwszej części pracy [A_44] przedstawiono zestawienie rejestrów i ewidencji prowadzonych w wybranych krajach Unii Europejskiej (9 państw). Porównanie dotyczy podstawowych rejestrów danych związanych z osobami fizycznymi, podmiotami prowadzącymi działalność gospodarczą, nieruchomościami oraz podstawowych ewidencji pojazdów (samochodów, statków powietrznych i statków pływających). Dla niektórych z omawianych krajów pominięte zostały informacje dotyczące określonych rejestrów i ewidencji ze względu na brak dostępu do takich informacji lub dostępne informacje są zbyt niejednoznaczne. Przedstawione charakterystyki wybranych zasobów danych, wybranych krajów Unii Europejskiej nie wyczerpują oczywiście tematyki całego zagadnienia. Zauważyć można, że zakres danych, sposób ich przechowywania, sposób dostępu bywa bardzo różny, w zależności od poziomu rozwoju, jak też uwarunkowań prawnych właściwych dla danego kraju. Polska pod tym względem nie różni się od pozostałych państw członkowskich. W części drugiej [A_44] znajduje się propozycja wybranych elementów uogólnionego modelu danych, który związany jest z zakresem danych przetwarzanych we wspomnianych rejestrach i ewidencjach, i który obejmuje wszystkie omawiane kraje.

W pierwszej części opracowania [A_45] przedstawiono podstawowe, zawierające najwięcej istotnych danych, rejestry i ewidencje, dotyczące osób fizycznych i osób prawnych. Wszystkie te zasoby są zbierane, przetwarzane, udostępniane i archiwizowane zgodnie z obowiązującymi, polskimi uregulowaniami prawnymi (na ogół są to akty w randze ustaw oraz – uzupełniające je – unormowania rangi rozporządzeń i uregulowań wewnętrznych odpowiednich resortów). Ze względu na dużą liczbę

wszelkiego rodzaju rejestrów, wykazów, ewidencji i spisów, do dalszej analizy wybrane zostały tylko te, które dotyczą najważniejszych informacji o osobach fizycznych i osobach prawnych oraz te, które zawierają informacje najbardziej pełną (zarówno w kontekście zakresu gromadzonych danych dla poszczególnych podmiotów, jak również w kontekście liczby jednostek, o których te dane są przetwarzane). Druga część opracowania [A_45] obejmuje charakterystykę uogólnionego modelu, który zakłada istnienie jednego systemu, dającego możliwość analizy wszystkich przetwarzanych danych w środowisku homogenicznym. O ile próba prowadzenia różnorodnego typu analiz w istniejących środowiskach heterogenicznych może być porównywana z przetwarzaniem typu „big data", o tyle skonstruowanie jednego modelu dla wszystkich przetwarzanych zasobów będzie mogło skutkować możliwością wykorzystania „tradycyjnych" metod analizy danych. W szczególności dotyczyć to będzie tych zasobów, które w „swoich" środowiskach są przetwarzane przy wykorzystaniu klasycznych, istniejących już metod i narzędzi informatycznych. Drugim istotnym elementem, rozpatrywanym w tej części, jest analiza podstaw prawnych związanych z przetwarzaniem zgromadzonych zasobów. Biorąc pod uwagę narzucone, często bardzo restrykcyjne, ograniczenia wynikające w uregulowań prawnych związanych z określonymi obszarami zastosowań (czasami bardzo ściśle zdefiniowanymi), przeprowadzono również analizę konsekwencji, które mogą wystąpić w przypadku zmiany tych uregulowań. Dotyczy to, z jednej strony – jeszcze większego uściślenia ograniczeń, z drugiej zaś – próby ich uogólnienia. Należy także zauważyć, że niektóre z charakteryzowanych zasobów mogą być przetwarzane (w części lub w całości) w sposób tradycyjny, czyli nie wykorzystujący technologii teleinformatycznych.

Istotne jest również wskazanie, jakie rodzaju korzyści mogą wynikać z wykorzystania proponowanego powyżej podejścia. W pracy [A_105] przedstawiona została propozycja wykorzystania analizowanych zasobów do wspomagania zarządzania w dowolnej organizacji. Proces dostosowywania organizacji do wdrożenia dowolnego systemu informatycznego lub integracji już istniejących systemów, należy zacząć od udzielenia odpowiedzi na podstawowe pytania: (i) Czy organizacja wie, jakie informacje są lub będą jej potrzebne ? (ii) Czy organizacja jest przygotowana do wykorzystania zintegrowanych informacji ? oraz (iii) Czy ograniczenia formalne (ustawodawstwo krajowe, ustawodawstwo unijne, przepisy wewnętrzne organizacji, etc.) dają możliwość pozyskania i wykorzystania informacji, w tym informacji pochodzących ze zintegrowanych źródeł ? W pracy [A_105] znajduje się próba przybliżenia niektórych zagadnień zawartych w tych pytaniach, ze szczególnym uwzględnieniem możliwości pozyskiwania danych z zasobów publicznych. Ze względu na złożoną problematykę integracji oraz szeroki zakres możliwych do wykorzystania danych, przedstawione rozważania zostały ograniczane do określonych typów organizacji oraz określonych zasobów informacyjnych. Należy również zauważyć, że możliwość dostępu do określonych zasobów informacji zmienia się z czasem. Wynika to przede wszystkim ze zmian technologicznych, a także z faktu, że coraz większy zakres danych jest przedmiotem zainteresowania osób i organizacji. Szybki rozwój platform integracyjnych oraz „podążająca" za tym rozwojem zmiana zainteresowania pozyskiwaniem danych przez różnego rodzaju organizacje, wymuszają na analitykach i projektantach konieczność kompleksowego podejścia do proponowanych rozwiązań. Dotyczy to zarówno integracji istniejących już źródeł danych, jak również możliwości pozyskiwania nowych danych (czy to poprzez integrację różnych zasobów, czy też poprzez budowę nowych systemów, obejmujących coraz to szersze zasoby danych). W pracy tej scharakteryzowane zostały również podstawowe zasoby (rejestry, ewidencje, bazy danych), które są dostępne publicznie, a których integracja nie tylko na poziomie krajowym, ale również europejskim, jest możliwa w niedalekiej przyszłości. Prace związane z integracją tych zasobów były prowadzone również na poziomie Unii Europejskiej (np. projekt STARK - projekt związany z tożsamością elektroniczną wszystkich mieszkańców krajów członkowskich). Przedstawiona charakterystyka zasobów danych dotyczyła wybranych krajów Unii Europejskiej: Czech, Francji, Hiszpanii, Holandii, Litwy, Niemiec, Węgier, Wielkiej Brytanii i Włoch.

Analiza zasobów informacyjnych, gromadzonych przez różnego rodzaju instytucje i organizacje, pozwala spojrzeć na nie jak na olbrzymią bazę danych (w literaturze przedmiotu często nazywaną zasobami danych). Zasoby te są gromadzone w różnej postaci, zarówno elektronicznej, jak i tradycyjnej – papierowej. W połączeniu z nowoczesną technologią, którą można zastosować do ich analizy, dają możliwość uzyskania ogromnej wiedzy na temat dowolnego podmiotu (dotyczy to zarówno osób fizycznych, jak i osób prawnych). Ze względu na różne technologie, które są wykorzystywane do przetwarzania tych zasobów, nie ma możliwości zastosowania uniwersalnych narzędzi informatycznych, które dawałyby możliwość łatwego pozyskiwania interesujących nas danych analitycznych. Szczególnie istotne jest to w przypadku dostępu do danych, które w całości lub częściowo przetwarzane są w sposób tradycyjny. W mniejszym stopniu dotyczy to zasobów przetwarzanych w izolowanych środowiskach informatycznych.

Funkcjonujące, praktyczne rozwiązania wykorzystujące olbrzymie zasoby danych związane są z koniecznością projektowania rozległych (i rozproszonych) systemów informatycznych, które wykorzystują rozproszone zasoby danych. W artykule [A_114] przedstawione zostały wybrane elementy związane z projektowaniem rozproszonych baz danych, ze szczególnym uwzględnieniem systemów informatycznych, które są narażone na celowe niszczenie elementów sieci komputerowej (na przykład systemów wojskowych). Rozważono problem rozproszenia, alokacji i replikacji rozproszonej bazy danych. Szczegółowo zagadnienia te zostały opisane w monografii [B_115]. W książce tej opisana została metoda fragmentacji, alokacji i replikacji zbiorów danych rozproszonej bazy danych (RBD). W rozdziale pierwszym przedstawione zostały podstawowe pojęcia, opisane metody rozwiązywania problemów związanych z projektowaniem rozproszonych baz danych. Scharakteryzowany został problem zastosowania RBD w specyficznych systemach informatycznych, które są narażone na celowe niszczenie elementów sieci komputerowej oraz problemy, które mogą być z tym związane. W rozdziale drugim zawarty został opis modelu matematycznego fragmentacji, alokacji i replikacji zbiorów danych w RBD. Rozdział trzeci zawiera różne sposoby formułowania zadań fragmentacji, alokacji i replikacji zbiorów danych w RBD oraz wybrane metody ich rozwiązywania. Symulacyjna metoda wyboru strategii fragmentacji, alokacji i replikacji zbiorów danych w RBD odpornej na niszczenie węzłów sieci rozproszonej został przedstawiona w kolejnym rozdziale (wraz z charakterystyką eksperymentu symulacyjnego wyznaczania tej strategii). Rozdział ostatni zawiera opis sposobu interpretacji wyników opracowanej metody w procesie projektowania RBD. Obie pozycje [A_114] i [B_115] pokazują możliwość rozwiązywania złożonych problemów z wykorzystaniem zarówno metod analitycznych, jak i symulacyjnych.

Charakterystyka wykorzystania hurtowni danych, jako jednego ze sposobów wspomagania zarządzania dużymi wolumenami danych, została przedstawiona na przykładzie wspomagania zarządzania wiedzą [B_108] i [B_109]. W [B_108] scharakteryzowany został sposób wykorzystania hurtowni danych w systemach wspomagających zarządzanie wiedzą. W pierwszej części opisano systemy zarządzania wiedzą, ich historyczne początki, stan wykorzystania takich systemów w Polsce. Szczegółowo zostały scharakteryzowane: wiedza jawna i wiedza ukryta, sposób zarządzania wiedzą oraz metodologie projektowania systemów zarządzania wiedzą. Wymienione zostały i opisane podstawowe narzędzia wspierające procesy zarządzania wiedzą. W końcowej części zostało scharakteryzowane wykorzystanie różnorodnego środowiska z hurtownią danych w systemach zarządzania wiedzą. Ostatnia część opisuje architekturę systemu zarządzania wiedzą oraz realizację podstawowych funkcji takiego systemu (gromadzenie wiedzy, oczyszczanie, składowanie, wyszukiwanie i dystrybucję wiedzy) w oparciu o wykorzystanie hurtowni danych. Natomiast w [B_109] scharakteryzowany został sposób wykorzystania wybranej implementacji narzędzi do projektowania hurtowni danych (SAS Institute) w systemie wspomagającym zarządzanie wiedzą. W pierwszej części narzędzia te zostały wymienione i krótko opisane. Przyjęte kryteria wykorzystano do oceny systemu zarządzania wiedzą opartego o wielowymiarowy model danych, systemu opartego o relacyjny model

danych. Ponadto przedstawiono koncepcję systemu zarządzania wiedzą wykorzystującego rozszerzony relacyjny model danych. Model ten został opracowany w oparciu o wyniki oceny dwóch wcześniejszych zastosowań.

Teoretyczne rozważania wskazane w powyższych opracowaniach zostały wykorzystane przez habilitanta praktycznie. W opracowaniu [B_112] został przedstawiony zarys sposobu realizacji projektu PESEL2 na tle szerszej perspektywy i roli, jaką powinien pełnić w unowocześnianiu funkcjonowania polskiej administracji i wykonywaniu przez nią usług publicznych. Natomiast w [B_113] program PESEL2 został przedstawiony jako jeden z elementów, które tworzą całość w ramach koncepcji społeczeństwa informacyjnego, obejmującego w szczególności obsługę obywatela i przedsiębiorcy oraz stworzenie możliwości świadczenia usług przez administrację publiczną za pośrednictwem środków komunikacji elektronicznej. Projekt PESEL2, którego realizacja planowana byłą na lata 2006-2008, był elementem Programu PESEL2. W programie tym, jednym z podstawowych założeń była budowa nowych i integracja istniejących systemów informatycznych w ścisłym związku z jednoczesnymi zmianami organizacyjnymi i prawnymi. Jest to próba budowy nowoczesnej e-administracji, polegającym na czymś więcej niż technicznej integracji systemów informatycznych funkcjonujących w administracji publicznej, w oparciu o jednolite techniczne standardy interfejsów i danych. Wprowadzane zmiany mają dotyczyć przede wszystkim definicji nowych procesów informacyjnych, ukierunkowując funkcjonowanie administracji na znoszenie istniejącej asymetrii praw, obowiązków i odpowiedzialności między państwem a obywatelem, w tym szczególnie na zniesienia asymetrii informacyjnej między państwem i obywatelem. Można zauważyć, że przedstawiona przez habilitanta w ówczesnym czasie **koncepcja biometrycznego dowodu osobistego** została zrealizowana dopiero w marcu 2019 r.

Monografia [B_110] stanowi kompendium wiedzy przydatnej funkcjonariuszom krajowych organów prowadzących postępowanie zmierzające do odzyskania szeroko rozumianego mienia pochodzącego z przestępstwa, dzięki wykorzystaniu instrumentów międzynarodowej pomocy prawnej. Celem zasadniczym było omówienie sposobu uzyskania informacji zgromadzonych w różnego rodzaju zbiorach, rejestrach, bazach danych, które mogą służyć przede wszystkim ustaleniu składników takiego mienia, ich aktualnego statusu prawnego, a także lokalizacji. Mimo dość dynamicznie rozwijającej się regulacji wspólnotowej, dotyczącej opisywanego zagadnienia, dyktującej przyjęcie określonych rozwiązań w prawie wewnętrznym poszczególnych krajów członkowskich Unii Europejskiej, do skutecznego wystąpienia z wnioskiem o pomoc prawną jest bardzo przydatne syntetyczne przedstawienie założeń materialnoprawnych i proceduralnych obowiązujących w porządku prawnym konkretnego państwa członkowskiego.

