UNIWERSYTET ŁÓDZKI
WYDZIAŁ ZARZĄDZANIA

Aneta Kaczmarek

Rozprawa doktorska

Kultura organizacyjna a dojrzałość systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych

Promotor: **dr hab. Anna Pamuła, prof. UŁ**
Promotor pomocniczy: **dr inż. Maciej Szmit**

ŁÓDŹ 2024

Spis treści

WPROWADZENIE **5**

1. DOJRZAŁOŚĆ SYSTEMÓW ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI 11

1.1. PODEJŚCIE PROCESOWE, DOJRZAŁOŚĆ PROCESOWA ORAZ DOJRZAŁOŚĆ SYSTEMU ZARZĄDZANIA **11**
1.1.1. Proces, zarządzanie procesowe, orientacja procesowa *11*
1.1.2. Dojrzałość procesowa *13*
1.1.3. Modele dojrzałości procesowej *16*
1.1.4. System zarządzania i ocena jego dojrzałości *23*
1.2. BEZPIECZEŃSTWO INFORMACJI, BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH ORAZ SYSTEMY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI **28**
1.2.1. Bezpieczeństwo informacji *28*
1.2.2. Bezpieczeństwo systemów informatycznych *33*
1.2.3. Systemy zarządzania bezpieczeństwem informacji *39*
1.2.4. Rodzina norm ISO/IEC 27k *45*
1.2.5. Seria NIST SP 800 ..... *49*
1.2.6. Normy BSI *50*
1.2.7. Dobre praktyki biblioteki ITIL *53*
1.2.8. ISACA COBIT 2019 ..... *58*
1.3. OCENA DOJRZAŁOŚCI UKIERUNKOWANA NA ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI – WYBRANE MODELE **62**
1.3.1. COBIT PM *63*
1.3.2. C2M2 ..... *68*
1.3.3. FAM/ISFAM *73*
1.3.4. Porównanie modeli oceny dojrzałości bezpieczeństwa informacji *77*

2. ORGANIZACYJNO-KULTUROWE UWARUNKOWANIA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI **79**

2.1. ORGANIZACJA I ORGANIZOWANIE **79**
2.2. KULTURA ORGANIZACYJNA INSTRUMENTEM ZARZĄDZANIA **86**
2.3. PARADYGMATY BADANIA KULTURY ORGANIZACYJNEJ **88**
2.4. PRÓBY ZDEFINIOWANIA KULTURY ORGANIZACYJNEJ **93**
2.5. FUNKCJE, MODELE, TYPOLOGIE KULTURY **97**
2.6. WYBRANE METODY BADAŃ KULTURY ORGANIZACYJNEJ W PARADYGMATACH FUNKCJONALISTYCZNO-SYSTEMOWYM I INTERPRETATYWNYM **106**
2.6.1. Metoda badań kultury organizacyjnej w paradygmacie funkcjonalistyczno-systemowym *106*
2.6.2. Metoda badań kultury organizacyjnej w paradygmacie interpretatywnym *111*
2.7. KULTURA ORGANIZACYJNA W SEKTORZE PUBLICZNYM **112**

3. METODYKA BADAŃ **116**

3.1. IDENTYFIKACJA LUKI BADAWCZEJ **116**
3.1.1. Przegląd i analiza literatury *116*
3.1.2. Kultura bezpieczeństwa informacji *126*
3.2. CELE I PRZEDMIOT BADAŃ **129**
3.3. SĄDY ADMINISTRACYJNE – ZARYS ZASAD FUNKCJONOWANIA **130**
3.3.1. Historia sądownictwa administracyjnego w Polsce oraz podstawy prawne ich działania *130*
3.3.2. Struktura organizacyjna i kierownictwo wojewódzkich sądów administracyjnych *133*
3.3.3. Regulacje dotyczące Systemów Zarządzania Bezpieczeństwem Informacji w Wojewódzkim Sądzie Administracyjnym *138*
3.4. METODY BADAWCZE **141**
3.4.1. Triangulacja metod, metody mieszane *141*
3.4.2. Plan badań *144*
3.5. PRÓBA BADAWCZA **146**
3.5.1. Próba badawcza – wywiad *146*
3.5.2. Próba badawcza – badanie dokumentów *146*
3.5.3. Próba badawcza – ankieta *146*
3.6. NARZĘDZIA BADAWCZE **148**

3.6.1. Opis narzędzi wykorzystanych w wywiadach 148
3.6.2. Lista kontrolna do analizy formalnej dokumentów oraz opis narzędzia oceniającego dojrzałość systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych 150
3.6.3. Kwestionariusz ankiety 153
3.7. PRZEBIEG BADAŃ 155
3.7.1. Przeprowadzenie wywiadów oraz analiza ich treści 156
3.7.2. Badanie dokumentów 159
3.7.3. Badanie ankietowe 159

4. WYNIKI 160

4.1. WYNIKI BADANIA – WYWIAD 160
4.1.1. Systemy zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych 160
4.1.2. Postrzeganie roli kultury organizacyjnej w organizacji przez kierownictwo sądu 168
4.1.3. Cechy kultury organizacyjnej wojewódzkich sądów związane z dojrzałością systemów zarządzania bezpieczeństwem informacji w sądach 174
4.2. WYNIKI Z ANKIETY REALIZOWANEJ WŚRÓD PRACOWNIKÓW WOJEWÓDZKICH SĄDÓW ADMINISTRACYJNYCH 176
4.2.1. Badanie profilu kultury organizacyjnej 176
4.2.2. Testy statystyczne dotyczące profili kultury organizacyjnej w wojewódzkich sądach administracyjnych 182
4.2.3. Szkolenia i opinie o bezpieczeństwie informacji osób pracujących w wojewódzkich sądach administracyjnych 184
4.2.4. Cechy kultury organizacyjnej wojewódzkich sądów administracyjnych a dojrzałość systemów zarządzania bezpieczeństwem informacji 186
4.3. WYNIKI BADANIA DOKUMENTÓW DOTYCZĄCYCH SYSTEMÓW ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W WOJEWÓDZKICH SĄDACH ADMINISTRACYJNYCH 192
4.4. WYNIKI TRIANGULACJI METOD BADAWCZYCH 193
4.4.1. Identyfikacja dominujących cech kultury organizacyjnej w wojewódzkich sądach administracyjnych – pierwszy cel przeprowadzonych badań 193
4.4.2. Rozpoznanie i analiza istniejącego stanu systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych – drugi cel przeprowadzonych badań 194
4.4.3. Ocena dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych – trzeci cel przeprowadzonego badania 196
4.4.4. Wyodrębnienie cech kultury organizacyjnej mających potencjalny związek z dojrzałością systemów zarządzania bezpieczeństwem informacji – czwarty cel przeprowadzonych badań 199

5. DYSKUSJA 201

6. REKOMENDACJE 204

7. ZAKOŃCZENIE 209

8. BIBLIOGRAFIA 212

ZAŁĄCZNIK 1. KWESTIONARIUSZ WYWIADU 234

ZAŁĄCZNIK 2. BADANIE DOKUMENTÓW DOTYCZĄCYCH SYSTEMÓW ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W WOJEWÓDZKICH SĄDACH ADMINISTRACYJNYCH 235

ZAŁĄCZNIK 3. KWESTIONARIUSZ ANKIETY 238

ZAŁĄCZNIK 4. ZESTAWIENIE DANYCH DOTYCZĄCYCH LICZBY WAŻNYCH CERTYFIKATÓW ISO/IEC 27001:2013 W ROKU 2022 W PORÓWNANIU Z DANYMI Z ROKU 2020 W POSZCZEGÓLNYCH KRAJACH 245

ZAŁĄCZNIK 5. STANDARDY SYSTEMÓW ZARZĄDZANIA MIĘDZYNARODOWEJ ORGANIZACJI NORMALIZACYJNEJ – ISO 250

ZAŁĄCZNIK 6. NARZĘDZIE DO OCENY DOJRZAŁOŚCI SYSTEMÓW ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI 251

ZAŁĄCZNIK 7. WYMIARY KULTURY ORGANIZACYJNEJ POSZCZEGÓLNYCH WOJEWÓDZKICH SĄDÓW ADMINISTRACYJNYCH – KWESTIONARIUSZ OCAI 254

ZAŁĄCZNIK 8. WYMIAR KULTURY ORGANIZACYJNEJ „CHARAKTERYSTYKA ORGANIZACJI” **255**

ZAŁĄCZNIK 9. WYMIAR KULTURY ORGANIZACYJNEJ „CO ZAPEWNIA SPÓJNOŚĆ?” **257**

ZAŁĄCZNIK 10. WYMIAR KULTURY ORGANIZACYJNEJ „NA CO KŁADZIE SIĘ NACISK?” **259**

ZAŁĄCZNIK 11. WYMIAR KULTURY ORGANIZACYJNEJ „KRYTERIA SUKCESU” **261**

SPIS TABEL **263**

SPIS RYSUNKÓW **264**

STRESZCZENIE ROZPRAWY W JĘZYKU POLSKIM **266**

STRESZCZENIE ROZPRAWY W JĘZYKU ANGIELSKIM **269**

Wprowadzenie

Współcześni interesariusze organizacji oczekują zapewnienia bezpieczeństwa jej zasobów informacyjnych, poufności, integralności i dostępności informacji – wymaga to od organizacji transformacji cyfrowej[1]. Incydenty bezpieczeństwa informacji mogą negatywnie wpłynąć na reputację organizacji[2] i spowodować straty finansowe[3]. Aby przeciwdziałać zagrożeniom, organizacje podejmują działania związane z wdrożeniem i utrzymaniem systemów zarządzania bezpieczeństwem informacji (skrót: SZBI), obejmujących zarówno rozwiązania organizacyjne, jak i techniczne[4]. Transformacja cyfrowa to także zaangażowanie członków organizacji we wdrażanie rozwiązań technicznych oraz budowanie kultury pozwalającej na dalszą efektywną i bezpieczną ich eksplorację[5]. Transformacja cyfrowa wpływa nie tylko na przyjęcie nowych rozwiązań, ale również na całą organizację, na jej zarządzanie, procesy, ludzi i kulturę organizacyjną[6]. Zmiany wynikające z wprowadzenia nowych technik cyfrowych powinny być kontrolowane przez zarządzających, tak aby podlegająca przekształceniu

[1] Transformacja cyfrowa – proces głębokich i radykalnych zmian za pośrednictwem technik cyfrowych (m.in. big data, blockchain, przetwarzanie w chmurze, internet rzeczy, sztuczna inteligencja, analityka, rozwiązania kognitywne itp.), które orientują organizację w nowym kierunku i wynoszą ją na zupełnie inny poziom efektywności, która opiera się na analizie danych (tłumaczenie własne), źródło: ISO/IEC TS 30105-9:2023 – 3.4

(ang. *digital transformation* – process of profound and radical change through digital technologies (including big data, blockchain, cloud computing, internet of things, artificial intelligence, analytics, cognitive solutions, etc.) that orients an organization in a new direction and takes it to an entirely different level of effectiveness, which is based on analytics of data).