Kolejnym przykładem wykorzystania zaproponowanego uogólnienia wykorzystywanych schematów zasobów danych jest rozdział 4: „Interoperacyjność modeli informacyjnych wykorzystywanych przez systemy informacji geograficznej w kontekście globalizacji” w monografii [B_89], którego autorem jest habilitant. Konieczność jednolitej polityki dotyczącej danych wykorzystywanych w systemach informatycznych, w tym systemach informacji geograficznej, wymaga standaryzacji zarówno samych systemów, jak i rejestrów związanych z tymi obszarami. Powyższe zagadnienia dotyczą nie tylko kwestii prawnych związanych z tymi obszarami danych, ale także rozwiązań informatycznych obowiązujących w poszczególnych państwach członkowskich UE. Osiągnięcie pełnej interoperacyjności jest prawdopodobnie kwestią przyszłości, niemniej prace przygotowawcze w tej dziedzinie powinny być realizowane od zaraz. Pierwszym krokiem powinno być skonstruowanie odpowiedniego modelu informacyjnego, który będzie stanowić podstawę do dalszych prac. Uzyskanie wymaganego homogenicznego systemu jest możliwe dla poziomu modelu danych (na przykład w ramach standaryzacji schematu bazy danych) z opracowaniem specjalistycznego metamodelu danych i wykorzystaniem metod eksploracji danych (szczególnie w tak zwanych tematycznych hurtowniach danych) lub przez zaprojektowanie oraz zbudowanie dedykowanego,

wyspecjalizowanego systemu. W pierwszej części przedstawiono zestawienie rejestrów i ewidencji prowadzonych w wybranych krajach Unii Europejskiej. Porównanie dotyczy podstawowych rejestrów danych związanych z osobami fizycznymi, podmiotami prowadzącymi działalność gospodarczą, nieruchomościami oraz podstawowych ewidencji pojazdów (samochodów, statków powietrznych i statków pływających). Dla niektórych z omawianych krajów pominięte zostały informacje dotyczące określonych rejestrów i ewidencji ze względu na brak dostępu do takich informacji lub dostępne informacje są zbyt niejednoznaczne. Przedstawione charakterystyki wybranych zasobów danych, wybranych krajów Unii Europejskiej nie wyczerpują oczywiście tematyki całego zagadnienia. Zauważyć należy, że zakres danych, sposób ich przechowywania, sposób dostępu bywa bardzo różny, w zależności od poziomu rozwoju, jak też uwarunkowań prawnych właściwych dla danego kraju. Polska pod tym względem nie różni się od pozostałych państw członkowskich. W części drugiej znajduje się propozycja wybranych elementów uogólnionego modelu danych, który związany jest z zakresem danych przetwarzanych we wspomnianych rejestrach i ewidencjach i który obejmuje wszystkie omawiane kraje.

Opracowana technologia (w ramach projektu IAFEC [P_1]) została również opisana w pracach [B_61] i [B_110], gdzie wskazano na możliwość wykorzystania opracowanych uogólnionych modeli danych w procesach związanych ze zwalczaniem i przeciwdziałaniem przestępczości. Obie prace wskazują jak istotna jest integracja systemów informatycznych. W szczególności dotyczy to integracji zasobów informacyjnych, które są w nich wykorzystywane – zarówno w obszarze jednolitych identyfikatorów, jak i semantyki przetwarzanych danych.

Spis tytułów publikacji podstawowych i uzupełniających wykorzystanych w prezentowanym zagadnieniu znajduje się poniżej. Szczegóły publikacji znajdują się wykazie opublikowanych prac naukowych.

[A_44] *Generalized data model in distributed registers.*
[A_45] *Interoperability and globalization of information models.*
[A_98] *Uogólniony model danych w rozproszonych rejestrach ewidencyjnych.*
[A_105] *Wspomaganie zarządzania - zasoby publiczne w wybranych krajach unijnych.*
[A_114] *Mathematical and Simulation Model of Fault Tolerance Distributed Database Systems.*
[P_1] *Projekt IAFEC.*
[P_2] *Projekt RFID.*
[B_61] *Rejestry publiczne wykorzystywane przez organy odpowiedzialne za wykrywanie i przeciwdziałanie przestępczości.*
[B_89] *Enhancing a City via GIS: Issues and challenges. Rozdział 4. Interoperability of information models used by geographic information systems in the context of globalization.*
[B_108] *Hurtownie danych w systemach zarządzania wiedzą.*
[B_109] *Hurtownia danych w systemie zarządzania wiedzą - rozwiązanie modelowe.*
[B_110] *Odzyskiwanie mienia w wybranych krajach Unii Europejskiej - rozwiązania prawne i bazy danych. Czechy, Francja, Hiszpania, Holandia, Litwa, Niemcy, Węgry, Wielka Brytania, Włochy.*
[B_112] *PESEL2 - projekt, program realizacyjny i rola systemu.*
[B_113] *Przebudowa i integracja rejestrów państwowych.*
[B_115] *Wybrane problemy projektowania rozproszonych baz danych.*

## II. Wybrane aspekty bezpieczeństwa w przetwarzaniu zasobów informacyjnych administracji publicznej; podejście zorientowane procesowo i oparte na analizie ryzyka

Ciągły rozwój technologii informatycznych oraz równie szybkie zmiany w otoczeniu projektowanych systemów informatycznych wymuszają znajdowanie rozwiązań, które w większym stopniu uwzględniałyby tą zmienność. Jedną z kwestii, która powinna być (a wręcz musi być) rozważana, jest ochrona i bezpieczeństwo informacji oraz ocena ryzyk związanych z utrzymaniem tego bezpieczeństwa. Przedstawione w pracach [A_6], [A_29], [A_40], [A_42], [A_96] oraz [A_106] propozycje pozwalają uwzględnić wiele elementów związanych z bezpieczeństwem informacji niezależnie od rozwiązań stosowanych obecnie czy też rozwiązań, które będą miały zastosowanie w przyszłości.

Zagadnienia dotyczące integracji systemów na bazie tworzenia platform integracyjnych oraz wsparcia tych działań poprzez wykorzystanie podejścia procesowego do tworzenia rozwiązań informatycznych zostały scharakteryzowane w [A_96] i [A_106] oraz w publikacjach uzupełniających [B_35], [B_41], [B_81], [B_94], [B_107] i [B_111]. Bezpieczeństwo zasobów informacyjnych (bezpieczeństwo informacji) opisano w [A_6] oraz w [B_1], [B_3], [B_5], [B_7], [B_11], [B_12], [B_15], [B_16], natomiast zagadnienia dotyczące zarządzania ryzykiem w bezpieczeństwie zasobów informacyjnych zostały scharakteryzowane w [A_29], [A_40] i [A_42] oraz w publikacjach uzupełniających [B_93], [B_19], [B_28]. Opisane tam modele i metody zarządzania ryzykiem w wielu przypadkach odwołują się do rozwiązań znanych i wykorzystywanych w innych obszarach (przykładowo, wykorzystanie metod optymalizacji wielokryterialnej).

W pracy [A_96] wskazano na ile istotna jest integracja wszystkich elementów infrastruktury teleinformatycznej. Integracja na poziomie technicznym oraz na poziomie oprogramowania systemowego jest w ogólności mocno zaawansowana. Największym wyzwaniem jest integracja na poziomie informacyjnym. Oprócz aspektów związanych z integracją danych (otrzymujemy w efekcie integrację informacyjną) bardzo istotna jest integracja na poziomie organizacyjnym oraz ściśle z tym związana integracja na poziomie otoczenia formalno-prawnego. W wielu organizacjach częste dyskusje i narady są skutkiem wrażenia, że ludzie w firmie pracują coraz więcej, a mimo to wyniki ekonomiczne są coraz gorsze (a co najmniej – nie rosną). Wyszukiwani są wybitni specjaliści, inwestycje są ostrożne, bezpieczne, uwzględniające zmiany rynkowe i zmiany w zachowaniach klientów. W ogólności, postępowanie członków zarządu jest zgodne z regułami zarządzania, a biznes nie rozwija się tak, jak powinien. Zwykle jednak nie wszyscy mają takie kłopoty - inne firmy, działające na podobnych lub tych samych rynkach, rozwijają się lub rosną o wiele szybciej. Co jest lub co może być przyczyną takiego stanu? Być może są bardziej zwinni, dzięki pewnemu fundamentowi działania, posiadają zintegrowane procesy biznesowe, a systemy informatyczne zapewniają elastyczność, bowiem wykorzystują platformę integracyjną. Być może implementują w swoich procesach takie technologie, które pomagają w sposób pewniejszy i wydajniejszy realizować podstawowe operacje, związane z prowadzoną działalnością. Być może podjęto decyzje, które operacje należy rozwijać i które z nich wymagają szczególnego traktowania, np. poprzez wprowadzenie lub rozbudowę systemów informatycznych, które są odpowiedzialne za te operacje lub je wspomagają. W tego typu przedsięwzięciach, technologie informatyczne, w tym i platforma integracyjna, stają się aktywami i stanowią jeden z głównych elementów fundamentu, zapewniającego firmie sprawność i elastyczność działania.

Kolejnym aspektem, który musi być brany pod uwagę to możliwość, a w niektórych przypadkach wręcz konieczność, wykorzystania podejścia procesowego w projektowaniu i wytwarzaniu systemów informatycznych wspomagających realizację usług (w tym usług publicznych). Podejście to zostało zaprezentowane w artykule [A_106]. Systemy wspomagające realizację usług (w szczególności

publicznych) wymagają ciągłego rozwoju i dostosowywania do zmieniających się warunków otoczenia (głównie prawnego), a zastosowanie podejścia procesowego w znacznym stopniu upraszcza i skraca czas potrzebny na wprowadzenie niezbędnych zmian. Scharakteryzowany został także przykładowy katalog usług, które mogą być realizowane przez takie systemy. Artykuł zawiera przykład rzeczywistego, funkcjonującego rozwiązania, zrealizowanego w oparciu o przedstawione podejście. Problemy związane z wykorzystaniem podejścia procesowego w środowiskach zintegrowanych zostały rozbudowane o elementy wynikające z konieczności zachowania określonego poziomu bezpieczeństwa zasobów, charakterystykę tego podejścia można znaleźć m.in. w pracach [A_42], [A_29], [A_6] oraz [A_40].

Bezpieczeństwo zasobu intelektualnego oraz konieczność zachowania ciągłości działania organizacji jest przedmiotem artykułu [A_42]. Celem tego artykułu było pokazanie wpływu, różnych kategorii czynników ryzyka zasobu intelektualnego, jako części składowej kapitału intelektualnego, na ich bezpieczeństwo oraz ciągłość działania. Na podstawie analizy literatury przedmiotu oraz własnych obserwacji podjęto próbę zdefiniowania trzech rodzajów modeli ryzyka aktywów intelektualnych. Istotną część opracowania poświęcono metodyce oceny ryzyka zasobu intelektualnego. Prezentowane podejście bierze pod uwagę różne kategorie czynników ryzyka, wynikających zarówno z architektury samego zasobu intelektualnego jak i również elementów, mających zastosowane w pozostałych procesach i obszarach zarządzania kapitałem intelektualnym. Przedstawione w tym artykule modele mogą stanowić punkt wyjściowy do opracowania metodyki szacowania ryzyka aktywów intelektualnych organizacji, właściwych polityk, np.: bezpieczeństwa informacyjnego organizacji, ryzyka czy jakości, które z kolei mogą stanowić wielkości wejściowe do opracowania systemu zarządzania ryzykiem kapitału intelektualnego organizacji.

W pracy [A_29] zaprezentowano metodykę zarządzania ryzykiem uwzględniającą przyjęty model ryzyka zasobu informacyjnego, metodę analizy i szacowania ryzyka oraz przykładowe obszary i czynniki ryzyka odnoszące się do zagrożeń występujących w poszczególnych fazach cyklu życia zasobu informacyjnego i wiążące je w sposób pozwalający na możliwie pełne i jednoznaczne wyznaczenie poziomu ryzyka, przy jednoczesnym zachowaniu praktycznej użyteczność proponowanego podejścia. W ostatnim czasie pojęcie oceny ryzyka zyskało na popularności w niemalże wszystkich dziedzinach życia, począwszy od biznesu przez medycynę po bezpieczeństwo informacyjne. Przedmiotem artykułu [A_29] jest metodyka zarządzania ryzykiem w bezpieczeństwie zasobów informacyjnych, do przetwarzania których wykorzystywane są technologie informacyjne, szczególnie technologie IT. Celem artykułu była prezentacja autorskiej metodyki zarządzania ryzykiem zasobów informacyjnych, uwzględniającej różne metody, modele i techniki z zakresu inżynierii ryzyka, istotnych z perspektywy zapewnienia kompletności procesu zarządzania ryzykiem w bezpieczeństwie oraz wyznaczania poziomu ryzyka zasobów informacyjnych. Na etapie opracowywania metodyki zastosowane zostały metody i narzędzia badawcze takie jak: studia literatury fachowej, krytyczna analiza dokumentów i różnych zasobów informacyjnych badanych jednostek organizacyjnych oraz rozmowy z właścicielami zasobów informacyjnych, administratorami baz danych lub systemów informatycznych. Artykuł prezentuje metodykę zarządzania ryzykiem uwzględniającą autorski model ryzyka zasobu informacyjnego oraz autorską metodę analizy i szacowania ryzyka, wiążące je w sposób pozwalający na skuteczne zarządzanie ryzykiem. Elementem obiektywizacji proponowanej w pracy metodyki jest odejście od powielania klasycznego procesu zarządzania ryzykiem i wprowadzenie dodatkowych elementów na etapach analizy, szacowania i ewaluacji ryzyka. W pierwszej części artykułu dokonano przeglądu aktualnie dostępnych metodyk zarządzania ryzykiem, zaczerpniętych zarówno z literatury fachowej, jak i z norm serii ISO. Kolejna część zawiera opis koncepcji metodyki zarządzania ryzykiem zasobów informacyjnych. Podstawowymi elementami składowymi przedstawionej metodyki są zasady, struktura ramowa oraz przegląd procesu zarządzania ryzykiem

zasobów informacyjnych. Rozdział ostatni stanowi uszczegółowienie i rozwinięcie koncepcji metodyki zarządzania ryzykiem zasobów informacyjnych.