[2] J.Y. Son,S.S. Kim, *Internet users' information privacy-protective responses: A taxonomy and a nomological model*, „MIS Quarterly" 2009, Vol. 32, No. 3, s. 503–529.

[3] *Cost of a Data Breach Report 2023*, https://www.ibm.com/downloads/cas/E3G5JMBP, dostęp: 1.06.2024 r.; S. Goel,H.A. Shawky, *Estimating the market impact of security breach announcements on firm values*, „Information and Management" 2009, Vol. 46, No. 7, s. 404–410.

[4] „Według Next Move Strategy Consulting globalny rynek cyberbezpieczeństwa w 2022 roku był wyceniony na blisko 222 miliardy dolarów. Prognozuje się, że do 2030 roku rynek ten przekroczy 657 miliardów dolarów" (tłumaczenie własne), źródło: A. Borgeaud, *Cyber security market revenue worldwide 2021–2030*, 8 stycznia 2024, https://www.statista.com/statistics/1256346/worldwide-cyber-security-market-revenues/, dostęp: 2.06.2024 r.

(ang. According to Next Move Strategy Consulting, the global cyber security market was valued at nearly 222 billion U.S. dollars in 2022. By 2030, the market is forecast to exceed 657 billion U.S. dollars).

[5] W. Pasmore, S. Winby, S.A. Mohrman, R. Vanasse, *Reflections: Sociotechnical Systems Design and Organization Change*, „Journal of Change Management" 2019, 19/2, s. 67–85; A. Pollini, C.C. Tiziana, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi, D. Guerri, *Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach*, Cognition, „Technology & Work" 2022, 24, nr 2 s. 371–390.

[6] W. Pasmore, S. Winby, S.A. Mohrman, R. Vanasse, op. cit., s. 67–85; M. Siemiński, K. Krukowski, P. Szamrowski, *Kształtowanie kultury organizacyjnej w administracji publicznej na przykładzie urzędów miast*, Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego, Olsztyn 2014, s. 92.

kultura organizacyjna sprzyjała zachowaniu bezpieczeństwa informacji[7]. Niezależnie od tego, jak zaawansowane rozwiązania techniczne zostaną wdrożone w organizacji w celu zapewnienia bezpieczeństwa informacji, istotne są postawy i działania członków organizacji. Terrence Deal i Allan Kennedy[8] wskazali, że kultura jest najważniejszym czynnikiem decydującym o sukcesie lub porażce organizacji. Shuchih Ernest Chang i Chin-Shien Lin[9] twierdzą, że kultura organizacji jest nośnikiem pomiędzy zarządzaniem a zachowaniem organizacyjnym. Wpływa ona na funkcjonowanie całej organizacji, jak również na skuteczność wdrażanych praktyk dotyczących bezpieczeństwa informacji. Kultura organizacyjna powinna być brana pod uwagę jako ważny czynnik wspierający wdrażanie i utrzymanie na optymalnym dla organizacji poziomie dojrzałości systemu zarządzania bezpieczeństwem informacji[10].

W literaturze światowej, jak i krajowej temat systemów zarządzania bezpieczeństwem informacji w kontekście kultury organizacyjnej był poruszany w ograniczonym zakresie. Zagrożenia związane z wojną konwencjonalną[11], prowadzona wojna w cyberprzestrzeni[12], niestabilność polityczno-społeczna[13] – to przykłady zjawisk, które wystąpiły nie tylko w odległych geograficznie obszarach świata, ale pojawiły się również w Polsce. Zwiększające się ryzyko utraty bezpieczeństwa

[7] M. Tang, T. Li M. Zhang, *The impacts of organizational culture on information security culture: A case study*, „Information Technology and Management" 2016, Vol. 17, s. 179–186; G. Dhillon, G. Torkzadeh, *Value-Focused Assessment of Information System Security in Organizations*, „Information Systems Journal" 2006, Vol. 16 (3), s. 293–314.

[8] T. Deal, A. Kennedy, *Corporate Culture: The Rites and Rituals of Corporate Life*, Addison–Wesley, New York 1982.

[9] S.E. Chang, C.-S. Lin, *Exploring organizational culture for information security management,* „Industrial Management and Data Systems" 2007, Vol. 107, No. 3, s. 438–458.

[10] E. Andrukiewicz, M. Kowalewski, *Praktyczne podejście do wdrażania systemów zarządzania bezpieczeństwem informacji w małych i średnich przedsiębiorstwach*, Studia Ekonomiczne, 2018, Vol. 355, s. 7–20.

[11] Ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. Dz. U. z 2024 r., poz. 507).

[12] Zarządzenie Nr 6 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 22 lutego 2022 r. w sprawie powołania sztabu koordynacyjnego w związku z wprowadzeniem stopnia alarmowego CHARLIE-CRP (Dz. Urz. ABW z 2022 r., poz. 4 z późn. zm.); Raport Departamentu Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów, *Kampania szpiegowska wiązana z rosyjskimi służbami specjalnymi,* źródło: *https://www.gov.pl/web/baza-wiedzy/kampania-szpiegowska-wiazana-z-rosyjskimi-sluzbami-specjalnymi*, dostęp: 14.04.2023 r.

„Zespoły CERT Polska (CSIRT NASK) oraz CSIRT MON zaobserwowały w tym tygodniu szeroko zakrojoną kampanię szkodliwego oprogramowania wymierzoną w polskie instytucje rządowe. Na podstawie wskaźników technicznych i podobieństwa do ataków opisywanych w przeszłości (m.in. na podmioty ukraińskie) można powiązać kampanię ze zbiorem aktywności APT28, który jest kojarzony z Głównym Zarządem Wywiadowczym Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GRU)", źródło: https://cert.pl/posts/2024/05/apt28-kampania/, dostęp: 9.05.2024 r.

[13] M. Bittencourt, R. Gupta, P. Makena, L. Stander, *Socio-political instability and growth dynamics,* „Economic Systems" 2022, Vol. 46(4), 101005.

informacji związane z turbulentnymi czasami, w których działają obecne organizacje, pojawia się nie tylko w organizacjach rynkowych, ale może nawet przede wszystkim w organizacjach z sektora publicznego. Stają się one bowiem celem grup hakerskich, które destabilizują ich działanie lub wręcz uniemożliwiają pełnienie ich funkcji. Zwiększona aktywność cyberprzestępców dotykała również wojewódzkie sądy administracyjne. Wystąpiły próby wykorzystywania luk w zabezpieczeniach systemów informatycznych, jak też braku odpowiednich postaw i zachowań związanych z bezpieczeństwem informacji wśród osób pracujących[14] w sądach. Istotne jest zatem zbadanie poziomu dojrzałości systemów zarządzania bezpieczeństwem informacji biorąc pod uwagę kulturowe uwarunkowania organizacji. Przeprowadzone badanie było badaniem pełnym obejmującym swoim zasięgiem wszystkie wojewódzkie sądy administracyjne (skrót: WSA). Wyniki badania wzbogaciły wiedzę o zarządzaniu bezpieczeństwem informacji i o kulturze organizacyjnej wojewódzkich sądów administracyjnych, tym samym przyczyniły się do rozwoju nauki w tym obszarze. Pomimo że badanie obejmowało swoim zasięgiem wybraną grupę organizacji sektora publicznego, można przypuszczać, że istnieje możliwość odniesienia uzyskanych wyników na pozostałe organizacje wymiaru sprawiedliwości lub szerzej na organizacje sektora publicznego.

Głównym celem dysertacji uczyniono zdiagnozowanie dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych z uwzględnieniem kontekstu kultury organizacyjnej. Oczekiwania interesariuszy i zmieniające się otoczenie zewnętrzne organizacji sektora publicznego wymusiły na nich przeprowadzenie transformacji cyfrowych oraz wdrożenie systemów zarządzania bezpieczeństwem przetwarzanych informacji. W niniejszej pracy została podjęta próba odpowiedzi na następujące pytania badawcze:

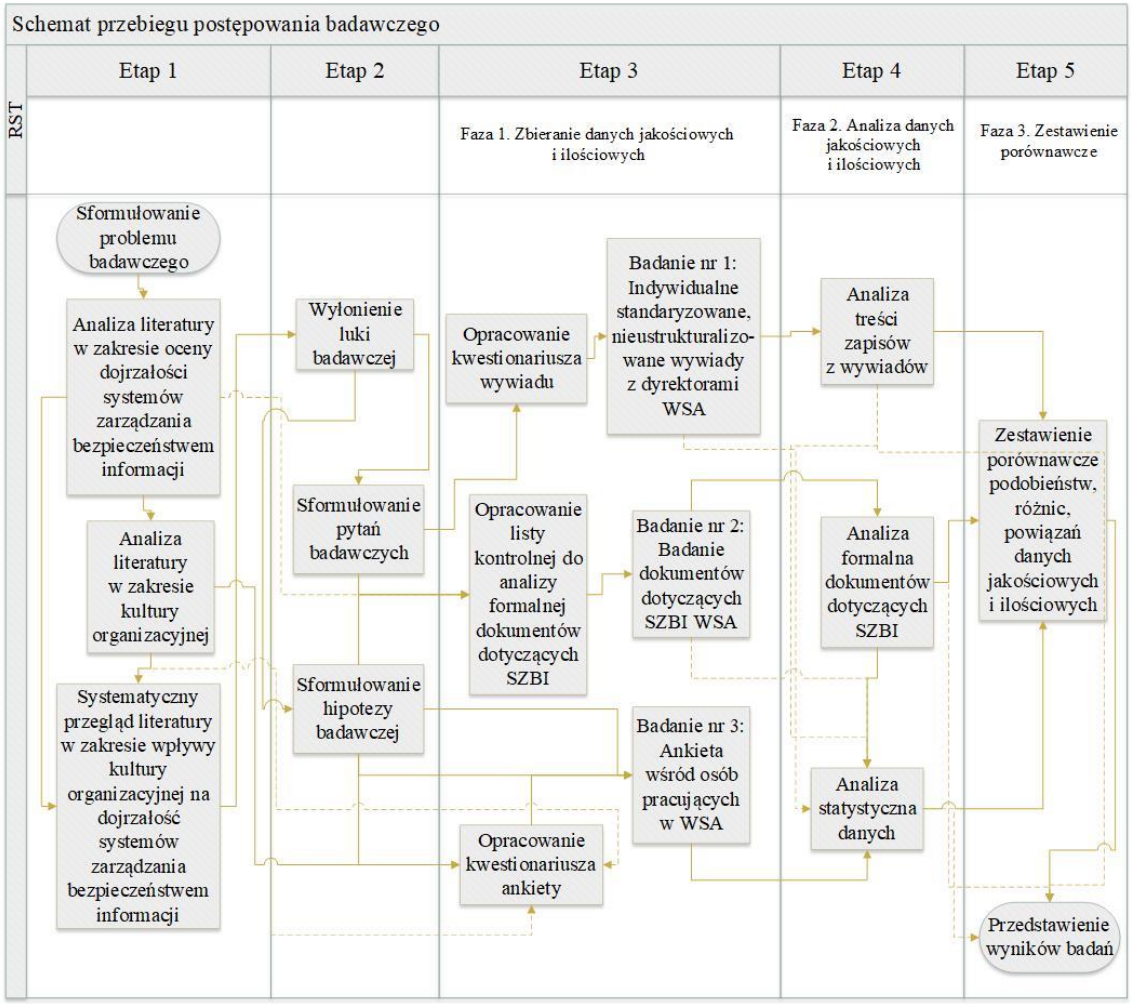
1. Jaki jest poziom dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych?
2. Jaki jest w ocenie pracowników dominujący profil kultury organizacyjnej w wojewódzkich sądach administracyjnych?
3. Czy istnieją cechy kultury organizacyjnej mające potencjalny związek z dojrzałością systemów zarządzania bezpieczeństwem informacji?