W artykule [A_6] przedstawiono koncepcję sposobu oceniania użyteczności konfiguracji bezpieczeństwa przy wykorzystaniu dwóch punktów odniesienia (ideału i anty-ideału). Koncepcja ta odpowiada naturalnej intencji zbliżania się do punktu idealnego. W przypadku istnienia kilku takich rozwiązań można uzyskać rozwiązanie, które zapewnia największe oddalenie się od sytuacji uważanej za najbardziej niepożądaną. W sensie metodycznym artykuł przedstawiony został w dwóch warstwach. Warstwa pierwsza zawiera model konfiguracji bezpieczeństwa, uwzględniający wielkości opisujące właściwości użytkowe oraz cząstkowe kryteria miar ich użyteczności. Warstwa druga to sformułowanie problemu wielokryterialnej optymalizacji konfiguracji bezpieczeństwa i zaproponowanie metody jego rozwiązania. Skuteczność przebiegu procesu przetwarzania informacji w organizacji, zależy istotnie od bieżących właściwości jakościowych np.: funkcjonalnych, niezawodnościowych, użytkowych, bezpieczeństwa systemu zabezpieczeń. W związku z powyższym istotne jest właściwe sterowanie bieżącymi właściwościami systemu zabezpieczeń poprzez generowanie najbardziej pożądanych konfiguracji bezpieczeństwa spośród zbioru rozwiązań dopuszczalnych, po wystąpieniu sytuacji awaryjnej. Najbardziej pożądaną konfiguracją bezpieczeństwa jest taka, która nie tylko zapewnia utrzymanie wymaganego poziomu bezpieczeństwa, ale charakteryzuje się również najlepszymi właściwościami użytkowymi Problem ten rozpatrzony został, jako zadanie wielokryterialnej optymalizacji konfiguracji bezpieczeństwa. Problem ten stanowi główny wątek artykułu i determinuje jego ramy. Artykuł ten prezentuje następujące elementy: (i) opracowanie modeli Systemu Zabezpieczeń i Konfiguracji Bezpieczeństwa, pozwalających uwzględnić zależność poziomu bieżącego bezpieczeństwa od losowych zmian czynników zagrożeń, mających istotne znaczenie dla bezpieczeństwa procesów przetwarzania informacji; (ii) zaproponowanie wielkości opisujących właściwości użytkowe konfiguracji bezpieczeństwa oraz cząstkowych kryteriów miar ich użyteczności oraz (iii) sformułowanie problemu wielokryterialnej optymalizacji konfiguracji bezpieczeństwa i zaproponowanie metody jego rozwiązania.

Rozwinięciem powyższych zagadnień jest również artykuł [A_40], w którym zaprezentowano opis metodyki analizy i zarządzania ryzykiem systemów informatycznych, uwzględniającej różne kategorie czynników ryzyka istotnych z perspektywy przetwarzania informacji wrażliwych oraz zapewnienia kompletności procesu wyznaczanie poziomu ryzyka systemów informatycznych. Przedstawiona metodyka podzielona została na metodę analizy ryzyka systemów informatycznych oraz metodę zarządzania tym ryzykiem. Poziom ryzyka systemu informatycznego szacowany za pomocą proponowanej metody analizy ryzyka stanowi wielkość wejściową do – przedstawionej w drugiej części artykułu – metody zarządzania ryzykiem systemów informatycznych, przetwarzających dokumenty o różnych poziomach wrażliwości.

Analizując różne podejścia do szacowania poziomu ryzyka i postępowania z nim, powstaje pytanie, czy istnieje możliwość stworzenia kompletnej i spójnej metodyki analizy procesów przetwarzających dokumenty o różnych poziomach wrażliwości, uwzględniającej różne kategorie czynników ryzyka i wiążącej je w sposób pozwalający na możliwie pełne i jednoznaczne wyznaczenie poziomu ryzyka dokumentów wrażliwych, przy jednoczesnym zachowaniu praktycznej użyteczności proponowanego podejścia. Artykuł [A_40] stanowi próbę odpowiedzi na tak postawione pytanie, prezentując opis metodyki szacowania i zarządzania ryzykiem systemu informatycznego, realizującego procesy przetwarzania dokumentów o różnych poziomach wrażliwości, która jest zdaniem autorów kompletną i spójną metodyką. Ponadto przedstawiona metodyka zapewnia podstawy dla jakościowej oceny ryzyka oraz uruchomienie bardziej szczegółowej analizy; stanowi podstawę do opracowania bardziej szczegółowej metodyki zarządzania ryzykiem w bezpieczeństwie informacji; umożliwia ewaluację ryzyka na różnych poziomach pewności; umożliwia skupienie uwagi na ryzyku procesów przetwarzających dokumenty o różnych poziomach wrażliwości; jest użyteczna zarówno z perspektywy

ryzyka wynikającego „z” (konkretnego zagrożenia), jak i ryzyka „dla” (danej wartości chronionej), np. ryzyka pożaru dla danej infrastruktury bez względu na źródło pochodzenia ryzyka; pozwala wykorzystać podejście scenariuszowe; umożliwia klasyfikację ryzyka w zakresie wiarygodnych poziomów konsekwencji; pozwala identyfikować występujące ryzyka będące pod kontrolą oraz te, które wymagają wdrożenia dodatkowej kontroli lub wzmocnienia istniejącej oraz zapewnia wyniki porównywalne do tych, które wynikają z wymogów dotyczących ograniczania ryzyka. Przedstawiony proces zarządzania ryzykiem jest usystematyzowaną metodą identyfikacji, analizy i ewaluacji ryzyka w ramach całego procesu oceny ryzyka oraz podejmowaniem powtarzalnych, racjonalnych i skutecznych działań w ramach postępowania z ryzykiem, wynikającego z przyjętej strategii zarządzania ryzykiem. Uszczegółowienie i rozwinięcie zagadnień, które zostały opisane powyżej, można znaleźć w pracach [B_35], [B_41], [B_81], [B_94], [B_107], [B_111] – w zakresie sposobów modelowania procesów zachodzących w organizacjach oraz [B_1], [B_5], [B_7], [B_11], [B_12], [B_15], [B_16], [B_19], [B_28], [B_93] – w obszarach związanych z zapewnieniem bezpieczeństwa informacji.

W artykule [B_41] przedstawiono koncepcję modelowania procesów biznesowych z zastosowaniem procesów dynamicznych. Opracowane rozszerzenie definicji procesu biznesowego pozwala na konstruowanie mechanizmu dynamicznego doboru kolejno realizowanych czynności, które pozwolą na realizacje założonego w definicji celu procesu. Mechanizm doboru kolejno realizowanych czynności procesu dynamicznego stanowi rozszerzenie funkcjonalności systemu zarządzania przepływem pracy, który uwzględnia stan realizacji procesu oraz stan środowisk usługowych. Podejście procesowe stosowane podczas modelowania, projektowania, implementacji i eksploatacji systemów informatycznych wymaga od wykonawców zamodelowania i zaprojektowania procesów biznesowych, które są podstawowym i niezbędnym elementem konstrukcyjnym systemu bazującego na podejściu procesowym. Istnieje możliwość zamodelowania praktycznie wszystkich procesów, które są stosowane w działalności firmy, jednak tak kompleksowe podejście powoduje znaczący przyrost złożoności – a co za tym idzie – kosztów wykonania takiego systemu. Jeśli budowanie systemu w podejściu procesowym jest realizowane w formie przyrostowej, to oznacza, że należy wyodrębnić te procesy lub grupy procesów, które powinny być zamodelowane i zaimplementowane w pierwszej kolejności. Jeśli organizacja korzysta już z systemów automatyzacji procesów, to analiza definicji i instancji tych procesów może wspomóc podejmowanie decyzji związanych między innymi z ich efektywnością i jakością wykorzystując do tego celu metody i narzędzia analizy procesów. Do głównych kryteriów wyboru należy zaliczyć procesy, które są najczęściej realizowane w organizacji (czynnik ilościowy), procesy, które mają istotny wpływ na efektywność i koszty funkcjonowania firmy (czynnik ekonomiczny) oraz procesy, które mają istotny wpływ na realizacje głównych celów firmy (czynnik strategiczny). Natomiast procesy rzadko realizowane lub charakteryzujące się dużą zmiennością swojej struktury wymagają dużego wysiłku od projektantów procesów biznesowych co w konsekwencji powoduje, że takie procesy są często bardzo złożone w swojej konstrukcji. W takich procesach relacja pomiędzy kosztem ich wytworzenia a potencjalnym zyskiem podczas ich zautomatyzowanego przetwarzania może być wysoce niezadawalająca. Istnieje możliwość modelowania i projektowania procesów, które nie wymagają na starcie od projektantów procesów bardzo wysokiej precyzji projektowej konstrukcji. Do takiej grupy procesów można zaliczyć procesy adaptacyjne, generyczne i dynamiczne.

W artykule [B_111] przedstawiono praktyczne rozwinięcie zagadnień prezentowanych w [A_96] oraz [A_106]. Scharakteryzowano wykorzystanie podejścia procesowe w realizacji usług publicznych oraz opisano przykład realizacji usług publicznych skonstruowany na bazie takiego podejścia. Można sobie wyobrazić sytuację, że obywatel lub pracownik firmy, chcąc wykonać dowolną czynność, która wymaga kontaktu z administracją, uruchamia dedykowaną stronę internetową i realizuje wybraną czynność bez konieczności przysłowiowego „wychodzenia z domu”. Zasadne wydaje się

oczekiwanie, że w nieodległej przyszłości będzie można korzystać z usług publicznych drogą elektroniczną. Podejście procesowe dające możliwości kompleksowego uwzględnienia tych zagadnień oraz z pewnością umożliwi szybszą realizację rozwiązań związanych z e-administracją, e-obywatelem, e-usługami, e-społeczeństwem (i być może inne zagadnienie z przedrostkiem e-…). Należy przy tym pamiętać, że to, co jest widoczne na stronie internetowej, to tylko „wierzchołek góry lodowej". Pozostał część, czyli systemy, które faktycznie realizują te usługi, są niewidoczne dla użytkownika. A całość jest na tyle użyteczna, na ile te systemy są w stanie realizować usługi. I to bez względu na to, czy są to systemy ręczne, czy automatyczne.

Z kolei, zaproponowana w artykule [B_35] metodyka stanowi propozycję podejścia do analizy i zarządzania ryzykiem procesów biznesowych, biorącego pod uwagę różne kategorie czynników ryzyka z różnych obszarów działalności organizacji. Przedstawiona w pracy metodyka podzielona jest na metodę analizy ryzyka procesów biznesowych oraz metodę zarządzania tym ryzykiem. Poziom ryzyka procesu biznesowego szacowany za pomocą proponowanej metody analizy ryzyka stanowi wielkość wejściową metody zarządzania ryzykiem procesów biznesowych oraz służy do opracowania strategii zarządzania ciągłością działania i strategii zapobiegania i redukcji ryzyka. Nowoczesna organizacja nie konkuruje już tylko ceną i jakością dostarczanych dóbr i usług, jak w organizacji klasycznej, ale także jakością i bezpieczeństwem procesów biznesowych przebiegających w jej wnętrzu. Umożliwia to dostarczenie klientom wartości, których oczekują. Dzieje się to dzięki szybkiemu reagowaniu na incydenty oraz minimalizacji przebiegów decyzyjnych. Analizując różne podejścia do szacowania poziomu ryzyka, powstaje pytanie czy istnieje możliwość stworzenia kompletnej i spójnej metodyki analizy procesów biznesowych, uwzględniającej różne kategorie czynników ryzyka i wiążącej je w sposób pozwalający na możliwie pełne i jednoznaczne wyznaczenie poziomu ryzyka procesów biznesowych, przy jednoczesnym zachowaniu praktycznej użyteczności proponowanego podejścia.

Dynamiczny rozwój informatyki, technologii informacyjnych oraz ich zastosowań w wielu dziedzinach nauki oraz życia jest coraz szerszy i intensywniejszy. Ma to bardzo duży wpływ na codzienne funkcjonowanie zarówno w świecie biznesu, jak i w życiu przeciętnego człowieka. Niektóre innowacje techniczne i technologiczne mogą w znacznym stopniu usprawnić działanie oraz zwiększyć bezpieczeństwo istotnych danych, a zatem także tzw. dokumentów wrażliwych. Technologia znakowania i identyfikacji dokumentów, jaką wykorzystano do prezentacji proponowanego podejścia, to technologia RFID (*ang. Radio-Frequency IDentification*). Zaprezentowany przykład [B_81] zastosowania technologii RFID związany jest z przetwarzaniem dokumentów o różnych poziomach wrażliwości i może mieć praktyczne znaczenie w sposobie obiegu tego rodzaju dokumentów w kancelarii tajnej jak i innych organizacjach, gdzie archiwizacja i obieg dokumentów ma istotne znaczenie dla ich funkcjonowania. Oprócz tego, że tego typu rozwiązania są bardzo złożone, to również składają się z wielu różnych elementów – przy czym ta różnorodność wynika z technologii jak i zakresu funkcjonowania oraz oddziaływania tych elementów składowych (m.in.: systemów informatycznych, teleinformatycznych, elektronicznych, mechanicznych, organizacyjnych, formalno-prawnych). Dlatego też celem pracy była weryfikacja możliwości zamodelowania głównych czynności realizowanych w kancelarii tajnej w wydaniu tradycyjnych (bez automatyzacji) i z zastosowaniem systemów automatyzujących przetwarzanie z wykorzystaniem systemów teleinformatycznych (systemy workflow, rejestry i zasoby danych) i technologii RFID oraz możliwość ich weryfikacji zgodności ze standardem notacji BPMN jak i poprzez zastosowanie metody symulacji procesów. Rozważania teoretyczne przedstawione w [B_81] zostały praktycznie zweryfikowane w ramach opracowania technologii podczas realizacji projektu RFID, który został szczegółowiej opisany w [P_2].

W artykule [B_94] przedstawiono rozważania na temat znaczenia bezpieczeństwa informacji w społeczeństwie informacyjnym pod kątem wybranych aspektów prawnych. Scharakteryzowano wybrane aspekty standaryzacji w ochronie publicznych baz danych, rejestrów i usług świadczonych przez administrację publiczną. Dla każdego wymienionego typu standardu, np. ustawa, norma czy

najlepsze praktyki stowarzyszone określono minimalne wymagania i działania, jakie powinny być podejmowane i realizowane przez służby bezpieczeństwa w celu zapewnienia podstawowego poziomu bezpieczeństwa informacji przetwarzanych w instytucjach. Ponadto podkreślono, że dane, informacja i wiedza odgrywają ogromną rolę we współczesnych społeczeństwach informacyjnych, porządkach prawnych i stosunkach międzyludzkich, a także w życiu konkretnego człowieka.