[14] J. Abulencia, *Insider attacks: Human-factors attacks and mitigation*, „Computer Fraud and Security" 2021, (5), s. 14 – 17.

Sformułowane powyżej problemy badawcze wpłynęły na zastosowanie badań o charakterze deskryptywnym i eksploracyjnym[15]. W pracy wykorzystywane były następujące metody badawcze[16]:

- analiza literatury krajowej i zagranicznej przedmiotu badań,
- badanie dokumentów,
- sondaż diagnostyczny (ankieta, wywiad standaryzowany nieustrukturalizowany[17]).

Zaplanowane zostało pięcioetapowe postępowanie badawcze, aby osiągnąć cel pracy (Rysunek 0.1).



Rysunek 0.1. Schemat przebiegu postępowania badawczego
RST-równoległa strategia triangulacyjna, źródło: opracowanie własne.

[15] J. Apanowicz, *Metodologia ogólna*, Wydawnictwo Diecezji Pelplińskiej „BERNARDINUM", Gdańsk 2002, s. 35.

[16] J. Niemczyk, *Metodologia nauk o zarządzaniu*, [w:] *Podstawy metodologii badań w naukach o zarządzaniu*, (red.) W. Czakon, Wolters Kluwer, Warszawa 2015, s. 24.

[17] M. Kostera, P. Krzyworzeka, M. Połeć, *Antropologia organizacji. Jak prowadzić badania terenowe?* Wydawnictwo Naukowe PWN, Warszawa 2023, s. 144–145.

Analiza literatury polskiej i światowej była pierwszym etapem pracy badawczej. Została ona przeprowadzona w trzech obszarach. Pierwszy z nich dotyczył oceny dojrzałości systemów zarządzania bezpieczeństwem informacji. Drugim obszarem była kultura organizacyjna – poznanie metod jej badania w różnych paradygmatach naukowych. W dwóch pierwszych tematach zastosowana została tradycyjna metodyka przeglądu literatury[18]. Trzecim analizowanym zagadnieniem był związek kultury organizacyjnej z dojrzałością systemów zarządzania bezpieczeństwem informacji. Ostatnia analiza została przeprowadzona z zastosowaniem systematycznego przeglądu literatury[19].

Przeprowadzone badanie literatury zaprezentowane w podrozdziale 3.1 pozwoliło na zidentyfikowanie luki badawczej. Zauważono, że problem zależności pomiędzy cechami kultury organizacyjnej a dojrzałością systemów zarządzania bezpieczeństwem informacji stanowi przedmiot zainteresowania badaczy, ale jest analizowany w sposób niewyczerpujący. Luka ta widoczna jest przede wszystkim w literaturze polskiej. Podjętym problemem badawczym w dysertacji było zbadanie tego związku w wojewódzkich sądach administracyjnych. Wyniki pracy mogą przyczynić się do lepszego zrozumienia zjawiska i pomóc w zidentyfikowaniu cech kultury organizacyjnej związanych z dojrzałością systemów zarządzania bezpieczeństwem informacji w organizacjach sektora publicznego. Zaprojektowane w dysertacji narzędzie badawcze do oceny dojrzałości systemów zarządzania bezpieczeństwem informacji (Podrozdział 3.6.2) może posłużyć za wzorzec w badaniach innych organizacji.

Prowadzone badania dotyczyły systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych w kontekście kultury organizacyjnej. Badania realizowane były w latach 2022–2023 wśród osób zaangażowanych we wdrażanie procesów związanych z SZBI (dyrektorzy, inspektorzy ochrony danych, specjaliści IT) oraz pozostałych pracowników sądów.

Prace zostały przeprowadzone w paradygmacie funkcjonalistyczno-systemowym, który według Łukasza Sułkowskiego jest bliski takim subdyscyplinom nauk o zarządzaniu, jak: rachunkowość zarządcza, zarządzanie logistyką czy zarządzanie informacją[20], oraz w paradygmacie interpretatywnym. Zastosowanie metod ilościowych

[18] W. Czekan, *Metodyka systematycznego przeglądu literatury*, [w:] *Podstawy metodologii badań w naukach o zarządzaniu*, (red.) W. Czekan, Wyd. III, Wolters Kluwer, Warszawa 2015.

[19] Ibidem.

[20] Ł. Sułkowski, *Paradygmaty nauk o zarządzaniu*, „Współczesne Zarządzanie" 2013, nr 2, s. 17–26.

i jakościowych pozwoliło na szersze zdiagnozowanie[21] związku pomiędzy kulturą organizacyjną a dojrzałością systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych.

Etap trzeci postępowania pokrywał się z fazą pierwszą zastosowanej równoległej strategii triangulacyjnej (skrót: RST) do osiągnięcia celu badań (Podrozdział 3.2, Podrozdział 3.7). Podczas tego etapu zbierane były dane zarówno jakościowe, jak i ilościowe. Etap 4, pokrywający się z fazą 2 RST, polegał na analizie zebranych danych. Etap 5 przebiegu postępowania badawczego, czyli faza 3 RST, to przedstawienie wyników badań.

W pierwszym rozdziale pracy przedstawione zostały wyniki analizy literatury dotyczącej problemów związanych z oceną dojrzałości systemów zarządzania bezpieczeństwem informacji. W drugim rozdziale zaprezentowane zostały różne perspektywy rozumienia i badania procesów kulturowych, zachodzących w organizacjach. Trzeci rozdział przedstawia metodykę przeprowadzonych badań. Ukazuje on proces identyfikacji luki badawczej i jej uzasadnienie. Prezentuje cele i przedmiot badań oraz opis wojewódzkich sądów administracyjnych – ich historię, strukturę organizacyjną i prawne wymagania dotyczące systemów zarządzania bezpieczeństwem informacji. Czwarty rozdział zawiera wyniki zarówno badań jakościowych, jak i ilościowych. W piątym rozdziale znajduje się omówienie podobieństw i różnic między wynikami dysertacji a pracami innych badaczy. Szósty rozdział przedstawia rekomendacje dotyczące rozwijania kultury bezpieczeństwa informacji w organizacji. Siódmy rozdział stanowi reasumpcję wyników przeprowadzonego postępowania badawczego, próbę oceny uzyskanych rezultatów badań i przedstawienie ich ograniczeń. Ósmym rozdziałem jest wykaz literatury wykorzystanej w dysertacji. Po bibliografii zamieszczone są załączniki, które zawierają m.in. narzędzia badawcze oraz inne materiały wykorzystywane podczas postępowania badawczego.

[21] G. Morgan, *Obrazy organizacji*, PWN, Warszawa 1997.

1. Dojrzałość systemów zarządzania bezpieczeństwem informacji

1.1. Podejście procesowe, dojrzałość procesowa oraz dojrzałość systemu zarządzania

1.1.1. Proces, zarządzanie procesowe, orientacja procesowa

Podejście procesowe (ang. *process approach*) uważane jest obecnie za jedną z podstawowych i najpowszechniej stosowanych orientacji w zarządzaniu organizacją[22]. Jest bazą wielu koncepcji zarządzania, takich jak: lean management, six sigma, knowledge management, oraz podstawą systemów zarządzania jakością – tworzonych zgodnie z wymaganiami norm z rodziny ISO 9000[23] i systemów zarządzania bezpieczeństwem informacji – zgodnych z wymogami normy ISO/IEC 27001[24]. Podejście to skupia się na procesach w organizacji jako podstawowym źródle efektywności, doskonałości operacyjnej i osiągania zamierzonych celów[25]. Stojące w centrum pojęcie procesu (ang. *business process*) definiowane jest przez Michaela Hammera i Jamesa Champy'ego jako zbiór działań wymagający na wejściu wkładu i dający na wyjściu rezultat stanowiący wartość dla interesariusza[26]. W normie PN-EN-ISO 9000:2015-*3.4.1* proces definiowany jest jako: „zbiór działań wzajemnie powiązanych lub wzajemnie oddziałujących, które wykorzystują wejścia procesu do dostarczenia zamierzonego rezultatu"[27]. Tym rezultatem może być dostarczenie wewnętrznemu lub zewnętrznemu interesariuszowi produktu, usługi lub informacji spełniających jego wymagania.

---

[22] S. Nowosielski, *Podejście procesowe w organizacjach*, Wydawnictwo Uniwersytetu Ekonomicznego, Wrocław 2009, s. 11; G. Jokiel, *Podejście procesowe w zarządzaniu – geneza i kierunki rozwoju* koncepcji, [w:] Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 52. Podejście procesowe w organizacjach, Wydawnictwo Uniwersytetu Ekonomicznego, Wrocław 2009, s. 20; P. Grajewski, *Procesowe zarządzanie organizacją*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2012, s. 22.

[23] T. Brzozowski, P. Rogala, *Podejście procesowe według norm ISO serii 9000 − istota i ewolucja*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, nr 470, Wrocław 2017, s. 19; G. Jokiel, op. cit., s. 20.