Praca [B_107] przedstawia model referencyjny architektury korporacyjnej – xGEA (*ang. cross-Government Enterprise Architecture*), który wprowadza identyfikację sposobności, jakie mają wspierać usprawnienia w obszarach, na których koncentrują się strategie. W szczególności są to obszary: (i) ukierunkowania projektowania usług z wykorzystaniem technologii IT na potrzeby użytkowników (obywateli i firm); (ii) stosowania podejścia usług współdzielonych oraz (iii) rozszerzania i pogłębiania profesjonalizmu w agendach rządowych. Model ten ukierunkowuje działania na większe ponowne użycie i współdzielenie zasobów. Zaczyna on również ukierunkowywać prace na wspólne techniki i metody. Powstaje wspólny język pozwalający na budowanie procesów współdzielenia i współpracy w organizacjach rządowych. Lista potencjalnych korzyści to: promowanie projektowania wspólnej infrastruktury, usprawnienie zarządzania ryzykiem, identyfikowanie i agregowanie potrzeb na promowanie efektywnego wykorzystania zasobów, uzgodnienia współdzielonych standardów dla promowania lepszej kooperacji pomiędzy agendami rządowymi, zwiększenie konkurencyjności w dostarczaniu usług IT i produktów, zwiększenie elastyczności biznesu i redukcję kosztów posiadania. W każdym kraju obywatele chcieliby mieć jeden punkt kontaktowy do realizacji wielu swoich potrzeb we współpracy z administracją publiczną. Biznes chce dostarczać informacji administracji rządowej tylko raz. Potrzeby takie muszą być spełniane przy stałej presji na jakość dostarczanych informacji i obniżanie kosztu. Prezentowany model może te potrzeby zaspakajać w szerszym zakresie.

W pracach [B_19], [B_28] i [B_93] przedstawiono metody analizy i szacowania ryzyka zasobów informacyjnych. Artykuł [B_28] prezentuje autorską metodę analizy i szacowania ryzyka zasobów informacyjnych/systemów informatycznych, uwzględniającą różne kategorie czynników ryzyka, istotnych z perspektywy zapewnienia kompletności procesu określania lub wyznaczania poziomu ryzyka zasobu informacyjnego, przetwarzanego zarówno tradycyjnie jak i z wykorzystaniem systemów informatycznych. Przedstawiona metoda ma charakter jakościowy i podzielona jest na etap analizy ryzyka i etap szacowania ryzyka zasobów informacyjnych. Elementem obiektywizacji proponowanej metody jakościowej jest odejście od wykorzystywania na etapie ewaluacji ryzyka od tradycyjnych map ryzyka, a zastosowanie wektora, którego składowe odzwierciedlają szeroką gamę czynników, mających istotny wpływ na bieżący poziom ryzyka zasobu informacyjnego. Do jej opracowania wykorzystano metody badawcze typu studia literatury fachowej, a także krytyczna analiza aktualnie dostępnych metod ilościowych i jakościowych analizy ryzyka stosowanych w badanych organizacjach, szczególnie jednostek kancelaryjnych przetwarzających dokumenty o różnych poziomach wrażliwości. Liczba czynników ryzyka uwzględnianych w proponowanej metodzie oraz ich wszechstronność zdecydowanie wyróżniają proponowane podejście na tle wykorzystywanych obecnie metod oceny ryzyka zasobów informacyjnych/systemów informatycznych, co zdaniem autorów stanowi jego niezaprzeczalną zaletę. Przedmiotem artykułu [B_19] jest model ryzyka systemu informacyjnego przetwarzającego dokumenty o różnym poziomie wrażliwości w jednostkach kancelaryjnych, wykorzystujących do przetwarzania danych systemy informatyczne i technologie RIFD. Model stanowi wielowymiarowe podejście do analizy ryzyka systemu informatycznego oraz procesów informacyjnych w nich realizowanych. Artykuł prezentuje model ryzyka i przykładowe czynniki ryzyka odnoszące się do zagrożeń występujących w poszczególnych fazach cyklu życia systemu informatycznego i wiążące je w sposób pozwalający na możliwie pełne i jednoznaczne wyznaczenie poziomu ryzyka, przy jednoczesnym zachowaniu praktycznej użyteczność proponowanego podejścia. Artykuł stanowi próbę odpowiedzi na pytanie: „czy istnieje możliwość stworzenia kompleksowego i adekwatnego modelu oceny ryzyka systemu informacyjnego, w którym przetwarzane są zasoby o różnych poziomach

wrażliwości”? Zaproponowany model został wykorzystany do opracowania ramowej struktury systemu zarzadzania ryzykiem oraz właściwej polityki bezpieczeństwa systemu informacyjnego w badanej jednostce kancelaryjnej, w której przeprowadzono szacowanie ryzyka z wykorzystaniem opracowanego modelu.

Zapewnienie wymaganego poziomu bezpieczeństwa organizacji lub wysokiego poziomu bezpieczeństwa dla wybranych obszarów przetwarzania informacji, wymaga opracowania strategii lub dobrego projektu zabezpieczeń, zgodnie ze sprawdzoną metodyką, a następnie wdrożenia tego projektu przez specjalistów z użyciem właściwie dobranych technologii oraz utrzymania skutecznych konfiguracji bezpieczeństwa . Zaprojektowane konfiguracje bezpieczeństwa o charakterze technicznym lub organizacyjnym powinny być oparte w znacznej mierze na wynikach analizy ryzyka, specyfikacji wymagań bezpieczeństwa, a także ogólnej teorii zabezpieczeń (m.in. wymagane jest dokonanie oceny użyteczności bieżącej konfiguracji bezpieczeństwa, weryfikacji odporności zastosowanych zabezpieczeń na strategię różnego typu ataków oraz rekonfiguracji systemu zabezpieczeń wskutek wystąpienia różnego typu sytuacji awaryjnych – utraty wymaganego poziomu bezpieczeństwa). W dostępnej literaturze brak jest propozycji metod oceny skuteczności systemu zabezpieczeń skonstruowanego na podstawie konfiguracji bezpieczeństwa lub konfiguracji zabezpieczeń o charakterze technicznym lub organizacyjnym. Na wyróżnienie zasługuje metoda zaproponowana w pracy Szulima i Kuchty ()[4]. Metoda ta ma charakter metody jakościowej. Możliwość praktycznego jej zastosowania jest ograniczona do bardzo wąskiej klasy wskaźników jakości. Nie może być wykorzystana do oceny użyteczności bieżącej konfiguracji bezpieczeństwa i procesu alokacji zabezpieczeń do poszczególnych konfiguracji bezpieczeństwa – procesu rekonfiguracji. Dostępne prace wykazują na rosnącą potrzebę automatyzacji procesu rekonfiguracji, związanej z opracowaniem procedur sterowania ryzykiem w procesach biznesowych. Brak metod oraz kryteriów oceny skuteczności środków bezpieczeństwa (technicznych i organizacyjnych) utrudnia ilościową ocenę skuteczności systemów zabezpieczeń. Wymusza się zatem korzystanie z oceny jakościowej. Ocena jakościowa jest subiektywna, a jej wynik, akceptacja poziomu ochrony zasobu lub jego odrzucenie, zależy od wiedzy i doświadczenia osoby oceniającej. Skuteczna ochrona obszarów przetwarzania informacji wymaga stosowania różnego rodzaju konfiguracji zabezpieczeń, w tym wprowadzenia kilku lub kilkunastu zabezpieczeń technicznych i organizacyjnych jednocześnie. Po uwzględnieniu zbioru tych zabezpieczeń oraz różnych charakterystyk powiązań (relacji, właściwości) pomiędzy tymi zabezpieczeniami, mamy do czynienia z systemem zabezpieczeń. Celem artykułu [B_ 15] było ukazanie i rekomendacja zarówno teoretycznych, jak i praktycznych podejść do oceny skuteczności systemu zabezpieczeń. Przy określeniu poziomu bezpieczeństwa w obszarach przetwarzania informacji w organizacji akcentuje się trzy istotne zagadnienia, charakterystyczne dla konstrukcji artykułu: (1) w bieżących chwilach muszą istnieć możliwości bezpiecznego wykonywania operacji przetwarzania danych (wymaganego zbioru zasobów informacyjnych), (2) w stosunku do zasobów wrażliwych wymaga się istnienia procesów ochronnych, które zapewniają utrzymanie odpowiednich atrybutów bezpieczeństwa na akceptowalnym poziomie ryzyka oraz (3) do utrzymania wymaganych atrybutów bezpieczeństwa, w stosunku do wybranej grupy zasobów służby bezpieczeństwa ustanawiają, wdrażają i utrzymują ściśle określone konfiguracje bezpieczeństwa, zapewniające tym zasobom wymagany poziomu bezpieczeństwa lub akceptowalną wartość ryzyka. W świetle powyższego, bieżący poziom bezpieczeństwa zasobów rozumiany jest jako możliwość uaktywnienia przez służbę bezpieczeństwa właściwego zbioru zabezpieczeń w systemie informacyjnym organizacji. Relacje zachodzące pomiędzy tymi zabezpieczeniami tworzą zbiór dopuszczalnych konfiguracji bezpieczeństwa, skonstruowanych na

[4] M. Szulim, M. Kuchta, *Metoda analizy skuteczności systemu bezpieczeństwa obiektu*, Biuletyn Wojskowej Akademii Technicznej, vol. LIX, nr 4, 2016.

bazie zbioru aktualnie sprawnych zabezpieczeń o charakterze technicznym lub organizacyjnym, będących w dyspozycji zespołu obsługiwania systemu zabezpieczeń.

Prace [B_1], [B_5], [B_7], [B_11], [B_12], [B_16] obejmują zagadnienia związane z modelowaniem systemów zabezpieczeń [B_12] i [B_1], oceną ich skuteczności [B_11], automatycznym konfigurowaniem, sterowaniem i monitorowaniem [B_7] i [B_5] oraz z modelem służb [B_16] dla potrzeb utrzymania wymaganego poziomu bezpieczeństwa informacyjnego.

Celem artykułu [B_16] było określenie modelu służby bezpieczeństwa i uzasadnienie metody sterowania bieżącymi właściwościami (np. użytkowymi, funkcjonalnymi, niezawodnościowymi, bezpieczeństwa itp.) jego składników, które zapewniałyby utrzymanie wymaganego poziomu bezpieczeństwa informacji w organizacji. Wymagany poziom bezpieczeństwa informacji w organizacji można osiągnąć poprzez podejmowanie właściwych decyzji sterujących, które uaktywniają odpowiednie zbiory procesów ochronnych, przyczyniających się do podniesienia bieżącego poziomu bezpieczeństwa ochranianym obiektom. Procesy ochronne wykorzystują odpowiednie metody i techniki ochronne (zabezpieczenia) o charakterze technicznym i organizacyjnym. Relacje zachodzące między uaktywnionymi zabezpieczeniami tworzą stosowne konfiguracje bezpieczeństwa. Odpowiednie sterowanie właściwościami użytkowymi tych konfiguracji bezpieczeństwa pozwala utrzymywać wymagany poziom bezpieczeństwa informacji w organizacji. W artykule [B_12] przedstawiono koncepcję utrzymywania wymaganego poziomu bezpieczeństwa systemu informacyjnego organizacji, poprzez odpowiednie sterowanie bieżące konfiguracjami zabezpieczeń systemu zabezpieczeń. Zaproponowano model systemu zabezpieczeń i scharakteryzowano jego podstawowe elementy na potrzeby utrzymywania bieżącego poziomu bezpieczeństw zasobów informacyjnych. Pożądaną bieżącą właściwość bezpieczeństwa uzyskuje się poprzez wygenerowanie odpowiedniej konfiguracji zabezpieczeń technicznych i organizacyjnych ze zbioru rozwiązań dopuszczalnych. Zaproponowana koncepcja uwzględniająca wpływ nie tylko podstawowych elementów bezpieczeństwa zasobów informacyjnych (np.: rodzaje zasobów, atrybuty bezpieczeństwa, zagrożenia, podatności), lecz również zmianę uwarunkowań pracy zarówno systemu informacyjnego, systemu zabezpieczeń, jak i całego środowiska zarządzania bezpieczeństwem i jakością organizacji. Z kolei w pracy [B_11] rozpatrzono zagadnienie oceny skuteczności systemu zabezpieczeń w aspekcie zarzadzania bezpieczeństwem informacji (zasobów informacyjnych systemu informacyjnego organizacji). Przyjęto założenie, że celem zabezpieczania jest uzyskanie zadeklarowanego poziomu ochrony zasobów systemu informacyjnego. Zatem poziom bezpieczeństwa systemów informacyjnych w danej organizacji implikowany jest oceną skuteczności systemu zabezpieczeń. Skuteczność działania systemu zabezpieczeń zależy przede wszystkim od właściwości użytkowych jego elementów składowych oraz różnych czynników występujących w jego otoczeniu. W artykule główną uwagę skupiono na elemencie, którym jest konfiguracja bezpieczeństwa, tj. konfiguracje techniczne i konfiguracje organizacyjnych zabezpieczeń. Przyjęto tezę, że skuteczność działania systemu zabezpieczeń można rozpatrywać jako mnogościową sumę skuteczności, powołanych w nim, konfiguracji zabezpieczeń. Ponadto przyjęto, że warunkiem koniecznym możliwości wyznaczania pożądanych miar (wskaźników) oceny skuteczności systemu zabezpieczeń jest zaproponowanie tych miar oraz opracowanie właściwych sposobów (metod) ich wyznaczania. W artykule [B_7] zaproponowano model zautomatyzowanego systemu kontroli i sterowania bieżącym poziomem bezpieczeństwa informacji. Wyróżniono i scharakteryzowano podstawowe elementy systemu, takie jak: podmiot działania, przedmiot działania oraz cel działania. Ponadto zdefiniowano pojęcie konfiguracji bezpieczeństwa oraz model podsystemu sterowania bieżącym poziomem bezpieczeństwa informacji w przypadku wystąpienia sytuacji awaryjnej. Rozważania teoretyczne zostały poparte przykładem. W artykule [B_5] przedstawiono metodę oceny użyteczności konfiguracji bezpieczeństwa ze zbioru dopuszczalnych konfiguracji bezpieczeństwa, po wystąpieniu sytuacji awaryjnej. Uważa się, że najlepsza konfiguracja bezpieczeństwa to taka, która nie tylko zapewnia utrzymanie wymaganego poziomu bezpieczeństwa zasobom informacyjnym, ale

charakteryzuje się najlepszymi wielkościami opisującymi jej właściwości użytkowe. Zaproponowano wielkości opisujące właściwości użytkowe konfiguracji bezpieczeństwa oraz cząstkowe kryteria miar ich użyteczności. Miarami użyteczności konfiguracji bezpieczeństwa są wskaźniki funkcjonalne, niezawodnościowe oraz bezpieczeństwa. Praca [B_1] obejmuje koncepcję utrzymywania wymaganego poziomu bezpieczeństwa aktywów systemu informacyjnego organizacji, poprzez podejmowanie właściwych decyzji sterujących, inicjujących generowanie odpowiednich konfiguracji bezpieczeństwa. Zaproponowano i sformułowano modele podmiotu i przedmiotu bezpieczeństwa oraz model systemu informacyjnego organizacji dla potrzeb sterowania bieżącym poziomem bezpieczeństwa informacji (zasobów informacyjnych) oraz bieżącymi właściwościami użytkowymi podsystemów działania, wchodzących w skład systemu informacyjnego organizacji.