[24] ISO/IEC 27001:2022 – najnowsze wydanie normy opracowanej przez Międzynarodową Organizację Normalizacyjną (ang. *International Organization for Standardization*, skrót: ISO) oraz przez Międzynarodową Komisję Elektrotechniczną (ang. *International Electrotechnical Commission*, skrót: IEC).

[25] H.A. Reijers, *Business Process Management: The evolution of a discipline*, „Computers in Industry" 2021, Vol. 126, s. 1.

[26] M. Hammer, J. Champy, *Reengineering the Corporation: A Manifesto for Business Revolution*, Harper Collins Publisher, New York 1993, s. 35.

[27] *PN-EN-ISO 9000:2015 Systemy Zarządzania Jakością. Podstawy i terminologia*, PKN, Warszawa.

Koncepcją związaną z podejściem procesowym jest zarządzanie procesowe (ang. *Business Process Management*), które przez Michaela Rosemanna, Tonię de Bruin, Tapia Hueffnera[28] jest postrzegane jako całościowa praktyka zarządzania organizacją wymagająca: zrozumienia i zaangażowania najwyższego kierownictwa, świadomych procesów, dobrze zdefiniowanej odpowiedzialności i kultury otwartej na procesy. Podejście stanowi zbiór metod i technik służących do: identyfikacji, ustalania priorytetów, analizy, doskonalenia i monitorowania procesów występujących w organizacji[29]. Podobnie Marlon Dumas, Marcello La Rosa, Jan Mendling i Hajo A. Reijers uważają zarządzanie procesowe za holistyczną koncepcję: „polegającą na nadzorowaniu sposobu, w jaki praca jest wykonywana w organizacji w celu zapewnienia spójnych wyników i wykorzystania możliwości doskonalenia"[30]. Podkreślają oni, że BPM nie polega na ulepszaniu sposobu wykonywania poszczególnych czynności, ale skupia się na zarządzaniu łańcuchami wydarzeń, działań i decyzji, których wyniki są wartościowe dla organizacji, jak i dla jej interesariuszy.

Wdrożenie zarządzania procesowego może wpłynąć na wzrost elastyczności, zwinności i zdolności reagowania na transformację cyfrową i inne zmiany zachodzące w otoczeniu, a także na poprawę innowacyjności i zaspokojenia potrzeb interesariuszy[31]. Opiera się ono na orientacji procesowej (ang. *Business Process Orientation*), która wychwytuje wzajemne powiązania między kluczowymi procesami biznesowymi a procesami wspomagającymi oraz ich zgodność ze strategiami, celami i polityką organizacji[32]. Orientacja procesowa to pojęcie nadrzędne do zarządzania procesowego i procesu. Jest to konstrukt wielowymiarowy, na który według Markusa Kohlbachera i Stefana Gruenwalda składają się następujące wymiary: projektowanie i dokumentacja procesów, zaangażowanie kierownictwa, ustanowienie właściciela

[28] M. Rosemann, T. de Bruin, T. Hueffner, *A Model for Business Process Management Maturity*, ACIS 2004 Proceedings, 6.

[29] A. Bitkowska, *The relationship between Business Process Management and Knowledge Management – selected aspects from a study of companies in Poland*, „Journal of Entrepreneurship, Management and Innovation" 2020, 16, s. 169–193.

[30] M. Dumas, M. La Rosa, J. Mendling, H.A. Reijers, *Introduction to Business Process Management*, [w:] *Fundamentals of Business Process Management*, (red.) M. Dumas, M. La Rosa, J. Mendling, H.A. Reijers, , Springer, Berlin, Heidelberg 2018, s. 1.

[31] F. Imgrund, M. Fischer, C. Janiesch, A. Winkelmann, *Approaching digitalization with business process management*, Proceedings of the MKWI, 2018, s. 1725–1736; A. Baiyere, H. Salmela, T. Tapanainen, *Digital transformation and the new logics of business process management*, „European Journal of Information Systems" 2020, 29(3), s. 238–259.

[32] T. de Bruin, M. Rosemann, *Towards a Business Process Management Maturity Model*. Proceedings of the 13th European Conference on Information Systems, 2005, s. 521–532; H.A. Reijers, *Business Process Management: The evolution of a discipline*, „Computers in Industry" 2021, Vol. 126, s. 4.

procesu, pomiar wydajności procesu, kultura organizacyjna zgodna z podejściem procesowym, stosowanie zasady ciągłego doskonalenia procesów oraz podporządkowana procesom struktura organizacyjna[33]. Orientacja procesowa to filozofia zarządzania, w której cała organizacja jest ukierunkowana na procesy, a nie tylko na pełnione funkcje czy struktury. W tej orientacji działania organizacji są projektowane wokół głównych procesów, które generują wartość dla interesariuszy. Wszyscy pracownicy są zaangażowani w osiąganie celów procesowych, a ich działania są ukierunkowane na ciągłą poprawę oraz zaspokojenie potrzeb odbiorców wewnątrz organizacji lub poza nią.

Podsumowując, podejście procesowe to ogólna koncepcja analizowania i doskonalenia procesów w organizacji, podczas gdy orientacja procesowa to głębsza filozofia zarządzania, która podkreśla, że cała organizacja powinna być zorientowana na procesy jako kluczowy element tworzenia wartości dla interesariuszy.