Spis tytułów publikacji podstawowych i uzupełniających wykorzystanych w prezentowanym zagadnieniu znajduje się poniżej. Szczegóły publikacji znajdują się wykazie opublikowanych prac naukowych.

[A_6] *Multicriteria optimization used for the information security - ideal and anty-ideal.*
[A_29] *Metodyka zarządzania ryzykiem w bezpieczeństwie zasobów informacyjnych.*
[A_40] *Multi-faceted methodology of the risk analysis and management referring to the IT system supporting the processing of documents at different levels of sensitivity.*
[A_42] *Models and method for the risk assessment of an intellectual resource.*
[A_96] *The importance of an integration platform within the organisation.*
[A_106] *Wspomaganie zarządzania w administracji - podejście procesowe a realizacja usług publicznych.*
[P_1] *Projekt IAFEC.*
[P_2] *Projekt RFID.*
[B_1] *Model of the Information System in the Organization for Controlling Current Level of Information Security.*
[B_3] *Zintegrowany system dostępu i analizy danych rejestrowych i ewidencyjnych* -w przygotowaniu
[B_5] *Assessment of the usefulness of the security configuration.*
[B_7] *Model of automated control and monitoring system of the current level of information security.*
[B_11] *Method for Assessing Efficiency of the Information Security Management System.*
[B_12] *The Security System for Maintenance of the Required Information Security Level.*
[B_15] *Ocena użyteczności systemu zabezpieczeń w systemie bezpieczeństwa informacji.*
[B_16] *Model służby bezpieczeństwa na potrzeby utrzymywania wymaganego poziomu bezpieczeństwa informacji w organizacji.*
[B_19] *An information system risk model for the risk management system of an organisation processing sensitive data.*
[B_28] *Metoda analizy i szacowania ryzyka zasobu informacyjnego.*
[B_35] *Wieloaspektowa metodyka analizy i zarządzania ryzykiem procesów biznesowych.*
[B_41] *Dynamic business process in workflow systems.*
[B_81] *Modelowanie procesów biznesowych przetwarzania dokumentów wrażliwych z wykorzystaniem technologii RFID.*
[B_93] *Selected aspects of risk management in respect of security of the document lifecycle management system with multiple levels of sensitivity.*
[B_94] *Wybrane aspekty standaryzacji w ochronie publicznych zasobów informacyjnych i świadczonych usług w kontekście społeczeństwa informacyjnego.*
[B_107] *Opis ram xGEA.*
[B_111] *Podejście procesowe a usługi publiczne realizowane przez administrację.*

## III. Wykorzystanie zaproponowanych modeli do zwalczenia przestępstw gospodarczych i finansowych; uwarunkowania legislacyjne

W pracach [A_9], [A_14], [A_66], [A_67], [A_68] oraz [A_88] opisano możliwość wykorzystania zaproponowanych wcześniej uogólnionych modeli danych w systemach wspierających zwalczanie różnego rodzaju przestępstw. W większości prac dotyczy to zwalczania przestępstw finansowych, ale wskazano również możliwości wykorzystania np. w walce przeciwko przestępstwom maltretowania dzieci. Podstawowe osiągnięcie dotyczy wskazania możliwości implementacji zaproponowanych modeli w rozwiązaniach praktycznych. Rozwiązano wiele problemów i zadań badawczych, które następnie zostały zweryfikowane w ramach opracowanych technologii. W ramach wskazanych publikacji poruszone zostały zagadnienia związane z wykorzystaniem istniejących rozwiązań w obszarach, w których dotychczas tych rozwiązań nie było. Np. dotyczy to nowych zastosowań biometrii i technologii RFID [A_67], [P_2]. Należy podkreślić, że propozycje nowych rozwiązań zawsze uwzględniały zmienność otoczenia, w szczególności otoczenia prawnego oraz jego potencjalny wpływ na proponowane zastosowania. Również w publikacjach uzupełniających wskazano możliwość wykorzystania zintegrowanych i uogólnionych modeli w systemach przeciwdziałania przestępstwom [B_3], [B_8], [B_10], [B_17], [B_38], [B_39] oraz [B_60]. Większość z nich dotyczy elementów zaimplementowanych w trakcie realizacji projektu [P_1]. Z jednej strony opracowane technologie pozwalały na weryfikację i rozwiązanie wielu problemów badawczych, z drugiej zaś – prace analityczno-projektowe pozwalały na opracowanie coraz lepszych (np. w kontekście ich skuteczności) rozwiązań technologicznych. Przedstawione publikacje wskazują również na to, jak istotny może być wpływ otoczenia prawnego (tzw. legislacji) na budowę efektywnych systemów informatycznych, w szczególności tych, które wykorzystują publiczne zasoby danych. Efektem prac badawczych jest m.in. wniosek dotyczący konieczności rozbudowy „Oceny skutków regulacji (OSR)" ()[5], które w sposób bardzo znaczący potrafią wpływać na istniejące i projektowane systemy informatyczne.

Współczesny rozwój technologii RFID oraz GPS, miniaturyzacja urządzeń, znaczna obniżka kosztów produkcji powodują, że technologie te znajdują coraz szersze zastosowanie. Efektem tego jest możliwość uzyskiwania dodatkowych informacji wynikających z posiadania danych, które są wynikiem funkcjonowania urządzeń wyposażonych i korzystających z technologii RFID. W połączeniu z technologią wykorzystywaną w systemach GPS można uzyskać dane służące nie tylko do bieżącego funkcjonowania systemów operacyjnych, ale również do wykonywania określonych analiz i badań, które mogą obejmować szeroki zakres dziedzinowy. Dotyczy to m.in. kwestii związanych z lokalizacją i równomiernym (pożądanym) rozłożeniem zasobów, możliwością właściwej reakcji na powstawanie niepożądanych zjawisk demograficznych lub gospodarczych, podejmowaniem szybkich i właściwych decyzji związanych z zarządzaniem zasobami. Dotyczy to zarówno zasobów wytwarzanych przez człowieka (produkty, infrastruktura, zanieczyszczenia), jak również zasobów naturalnych (woda, populacje zwierząt, naturalne zasoby roślinne). Rozwój nowoczesnych technologii, takich jak: biometria, RFID, czy GPS, daje możliwość ich zastosowania w wielu obszarach funkcjonowania człowieka. Jeszcze większym wyzwaniem dającym jeszcze większe możliwości praktycznego zastosowania, jest ich połączenie. Efektem tego połączenia może być uzyskanie dodatkowych danych,

[5] OSR – Ocena Skutków Regulacji - jeden z załączników do projektu aktu normatywnego, który opisuje przewidywane skutki proponowanych regulacji według metody analizy kosztów i korzyści. W założeniu OSR powinna zapewniać podmiotom odpowiedzialnym za tworzenie prawa świadomość konsekwencji, jakie przygotowany akt prawny może wywołać w życiu społecznym. OSR stanowi ważny element w procesie stanowienia dobrego prawa, gdyż pozwala na dostarczenie konkretnych merytorycznych argumentów dla wprowadzenia danej legislacji.

a co za tym idzie dodatkowych informacji, których pozyskanie zajęłoby znacznie więcej czasu i wymagałoby znacznie większych nakładów finansowych. W [A_67] zaprezentowana została idea stworzenia systemu lokalizacji i monitorowania osób wykorzystująca znane i częściowo już wykorzystywane rozwiązania technologiczne w obszarze biometrii, RFID oraz GPS. Praktyczne wykorzystanie proponowanych rozwiązań uwarunkowane jest poziomem zaawansowania technologicznego w poszczególnych dziedzinach i rozwojem organizacyjno-prawnym wszystkich interesariuszy.

Stworzenie jednolitych modeli rejestrów i ewidencji danych wykorzystywanych w systemach informatycznych jest niekwestionowaną koniecznością. Wynika to m.in. z możliwości korzystania ze swobodnego przepływu osób, towarów, usług i kapitału np. w obrębie Unii Europejskiej. Próby integracji funkcjonujących zasobów danych oraz systemów informatycznych, w których te zasoby funkcjonują, wskazują jak skomplikowany i kosztowny jest to proces. Mimo to, potrzeba opracowania uogólnionych modeli danych (co najmniej na poziomie pojęciowym i konceptualnym) obejmujących zarówno zakres jak i przepływ danych wydaje się nieunikniona. Uzyskanie pożądanego rezultatu np. w postaci jednorodnego systemu jest możliwe na poziomie modelu danych. Utworzenie specjalizowanego metamodelu danych daje możliwość wykorzystania metod stosowanych w eksploracji danych. Innym sposobem jest zaprojektowanie i budowa od podstaw, dedykowanych, specjalizowanych systemów informatycznych. Bez względu na sposób podejścia, należy dążyć do uzyskania integracji systemów poprzez ujednolicenie sposobów identyfikacji wszystkich obiektów, o których dane są zbierane, przetwarzane i udostępniane. Bez rozwiązania problemów identyfikacyjnych, które zostały przedstawione w [A_68], wszelkie dalsze działania związane z integracją mogą być skazane na porażkę. Podstawowym zagadnieniem, z którym mamy do czynienia w trakcie analizy różnorodnych zasobów danych, są problemy wynikające z **zastosowania różnych sposobów identyfikacji obiektów**. W praktyce, dopiero od niedawna zaczęto zwracać uwagę na to, że obiekty występujące w różnych rejestrach i ewidencjach powinny być identyfikowane w ten sam sposób. Refleksja ta wynika między innymi z faktu występowania poważnych problemów w trakcie prób równoczesnej analizy zawartości kilku rejestrów lub ewidencji. Nawet jeśli w obrębie pojedynczych rejestrów identyfikacja obiektów jest właściwa, to w przypadku prób jednoczesnego wykorzystania kilku z nich następowały ogromne problemy z powiązaniem obiektów, o których dane były przechowywane wielu miejscach. Biorąc pod uwagę powyższe problemy, zasadne wydaje się przeanalizowanie większej liczby rejestrów pod względem ich ujednolicenia oraz wskazanie zasad lub reguł, które powinny być przestrzegane w trakcie tworzenia kolejnych rejestrów lub ewidencji, czy też w momencie pracy nad wprowadzaniem lub modernizacją narzędzi informatycznych wspomagających wykorzystywanie już istniejących rejestrów i ewidencji. Z uwagi na rozwój technologii informatycznych i wynikający z niego przymus modyfikacji istniejących już rozwiązań, wprowadzenie i zastosowanie nowych reguł w procesie tworzenia jednolitych rejestrów i ewidencji wydaje się koniecznością.

W pracy [A_66] przedstawiono propozycje wykorzystania technologii biometrycznych zarówno do identyfikacji osób (w dokumentach identyfikacyjnych), jak i również do utrzymania odpowiedniego poziomu bezpieczeństwa danych, które się w tych dokumentach znajdują. Z identyfikacją osób mamy do czynienia począwszy od wystawienia Aktu Urodzenia, a skończywszy na Akcie Zgonu. W trakcie tego okresu, osoba jest wyposażana w wiele dokumentów, które zawierają dane identyfikacyjne – książeczka zdrowia, legitymacja szkolna, dowód osobisty, legitymacja studencka, paszport, prawo jazdy, legitymacja służbowa, identyfikator pracowniczy, karta dostępowa, imienna karta członkowska, karta pobytu (…) – ogólnie można stwierdzić, że zbiór ten obejmuje wszelkie dokumenty, które zawierają dane związane z imionami, nazwiskiem, datą urodzenia oraz zdjęcie. Zarówno dowód osobisty, jak i paszport, są dokumentami stwierdzającymi tożsamość. Dotyczy to przede wszystkim osób pełnoletnich, dzieci i młodzież (osoby poniżej 18-ego roku życia) również mogą otrzymać dowód osobisty lub paszport, ale obowiązek posiadania dowodu osobistego dotyczy

tylko osób pełnoletnich. Pozostałe dokumenty traktuje się raczej jako dokumenty potwierdzające tożsamość (częstym przypadkiem potwierdzania tożsamości jest okazanie przez daną osobę jednego lub dwóch dowolnych dokumentów ze zdjęciem). Z tego też względu dowód osobisty i paszport są traktowane w sposób szczególny. Dane identyfikacyjne umieszczone na/w dowodzie osobistym lub paszporcie są chronione w bardzo restrykcyjny sposób. Służą temu zarówno zabezpieczenia samych „czystych" blankietów (np.: rodzaj materiałów z jakich są wykonane, zabezpieczenia przed próbami zmian ich zawartości), zabezpieczenia związane z procesem zbierania i nanoszenia danych identyfikacyjnych na blankiety (tzw. personalizacja) oraz zabezpieczenia związane z dystrybucją i użytkowaniem dowodów osobistych oraz paszportów [A_66]. W opracowaniu scharakteryzowane zostały również różnorodne biometrie, mogące znaleźć zastosowanie w zabezpieczaniu dokumentów identyfikacyjnych (zarówno cechy fizyczne, jak i behawioralne), określając równocześnie możliwości i ograniczenia w masowym ich zastosowaniu. Możliwość, a w niektórych sytuacjach – konieczność, zastosowania danych biometrycznych wynika z coraz szerszego wykorzystania technologii informatycznych (w szczególności internetowych) w życiu codziennym i coraz częstszych prób kradzieży tożsamości osób korzystających z tych technologii. Dokument biometryczny jest pewnego rodzaju „łącznikiem", który pozwala powiązać ze sobą „osobę fizyczną" („człowieka z krwi i kości") z „osobą cyfrową" („człowieka elektronicznego złożonego z zer i jedynek"), która funkcjonuje tylko w systemie informatycznym.

W publikacjach [A_88], [A_9] oraz [A_14] przedstawione zostały koncepcje praktycznego zastosowania technologii informatycznych wykorzystujących uogólniony model danych w zwalczaniu wszelkiego rodzaju przestępczości. Praca [A_14] przedstawiona koncepcję wykorzystania metodologii rozpoznawania wzorców do wykrywania dokumentów (dowodów) świadczących o realizacji przestępczych transakcji finansowych. W metodzie wykorzystano analogie do procesów diagnostycznych rozpoznawania jednostek chorobowych w medycynie. Problematyka wykrywania transakcji finansowych związanych z działalnością przestępczą (przestępstwa finansowe, wspieranie terroryzmu, pranie brudnych pieniędzy) jest zagadnieniem bardzo trudnym i złożonym. Łączna liczba transakcji finansowych na krajowym rynku finansowym sięga dziennie kilku milionów operacji. Zakres różnorodności transakcji finansowych jest niezwykle szeroki. Transakcje finansowe realizowane są w różnych środowiskach transakcyjnych: środowiskach fizycznych, w sieciach lokalnych, pocztowych i w sieciach globalnych typu Internet. "Wyłuskanie" transakcji przestępczych jest zatem procesem niezwykle złożonym a z drugiej strony niezwykle ważnym gdyż może prowadzić do szybkiego i skutecznego identyfikowania grup przestępczych jak również predykcji samych przestępstw finansowych, a tym samym umożliwiać ich wcześniejsze wykrywanie i zapobieganie. Stąd też poszczególne państwa (w tym cała Unia Europejska) wprowadzają szereg przepisów (w tym w randze Ustaw) nakazujących instytucjom obrotu finansowego realizację odpowiednich obowiązków (procedur), gwarantujących skuteczne działania pozwalające zwalczać te zjawiska. Zgodnie z przepisami odpowiednich ustaw instytucje finansowe, w ramach stosowania środków bezpieczeństwa finansowego: „mają obowiązek prowadzenia bieżącego monitoringu stosunków gospodarczych, włącznie z badaniem transakcji dokonywanych w trakcie trwania tych stosunków w celu zapewnienia, że prowadzone transakcje są zgodne z wiedzą instytucji na temat klienta, profilu działalności oraz ryzyka, w tym w miarę możliwości, źródeł pochodzenia środków, jak również zapewnienie, że posiadane dokumenty, dane lub informacje są na bieżąco uaktualniane" ()[6]. Ze względu na skalę i złożoność systemu przepływów finansowych a przede wszystkim na wyjątkową rolę detekcji przestępczych transakcji finansowych w skutecznym wykrywaniu i zapobieganiu działalności przestępczej, koniecznością stało się wykorzystywanie odpowiednio zaprojektowanych systemów

[6] S. Acid, L.M. Campos, *A comparison of learning algorithms for Bayesian Networks: a case study based on data from an emergency medical service,* Artificial Intelligence in Medicine, vol. 30, pp. 215–232, 2004.

informatycznych, wspomagających taką działalność. Odpowiednio zaprojektowane i zrealizowane systemy informatyczne mogą się okazać bardzo skutecznym narzędziem wspomagającym wykrywanie przestępczych transakcji finansowych. Głównym modułem takich systemów jest podsystem rozpoznawania wzorców dokumentów transakcyjnych służących przestępczej działalności finansowej a w nim wielokryterialny moduł badania podobieństwa ()[7]. Automatycznie wyselekcjonowany zbiór „podejrzanych dokumentów finansowych" może być następnie zweryfikowany „ręcznie" przez ekspertów i wykorzystany do kolejnych działań operacyjnych.

W pracy [A_88] przedstawiono analizę dostępnych zasobów danych w zakresie możliwości ich wykorzystania do wykrywania i przeciwdziałania przestępczości (głównie finansowej). Analizie podlegały przede wszystkim aspekty związane m.in. z: podstawą prawną funkcjonowania zasobu, organami prowadzącymi rejestr/ewidencję, zakresem gromadzonych danych, sposobem przetwarzania oraz istniejącymi powiązaniami i zależnościami z innymi zasobami danych. Uwzględnione zostały m.in. takie rejestry i zasoby danych jak: Centralna Ewidencja Ludności (rejestr PESEL), dane gromadzone przez Urzędy Stanu Cywilnego, Zakład Ubezpieczeń Społecznych, Krajowy Rejestr Sądowy, REGON, Krajowy Rejestr Karny, Nowa Księga Wieczysta, Rejestr Zastawów, zasoby danych gromadzonych przez Głównego Inspektora Informacji Finansowej), Monitor Sądowy i Gospodarczy, Centralna Ewidencja i Informacja o Działalności Gospodarczej, Krajowa Ewidencja Podatników, Centralna Ewidencja Pojazdów i Centralna Ewidencja Kierowców, zasoby Urzędów Skarbowych i Urzędów Kontroli Skarbowej, System Informacyjny Schengen oraz Wizowy System Informacyjny, bazy danych Służby Celnej. Analiza dotyczyła możliwości wykorzystania dostępnych zasobów danych w zakresie oceny ich przydatności do wykrywania i przeciwdziałania przestępczości finansowej. Zawartość przedstawionych zasobów danych została ograniczona z punktu widzenia obszaru finansowego i własnościowego. Są to rejestry udostępnione przez instytucje odpowiedzialne za ich utrzymanie. Przeprowadzona analiza obejmuje dane, które mogą być wykorzystane do wykrywania i przeciwdziałania przestępczości finansowej (m.in. ich zawartość informacyjna, sposoby przetwarzania, sposoby i tryby dostępu) oraz opis ich faktycznego, aktualnego wykorzystania przez instytucje powołane do ścigania tego rodzaju przestępstw. Wskazano również na ograniczenia związane z dostępem do analizowanych zasobów, w tym elementy bezpieczeństwa związane z ochroną i przetwarzanych danych. Wykonana analiza może pozwolić również w przyszłości na opis i rekomendacje użycia dostępnych modeli dziedzinowych np. ontologii lub modeli obiektowych wykorzystywanych w narzędziach identyfikacji i monitoringu np. operacji finansowych. Modele te będą pomocne w zautomatyzowaniu działań organów zajmujących się ściganiem tego rodzaju przestępstw, a także relacjami dotyczącymi współdziałania w tym zakresie (w tym wzajemną wymianę informacji, nie tylko instytucjonalną wynikającą z regulacji prawnych). Charakterystyka obejmuje analizę zasobów i zbiorów danych, które pozornie nie dotyczą np. stosunków własnościowych, ale mogą stanowić informację wyjściową, to jest taką która umożliwi uzyskanie takich danych (np. identyfikacja osoby). Analiza danych gromadzonych w poszczególnych zbiorach i rejestrach obejmuje m.in. ich zawartość informacyjną (dane bieżące, historyczne), strukturę (atrybuty, szacunkowy procent wypełnienia), dynamikę zmian zawartości (ile jest, ile przybywa/ubywa w czasie), powiązania z innymi

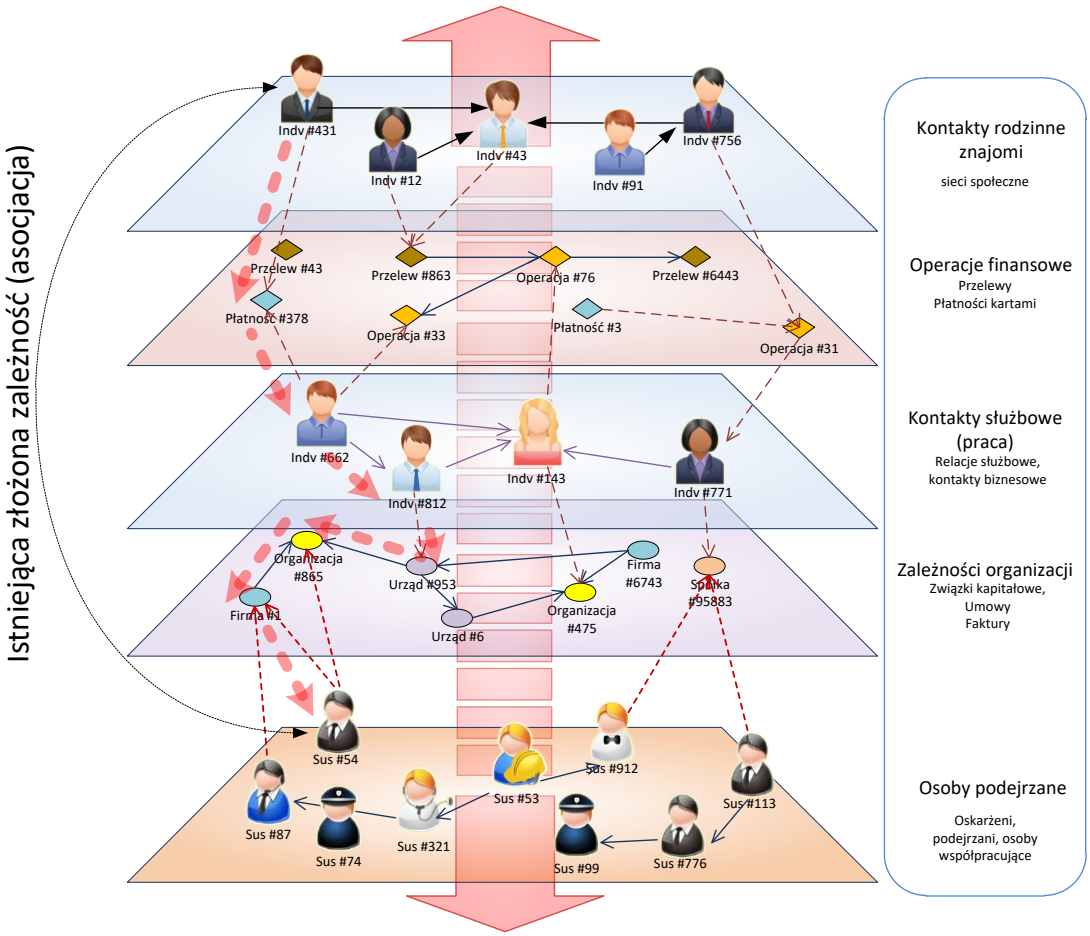
[7] A. Ameljańczyk, *Metryki Minkowskiego w tworzeniu uniwersalnych algorytmów rankingowych*, Biuletyn WAT, Vol. LXIII, Nr 2, str. 324–336, 2014.
A. Ameljańczyk, *Analiza wpływu przyjętej koncepcji modelowania systemu wspomagania decyzji medycznych na sposób generowania ścieżek klinicznych*, Biuletyn Instytutu Systemów Informatycznych, Nr 4, str. 1-6, 2009.
A. Ameljańczyk, *Wielokryterialne mechanizmy wspomagania podejmowania decyzji klinicznych w modelu repozytorium w oparciu o wzorce*, Biuletyn Instytutu Systemów Informatycznych Nr 5, str. 2-8, 2010.
A. Ameljańczyk, *Metoda podziału zbioru obiektów na wielokryterialne klastry jakościowe*, Biuletyn Instytutu Systemów Informatycznych, Nr 12, str. 1–7, 2013.

rejestrami/ewidencjami, sposoby przetwarzania (zarówno centralnie lub lokalnie, jak i elektronicznie lub tradycyjnie/papierowo).

Z kolei w pracy [A_9] przedstawiono propozycję innego spojrzenia na eksploatację istniejących zasobów danych w połączeniu z nowoczesnymi metodami wykorzystywanymi do przetwarzania danych. Współczesne technologie teleinformatyczne umożliwiają efektywne operowanie na ogromnych ilościach danych. Tworzenie dedykowanych modeli analitycznych pozwala na skuteczne przeciwdziałanie i zwalczanie przestępczości, np. przestępstw dokonywanych przeciwko osobom, w tym również zapobieganie maltretowania dzieci. Scharakteryzowano możliwość wykorzystania istniejących od dawna rejestrów i ewidencji danych w celu zapobiegania takim przestępstwom. Operowanie nowoczesnymi metodami i narzędziami IT w połączeniu z dobrze zdefiniowanymi i zintegrowanymi zasobami danych, nie tylko narodowych, pozwala na zwiększenie wykrywalności określonych rodzajów przestępstw bez konieczności angażowania dodatkowych sił i środków. Podane przykłady, pomimo tego że dotyczą zasobów danych w wybranych krajach, mogą znaleźć również zastosowanie w wielu innych miejscach na świecie. Takie podejście jest jak najbardziej uzasadnione również z tego względu, że współczesna działalność przestępcza jest działalnością międzynarodową.

Uszczegółowienie i rozwinięcie zagadnień, które zostały przedstawione w [A_67], [A_68], [A_66], [A_88], [A_9] oraz [A_14] można znaleźć w [B_3], [B_8], [B_10], [B_17], [B_38], [B_39] i [B_60] – głównie w ramach obszarów związanych ze zwalczaniem przestępczości gospodarczej.

Koncepcję wykorzystania uogólnionego modelu danych do tworzenia nowoczesnych narzędzi teleinformatycznych, wspomagających organy i instytucje zwalczające przestępczość gospodarczą, można przedstawić schematycznie jak na rysunku nr 1. Technologia opracowana w ramach projektu IAFEC, opisanego w [P_1], w przejrzysty sposób pokazuje zalety wykorzystania tej koncepcji.




Rysunek nr 1. Zależności pomiędzy podmiotami/osobami.

Koncepcja ta została m.in. scharakteryzowana w monografii [B_3]. Opisany tam, zintegrowany system dostępu i analizy danych rejestrowych i ewidencyjnych jest projektem rozwojowym w zakresie obronności i bezpieczeństwa państwa. Priorytetowym obszarem badań, w którym projekt został złożony, są nowoczesne technologie i innowacyjne rozwiązania w zakresie wykorzystywania danych wrażliwych, wykrywania i przeciwdziałania przestępczości finansowej. Zgodnie z warunkami konkursu projekt dotyczył dziedziny z obszaru obronności i bezpieczeństwa państwa, w tym bowiem obszarze sytuuje się zjawisko, jakim jest przestępczość finansowa. Przestępczość finansowa, rozumiana często jako przestępczość gospodarcza, nazywana również przestępczością „białych kołnierzyków", jest zjawiskiem wielowymiarowym, a jednym z tych wymiarów jest aspekt bezpieczeństwa państwa. Zapewnienie bezpieczeństwa w kontekście militarnym oraz pozamilitarnym jest fundamentalnym zadaniem państwa. W ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu czytamy, że do zadań ABW należy: rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa. Zgodnie z ustawą zadaniem ABW jest rozpoznawanie, zapobieganie i wykrywanie przestępstw godzących w podstawy ekonomiczne państwa. Grzemski i Krześ ()[8] w swojej analizie dotyczącej przestępstw godzących w podstawy ekonomiczne państwa, wymienionych w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, zwracają uwagę na fakt, że ani w ustawie o ABW i AW, ani we wcześniejszej ustawie o Urzędzie Ochrony Państwa nie ma definicji pojęcia „podstawy ekonomiczne państwa". Na ogólniejszym poziomie z pewnością można stwierdzić, że bezpieczeństwo ekonomiczne państwa jest jednym z elementów składających się na bezpieczeństwo narodowe, co wynika z tego, że państwo prowadzi określoną politykę społeczno-gospodarczą. Zapewnienie bezpieczeństwa fundamentalnych interesów ekonomicznych państwa w sposób istotny wpływa na funkcjonowanie państwa jako całości, a także poszczególnych instytucji odpowiedzialnych za redystrybucję dóbr dla obywateli.

W pracy [B_8] przedstawiono narzędzia i metodę przeznaczoną do rozpoznawania i oceny oszustw finansowych w oparciu o strumień danych transakcyjnych pochodzących z instytucji finansowych. Przedstawione nowatorskie podejście ma na celu przetwarzanie danych uwzględniające kontekst, wynikające z zastosowania ontologii i zdolności rozumowania wykorzystujących DL i FOL ()[9]. Terminologia domenowa definiuje podstawowe pojęcia, relacje i reguły klasyfikacji, które zapewniają możliwości przetwarzania semantycznego. W artykule podsumowano zasadność wdrożenia koncepcji zestawu narzędzi do identyfikacji oszustw opartych na zestawie ontologii rozwiązywania problemów. Metody, algorytmy i oprogramowanie są źródłem dla narzędzi analitycznych IAFEC pokazujących analizę powiązań semantycznych. Nowością w tym podejściu jest włączenie heterogenicznej analizy danych, która łączy różne warstwy danych, rozszerzając zakres dostępnych powiązań między osobami, organizacjami i podmiotami rynku finansowego. Obszerne opisy domen zapewniają wiele sposobów wyrażania relacji w rodzinach, grupach społecznych, organizacjach, transakcjach finansowych i innych zależnościach. Postęp w automatycznym analizowaniu i dostępność narzędzi do przetwarzania semantycznego mogą wspierać analityków w rozszerzeniu istniejących metod analizy linków na kontekstowe przetwarzanie wiedzy. Prezentowane badania zapewniają szerzy wgląd w analityczną metodę i algorytmy, które opierają się na logicznym rozumowaniu, identyfikacji i ocenie skojarzeń występujących w transakcjach finansowych uzupełnionych danymi wywiadowczymi.

[8] J. Grzemski, A. Krześ, Analiza pojęcia „*przestępstwa godzące w podstawy ekonomiczne państwa*" w ustawie z dnia 24 maja 2002 r., o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, w: *Przegląd Bezpieczeństwa Wewnętrznego*, Nr 2 (2012), s. 150–153.

[9] F. Baader, D. McGuinness, D. Nardi, P. Patel-Schneider, The Description Logic Handbook: Theory, Implementation, and applications, Cambridge University Press, ISBN 0521876257, 2007.

S. Staab, R. Studer, Handbook on Ontologies, Springer, ISBN 3540408347, 2004.

Opracowana metoda została dostarczana jako samodzielna aplikacja komputerowa zintegrowana z odpowiednimi sterownikami oraz usługami integracji danych (w ramach realizacji zadań wynikających z zakresu projektu opisanego w [P_1]).

Rozwój metod oraz technologii teleinformatycznych, w połączeniu z ewolucją modeli danych, daje zupełnie nowe możliwości ich wykorzystania w różnych obszarach działalności człowieka. W szczególności dotyczy to tych obszarów, które do tej pory były pomijane np. ze względu na ogromną ilość danych oraz brak narzędzi analitycznych, które mogłyby być wykorzystane do ich skutecznego i efektywnego przetwarzania i analizy. Zainteresowanie wykorzystaniem dużych zasobów danych (Data Werhouse, Big Data, noSQL Databases, strumieniowe BD) w dużej mierze sprowadza się do przetwarzania coraz większej ilości danych oraz coraz większych wolumenów danych. To samo dotyczy sieci społecznościowych. Pojawianie się coraz to nowszych rozwiązań w obszarze danych (i informacji) skutkuje na ogół pojawieniem się coraz to nowszych narzędzi teleinformatycznych do ich obsługi. Odnosi się wrażenie, że zapomniano o „starych", dobrze ustrukturalizowanych bazach danych, które były i są przetwarzane w klasyczny sposób. W pracy [B_10] przedstawiono próbę spojrzenia na te „stare" zasoby danych w połączeniu z wykorzystaniem najnowszych technik i metod informatycznych do ich analizy. Prezentowane podejście dotyczy rejestrów, ewidencji tzw. publicznych, które obejmują swoją zawartością całą populację danego kraju (regionu) lub zawierają dane o wszystkich obiektach określonego typu (np. ewidencja nieruchomości). Ich podstawową cechą jest to, że są prowadzone od kilkunastu lub kilkudziesięciu lat (nawet jeżeli w pierwotnej wersji były prowadzone w sposób tradycyjny, czyli papierowy), są publiczne (co nie zawsze oznacza, że każdy może z nich korzystać) i na ogół zarządza nimi administracja rządowa lub publiczna. Niepodważalną zaletą takich klasycznych baz danych jest również to, że zawarte w nich dane są w większości przypadków „wyczyszczone" i zupełne. Prezentowane przykłady dotyczą głównie rejestrów i ewidencji polskich, ale wskazano, że proponowane rozwiązania mogą być także zastosowane w innych krajach, nie tylko europejskich. Przykłady obejmują zagadnienia związane z analizą pozornie nie związanych ze sobą rejestrów i ewidencji i wyszukiwaniem powiązań pomiędzy różnymi osobami (podmiotami), ze szczególnym wskazaniem możliwości wykorzystania tych wyników w przeciwdziałaniu i wykrywaniu działań niezgodnych z prawem, w tym analiz dotyczących przestępstw przeciwko osobom.

Kolejne trzy pozycje [B_38], [B_39] i [B_17] przedstawiają koncepcję systemu IAFEC (*ang. Information Analysis of Financial and Economic Crime*), która powstała jako efekt realizacji pracy naukowo-badawczej zleconej przez Narodowe Centrum Badań i Rozwoju [P_1]. Celem artykułu [B_28] było przedstawienie koncepcji systemu informatycznego wspomagającego zwalczanie przestępczości gospodarczej z uwzględnieniem koniecznych modyfikacji otoczenia organizacyjno-prawnego. Koncepcja systemu IAFEC powstała jako konsekwencja prac prowadzonych w obszarze możliwości wykorzystania różnorodnych zasobów danych do przeciwdziałania przestępczości gospodarczej (głównie w obszarze finansów). Wielkość tych zasobów oraz ich zmienność powoduje, że dotychczas wykorzystywane narzędzia i metody służące do szeroko rozumianej analizy danych okazują się zbyt proste oraz nie spełniają założonych oczekiwań. Przedstawione propozycje wskazują inne sposoby zastosowania znanych metod, jak również dotyczą wykorzystania innych, dotychczas nie wykorzystywanych lub wykorzystywanych w niewielkim stopniu, metod i technik prowadzenia analiz w obszarze tak rozległych zasobów danych. Zwrócono również uwagę na uwarunkowania formalno-prawne, które w wielu sytuacjach tworzą daleko idące ograniczenia i uniemożliwiają przeprowadzenie skutecznych analiz i wynikających z nich działań prewencyjnych. W pracy przedstawione zostały podstawowe zagadnienia związane z koncepcją projektowanego systemu, traktowanego jako zbiór narzędzi służących do wykrywania i przeciwdziałania niekorzystnym zjawiskom gospodarczym. Natomiast celem artykułu [B_39] było zaprezentowanie nowoczesnej architektury oraz koncepcji systemu wspomagającego analizę danych w oparciu o heterogeniczne zasoby, a także wykorzystującej podejście usługowe typu SOA (ang. Service Oriented Architecture) dla różnorodnych metod analizy

danych bazujące na zróżnicowanych metodach i algorytmach analizy (metody analizy grafowo-sieciowej poszukiwania dróg w homogenicznych i wielowarstwowych grafach) na potrzeby wspomagania zwalczania przestępczości gospodarczej. Zaproponowana architektura przedstawiona została z punktu widzenia roli „Analityka", który odpowiada za przygotowanie danych do analizy, przeprowadzenie tej analizy oraz przedstawienie jej wyników do dalszego procedowania. Wielkość proponowanych do wykorzystania zasobów danych oraz ich zmienność powoduje, że dotychczas wykorzystywane narzędzia i metody służące do analizy danych okazują się niewystarczające. Z punktu widzenia decydentów, możliwość uzyskania informacji opartej na przeanalizowaniu wszystkich możliwych przesłanek określonych działań daje możliwość podjęcia zdecydowanie lepszych jakościowo decyzji co do dalszego postepowania (zmniejsza się ryzyko podjęcia decyzji błędnych). Zarówno w trakcie opracowywania koncepcji [B_38], jak i architektury systemu [B_39], jednym z przyjętych założeń była chęć uzyskania satysfakcjonujących wyników badań jeszcze przed „zmaterializowaniem się" przestępstwa finansowego, tak aby można było zminimalizować lub wręcz wyeliminować potencjalne (negatywne) skutki tego przedsięwzięcia. Uzupełnieniem tych dwóch artykułów jest praca [B_17], która przedstawia opracowane i zaimplementowane elementy systemu wykrywania i przeciwdziałania przestępstwom finansowym – IAFEC. Powstały na podstawie koncepcji system IAFEC wykorzystuje również do analizy bazy danych modelu sieciowego. W artykule przedstawiono ogólną architekturę systemu oraz jego zasoby informacyjne wraz z metodą pozyskiwania danych dla przyjętego modelu danych. Każdego roku, państwo odnotowuje coraz wyższe straty w budżecie wynikające z przestępstw finansowych, a w szczególności z „prania brudnych pieniędzy". Funkcjonujący w Polsce model wykrywania i przeciwdziałania takiej działalności ma charakter rozproszony, gdyż opiera się na działaniach wielu niezależnych organów i instytucji. Ponadto, rozwój technologii utrudnia skuteczne wykrywanie przestępczości finansowej, a stosowane dotychczas metody opierają się na analizie manualnej. Szansę na zwiększenie skuteczności wykrywania prania pieniędzy stanowi automatyzacja procesów pozyskiwania danych oraz ich analizy. Przedstawiony problem stał się podstawą podjęcia prac, a w konsekwencji opracowania systemu IAFEC, przeznaczonego do analizy danych pod kątem wykrywania i przeciwdziałania przestępstwom finansowym.

Powyższe opracowania musiały mieć oparcie w szeroko rozumianym otoczeniu prawnym. Jego analiza została przedstawiona m.in. w [B_60]. Ostatnie lata spowodowały znaczący wzrost przestępstw gospodarczych powiązanych z wykorzystaniem nowoczesnych technologii teleinformatycznych. Z drugiej strony, ta sama technologia pozwala również na efektywniejsze zwalczanie tej przestępczości, w szczególności przestępczości gospodarczej związanej z praniem pieniędzy. Konsekwencjami tego rozwoju są także zmiany i poszerzenie regulacji prawnych dotyczących zagadnień przestępstw gospodarczych oraz wykorzystania narzędzi i metod informatycznych w ich zwalczaniu. W szczególności, znaczącej zmianie uległy regulacje prawne związane z ochroną informacji i zbiorów danych, m.in. w obszarze tajemnicy bankowej, tajemnicy skarbowej, tajemnicy podatkowej, tajemnicy telekomunikacyjnej oraz ochrony danych osobowych. W książce [B_60] przedstawiono podstawowe zagadnienia związane z możliwością przetwarzania danych z tego obszaru. Scharakteryzowany zakres zbieranych i przetwarzanych danych został zestawiony z możliwościami i koniecznością ich udostępniania. Szczególny nacisk został położony udostępnianie danych organom odpowiedzialnym za przeciwdziałanie i wykrywanie przestępstw gospodarczych związanych z praniem pieniędzy. Dużą uwagę zwrócono na ograniczenia prawne wynikające z konieczności przestrzegania tajemnic (m.in. tajemnicy bankowej, skarbowej, celnej, doradcy podatkowego, telekomunikacyjnej, ubezpieczeniowej, lekarskiej, statystycznej, korespondencji oraz tajemnic służbowych i zawodowych). Przedstawiona analiza związana jest przede wszystkim z możliwościami samego udostępniania, jak również z możliwym zakresem przetwarzanych i udostępnianych danych. Przedstawione przykłady wskazują, że – zgodnie z obowiązującym prawem – można w znakomity sposób powiązać rozwiązania informatyczne z dostępem do odpowiednich baz danych i w efektywny sposób zwalczać przestępczość

gospodarczą. Siłą rzeczy, zaprezentowane przykłady zostały zanonimizowane i zawężone do podstawowych faktów przydatnych w tego typu analizie. W ostatniej części zwrócono uwagę na konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa przy przetwarzaniu i udostępnianiu danych związanych z przestępczością finansową.

Jednym z nowatorskich zastosowań technologii, mającym wykazać możliwość wykorzystania technologii RFID do bezpiecznego przetwarzania dokumentów (i innych nośników) zawierających informacje wrażliwe, było wykonanie projektu pt.: „Elektroniczny system zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości", które charakterystyka znajduje się w [P_2]. Celem głównym projektu było „Opracowanie innowacyjnego systemu czytników i obsługi informatycznej", w ramach priorytetowego obszaru badawczego „Nowoczesne technologie innowacyjne i rozwiązania w zakresie wykrywania, zwalczania i neutralizacji zagrożeń". W ramach realizacji tego celu został opracowany system oznaczania nośników elektronicznych i dokumentów papierowych identyfikatorami RFID oraz zaprojektowano lub rozwinięto odpowiednie urządzenia, które służyły realizacji tego zadania. Efektem końcowym realizacji projektu jest prototyp nowoczesnej kancelarii tajnej, w której wykorzystywane są najnowsze osiągnięcia z zakresu technologii RFID oraz dostosowany do tej technologii sposób funkcjonowania i zarządzania kancelarią, dający możliwość pracy z dokumentami posiadającymi różne poziomy wrażliwości.

W ramach realizacji projektu opracowano model zunifikowanych procesów zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości. Przed wykonaniem i wdrożeniem systemu, zgodnie z wymaganiami Gestora, procesy nietypowe wymagające niestandardowej obsługi wymagały dodatkowego zdefiniowania. Cel główny projektu został osiągnięty etapowo, poprzez realizację poszczególnych celów szczegółowych. Opracowanie nowoczesnego systemu oznaczania nośników elektronicznych i dokumentów papierowych identyfikatorami RFID oraz zaprojektowanie lub rozwinięcie odpowiednich urządzeń do realizacji tego zadania, wymagało realizacji następujących celów szczegółowych: (1) opracowanie systemu zdalnej identyfikacji nośników jawnych i niejawnych oznakowanych etykietami do odczytu radiowego w miejscach składowania i pracy w czasie rzeczywistym; (2) opracowanie systemu automatycznej inwentaryzacji dokumentów jawnych i niejawnych ułożonych w stosach i zawartych w segregatorach wraz z automatycznym wykryciem zmiany ich położenia; (3) opracowanie systemu kontroli przepływu nośników i dokumentów jawnych i niejawnych pomiędzy strefami bezpieczeństwa wraz z modułem kontroli uprawnień osób do dokumentu jawnego i niejawnego; (4) opracowanie systemu elektronicznego zabezpieczenia nośników i dokumentów przed nieuprawnionym przemieszczeniem; (5) automatyczna identyfikacja nośników oraz dokumentów nie tylko w obszarze składowania, ale również na stanowiskach pracy; (6) opracowanie technologii zabezpieczeń przed wielokrotnym kopiowaniem dokumentu jawnego i niejawnego; (7) opracowanie metody operacji drukowania dokumentu jawnego i niejawnego z ograniczoną ilością egzemplarzy oraz (8) identyfikacja położenia pojedynczego dokumentu jawnego i niejawnego z dokładnością do ustalonego położenia teczki lub woluminu.

Spis tytułów publikacji podstawowych i uzupełniających wykorzystanych w prezentowanym zagadnieniu znajduje się poniżej. Szczegóły publikacji znajdują się wykazie opublikowanych prac naukowych.

[A_9] *Application possibilities of Advanced Analysis of Public Data Sources in the Fight Against Child Maltreatment.*

[A_14] *Multicriteria Methods for Identifying Patterns in the Analysis of the Flow of "Dangerous Financial Documents".*

[A_66] *Use of biometric data in identification documents.*

[A_67] *Location with the use of the RFID and GPS technologies - opportunities and threats.*

[A_68] *Objects identification in the information models used by information systems.*

[A_88] *Rejestry i zasoby informacyjne wykorzystywane przez organy odpowiedzialne za wykrywanie*

*i przeciwdziałanie przestępczości.*

[P_1] *Projekt IAFEC.*

[P_2] *Projekt RFID.*

[B_3] *Zintegrowany system dostępu i analizy danych rejestrowych i ewidencyjnych* –w przygotowaniu

[B_8] *Financial fraud recognition and identification method using reasoning and quantitative association evaluation.*

[B_10] *Przestrzenne uwarunkowania wykorzystania zaawansowanej analizy danych w przeciwdziałaniu przestępczości.*

[B_17] *Wykrywanie i przeciwdziałanie przestępstwom finansowym z wykorzystaniem sieciowych baz danych - system IAFEC.*

[B_38] *Koncepcja systemu informatycznego wspomagającego zwalczanie przestępczości gospodarczej na przykładzie systemu IAFEC.*

[B_39] *Architektura systemu informatycznego wspomagającego zwalczanie przestępczości gospodarczej na przykładzie systemu IAFEC.*

[B_60] *Gromadzenie i przetwarzanie danych mających związek ze zwalczaniem przestępczości finansowej: Zasady dostępu, ograniczenia prawne*.

## Podsumowanie

Rozwój technologii teleinformatycznych zmusza do adekwatnych zmian w sposobie postrzegania ich wpływu na teraźniejszość i przyszłość. Zagadnienia przedstawione we wskazanych powyżej publikacjach pozwalają przyjąć założenie, że stanowią one istotny wkład w rozwój dyscypliny, jaką jest informatyka, w szczególności w postrzeganie danych i informacji jako podstawowych jej elementów.

Przedstawione publikacje, dotyczące zarówno rozważań teoretycznych, jak i pokazujące możliwość praktycznego zastosowania wyników prowadzonych badań, jednoznacznie wskazują, że rozwój dyscypliny informatyka (w ramach dziedziny nauk technicznych) nie jest możliwy bez uwzględnienia zmienności otoczenia, które z kolei jest odzwierciedleniem zagadnień wchodzących w skład innych dyscyplin (a często też i dziedzin). Te zależności są coraz bardziej złożone. Im większe obszary działalności człowieka podlegają wpływom nowych technologii, tym większa ich część staje się obszarem funkcjonowania dyscypliny „informatyka". Habilitant w przedstawionych do oceny pracach dokonał próby wskazania zależności oraz wzajemnego wpływu pomiędzy otoczeniem definiującym to „**jakie informacje będą potrzebne**" a środowiskiem, w którym podejmuje się decyzje o tym „**jakie dane będą przetwarzane**" aby te informacje były dostępne. W swoich pracach pokazał również praktyczne rozwiązania powiązane z opracowaniem i wykorzystaniem technologii teleinformatycznych, które w znakomitym stopniu ułatwiają uwzględnienie tych zależności. Należy podkreślić, że przedstawione rozważania każdorazowo uwzględniają **konieczność zachowania bezpieczeństwa** danych/informacji i **muszą uwzględniać uwarunkowania prawne**.

Wyniki uzyskane w trakcie wielu lat prac naukowo-badawczych, dotyczące prezentowanych zagadnień, podzielonych na trzy grupy tematyczne:

- uogólniony i dziedzinowe modele danych w odniesieniu do repozytoriów i rejestrów administracji publicznej; zasoby informacyjne administracji publicznej;
- wybrane aspekty bezpieczeństwa w przetwarzaniu zasobów informacyjnych administracji publicznej; podejście zorientowane procesowo i oparte na analizie ryzyka;
- wykorzystania zaproponowanych modeli do zwalczenia przestępstw gospodarczych i finansowych; uwarunkowania legislacyjne;

wskazują na możliwość postrzegania pewnych zjawisk w szerszej perspektywie, niejednokrotnie wbrew pierwotnym założeniom wynikającym z ograniczeń narzędziowych. Wykorzystanie przez habilitanta zaawansowanych modeli matematycznych taką możliwość pokazało. Również przedstawiając wybrane aspekty bezpieczeństwa w przetwarzaniu zasobów informacyjnych administracji publicznej habilitant wskazał, że analiza zasobów danych (zarówno ilościowa, jak i jakościowa) może być prowadzona w oparciu o heterogeniczne źródła danych, ale mające zbliżoną semantykę.

Analiza dostępnej literatury pokazała, że brak jest pozycji obejmujących swoim zakresem tak zróżnicowane obszary. Dostępne publikacje krajowe i międzynarodowe odnoszą się jedynie do wybranych pojedynczych elementów opisanych w niniejszym autoreferacie. Powoływane źródła i odwołania wskazują, że przedstawiony zakres publikacji w znaczącym stopniu może przyczynić się do szerszego spojrzenia na poruszane zagadnienia i w wyraźnym stopniu przyczynić się do powiększenia dorobku w ramach dyscypliny informatyka w dziedzinie nauk technicznych.

Omówienie pozostałych osiągnięć naukowo - badawczych.

| **Zakres tematyczny** | liczba | razem |
|---|---|---|
| Grupa „A" – publikacje obejmujące wskazane osiągnięcie naukowe (w tym 2 raporty z realizacji projektu) | **17** (+2) | |
| Grupa „B" – publikacje uzupełniające dorobek w zakresie osiągnięcia naukowego | 31 | |
| Grupa „C" – pozostałe publikacje | 68 | 116+2 |
| **Rodzaj publikacji** | | |
| Monografie | 5 | |
| Artykuły w czasopismach | 49 | |
| Rozdziały w monografiach | 44 | |
| Redakcja naukowa monografii | 7 (+2) | |
| Publikowane materiały konferencyjne | 11 | 116+2 |
| **Autorstwo** | | |
| Autor (samodzielnie) | **37** | |
| Współautor (dwóch autorów) | 28 | |
| Współautor (trzech autorów) | 22 | |
| Współautor (czterech autorów i więcej) | 29 (+2) | 116+2 |

Tabela 2. Sumaryczne dane dotyczące liczby publikacji w okresie od roku 2000.

Habilitant brał udział w realizacji **8 projektów naukowo-badawczych**, z czego **w dwóch pełnił funkcję Kierownika Projektu**. Dwa z tych projektów obejmowały współpracę z zagranicznymi ośrodkami naukowymi, jeden z nich obejmował współpracę z ośrodkami naukowymi ze Stanów Zjednoczonych, a drugi dotyczył współpracy w ramach Unii Europejskiej.

Habilitant uczestniczył w **17 zagranicznych** (ew. międzynarodowych) konferencjach naukowych, na których występował **42 razy w roli prelegenta** (lub współprowadzącego prelekcję). Tematyka wystąpień była ściśle powiązana z tematyką publikacji wskazanych jako osiągnięcie naukowe, część z tych wystąpień było później opublikowane w czasopismach lub materiałach konferencyjnych. Ponadto uczestniczył w **29 krajowych** konferencjach naukowych, gdzie występował w roli prelegenta **36 razy**. Aktywnie uczestniczył w seminariach tematycznych w zakresie popularyzacji nauki.

Aktywny udział w konferencjach naukowych polegał m.in. na **prowadzeniu 7 sesji** tematycznych (specjalnych) **na 4 konferencjach międzynarodowych** oraz jednej krajowej. Habilitant **był członkiem Komitetów Naukowych lub Sterujących na 6 konferencjach międzynarodowych**. Był również członkiem Komitetu Organizacyjnego konferencji krajowej. Brał udział w 5 konsorcjach (głównie w celu realizacji projektów naukowo-badawczych).

Był promotorem około **150 prac dyplomowych** (na studiach podyplomowych – 5, jednolitych – 47, pierwszego i drugiego stopnia – 93). Sprawował opiekę naukową nad studentami indywidualnymi. Wykonał szereg ekspertyz i opracowań na zamówienie z obszaru obejmującego wskazane osiągnięcie naukowe (obejmujących m.in. recenzje projektów naukowo-badawczych). Brał i bierze udział w zespołach eksperckich z tego zakresu.

Habilitant otrzymał wiele medali i odznaczeń, w tym „Medal Komisji Edukacji Narodowej", przyznawany przez Ministra Edukacji Narodowej.

Należy również zauważyć, że habilitant – oprócz pracy we wskazanych jednostkach naukowych – pracował także w jednostkach administracji publicznej oraz w przedsiębiorstwach komercyjnych. Zatrudnienie i praca w tych podmiotach było bardzo dobrym przykładem powiązania koncepcji i rozwiązań powstających w ramach prac naukowo-badawczych a rzeczywistym wykorzystaniem ich efektów w tworzeniu systemów informatycznych mających funkcjonować w praktyce. Przykłady systemów, które zostały zaprojektowane i wdrożone w różnych obszarach funkcjonowania człowieka, dobitnie wskazują na właściwy kierunek i rozwój osiągnięć naukowych, które są przedmiotem niniejszego referatu. Z drugiej strony, praktyczne doświadczenie habilitanta było pomocne w opracowaniu zagadnień opisanych w prezentowanych publikacjach.

Doświadczenie habilitanta wynika m.in. z pracy w takich instytucjach, jak:

1. PKO BP, w latach 1991-2001. Analityk danych. Systemy klasy ERP na potrzeby sprawozdawczości zarządczej.
2. Ministerstwo Sprawiedliwości, 2003-2005. Realizacja oraz nadzór nad projektami systemów wykorzystywanych w resorcie sprawiedliwości. W tym: systemy rejestrowe (Krajowy Rejestr Sądowy, Rejestr Zastawów, Elektroniczna Księga Wieczysta), systemy wspomagające pracę sądów, System Informatyczny Prokuratur, projekty związane z wykorzystaniem środków pomocowych (m.in. PHARE, Transition Facility, SIS II VIS).
3. Ministerstwo Spraw Wewnętrznych i Administracji, 2005-2008. Realizacja oraz nadzór nad projektami systemów rejestrowych eksploatowanych w MSWiA (System PESEL, Ogólnopolska Ewidencja Wydanych i Utraconych Dowodów Osobistych, Centralna Ewidencja Wydanych i Unieważnionych Paszportów). Nadzór i realizacja projektów związanych z wprowadzeniem danych biometrycznych do paszportów i dokumentów podróży dla cudzoziemców. Przygotowanie projektu nowego, biometrycznego dowodu osobistego. Koncepcja i implementacja system nowego paszportu biometrycznego – wdrożenie systemu wraz z rozpoczęciem wydawania paszportów biometrycznych.
4. Redakcja „Polityki", 1994-2004; projekt, implementacja, wdrożenie i utrzymanie systemu rozliczeń finansowych i prenumeraty.
5. „Office Depot", 1998-2002, projekt, implementacja, wdrożenie i utrzymanie systemu do obsługi sieci sklepów.
6. Spółdzielnia Mieszkaniowa "STROP", 1991-1994. Projektowanie i programowanie aplikacji finansowych oraz rozliczania kredytów mieszkaniowych.

Zadania realizowane w ramach pracy we wskazanych instytucjach, były ściśle powiązane z zakresem prac badawczo-rozwojowych prowadzonych przez habilitanta. Pozwalały w sposób twórczy i innowacyjny powiązać wyniki teoretyczne w praktyką. Dawały możliwość, z jednej strony – weryfikacji założeń, przyjętych w trakcie rozważań teoretycznych, w praktycznej realizacji zadań, z drugiej zaś – wykorzystania doświadczeń, zdobytych w trakcie realizacji projektów informatycznych, w dalszym rozwoju prowadzonych prac teoretycznych.

Szczegóły dotyczące wskazanych w tym punkcie pozostałych osiągnięć naukowo-badawczych znajdują się w załączniku „Z.3. Wykaz opublikowanych prac naukowych i osiągnięć …".

……
*Maciej Kiedrowicz*