1.1.2. Dojrzałość procesowa

Watts S. Humphrey[34], który czerpał z prac Philipa B. Crosbiego[35], jest uważany za twórcę koncepcji dojrzałości procesowej. Zdefiniował ją jako stopień, w jakim procesy są: identyfikowane, zarządzane, mierzone, kontrolowane, jak i skuteczne. Według Markusa Kohlbachera i Hajo A. Reijersa[36] istotne aspekty dojrzałości procesowej obejmują: dokumentację procesu, zaangażowanie kierownictwa, własność procesu, pomiar i monitorowanie procesu oraz metody i techniki ciągłego doskonalenia procesu, a także kulturę i strukturę organizacji. Pokrywają się one z wymiarami orientacji procesowej wymienionymi w podrozdziale 1.1.1.

W naukach o zarządzaniu pojęcie „dojrzałość" występuje często w kontekście dojrzałości procesów występujących w organizacji, jak i w odniesieniu do całej organizacji[37]. Przykłady definicji tego terminu wraz ze wskazaniem ich źródła zaprezentowane są poniżej (Tabela 1.1).

---

[33] M. Kohlbacher, S. Gruenwald, *Process orientation: Conceptualization and measurement*, „Business Process Management Journal" 2011, Vol. 17, No. 2, s. 267–283.

[34] W.S. Humphrey, *Characterizing the software process: A maturity framework*, Carnegie Mellon University/Software Engineering Institute, Pittsburgh 1987, s. 2.

[35] P. B. Crosby, *Quality is free: The Art of Making Quality Certain*, McGraw–Hill, New York 1979.

[36] M. Kohlegger, H.A. Reijers, *The effects of process-oriented organizational design on firm performance*, „Business Process Management Journal" 2013, Vol. 19(2), s. 245–262.

[37] A. Maier, J. Moultrie, P. Clarkson, *Assessing Organizational Capabilities: Reviewing and Guiding the Development of Maturity Grids*, „IEEE Transactions on Engineering Management" 2012, Vol. 59, s. 138–159.

Tabela 1.1. Zestawienie wybranych definicji dojrzałości procesowej organizacji oraz dojrzałości organizacji

Źródło	**Definicje dojrzałości**
P. Grajewski, *Organizacja procesowa*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2016, s. 123.	Dojrzałość procesowa organizacji wyraża się zakresem, w jakim procesy są formalnie: zdefiniowane, zarządzane, elastyczne, mierzone i efektywne.
G. Grela, *Ocena poziomu dojrzałości procesowej organizacji*, „Nierówności Społeczne a Wzrost Gospodarczy" 2009, 35, s. 170.	Dojrzałość procesowa to stopień, w jakim wszystkie zasoby organizacji są optymalnie alokowane w stabilnych i opomiarowanych procesach, które umożliwiają realizację celów strategicznych organizacji.
J. Auksztol, M. Chomuszko, *Modelowanie organizacji procesowej*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 42.	Przez pojęcie organizacji „dojrzałej procesowo" rozumieją taką organizację, której procesy można uznać za dojrzałe z jakościowego punktu widzenia.
T.B. Kalinowski, *Modele oceny dojrzałości procesów*, „Acta Universitatis Lodziensis Folia Oeconomica" 2011, 258, s. 173.	„Dojrzałość" w odniesieniu do procesów jest najczęściej definiowana jako zdolność organizacji oraz realizowanych przez nią procesów do systematycznego dostarczania coraz lepszych rezultatów działalności.
M. Trocki, *Organizacja projektowa. Podstawy, modele, rozwiązania*, PWE, Warszawa 2014, s. 224.	Dojrzałość procesowa jest elementem dojrzałości organizacji i postrzega się ją jako zdolność organizacji do efektywnego zarządzania procesami wspierającymi realizację jej celów.
ISACA[38] Glossary of Terms English-Polish Third edition (2015), http://www.isaca.org/About-ISACA/History/Documents/ISACA-Glossary-English-Polish_mis_Pol_0715.pdf, s. 42, dostęp: 21.12.2019 r.	Dojrzałość – w działalności biznesowej wskazuje stopień rzetelności lub zależności, jaki firma może przypisać procesowi osiągania pożądanych celów lub założeń. (ang. *Maturity – in business, indicates the degree of reliability or dependency that the business can place on a process achieving the desired goals or objectives*)
R. Brajer-Marczak, *Dojrzałość*	Dojrzałość organizacji oznacza osiągnięcie

[38] ISACA (ang. Information Systems Audit and Control Association, pol. Stowarzyszenie Audytu i Kontroli Systemów Informatycznych) – międzynarodowe stowarzyszenie osób zajmujących się zawodowo zagadnieniami dotyczącymi audytu, kontroli, bezpieczeństwa oraz innymi aspektami zarządzania systemami informatycznymi.

Źródło	Definicje dojrzałości
procesowa i dojrzałość projektowa organizacji – analiza porównawcza, „Przedsiębiorczość i Zarządzanie" 2017, 3(II), s. 53.	przez organizację takiego poziomu rozwoju, na którym stosuje ona w sposób systematyczny takie narzędzia i techniki zarządzania, które zwiększają jej skuteczność i efektywność.
M. Paulk, B. Curtis, M B. Chrissis, C. Weber, *Capability Maturity Model for Software, Version 1.1 Book, January 1993 CITATIONS*. Software Engineering Institute, s. 4.	Dojrzałość to specyficzny proces mający na celu wyraźne zdefiniowanie, mierzenie i kontrolowanie ewolucji podmiotu, a także zarządzanie nią.
E.S. Andersen, S.A. Jessen, *Project maturity in organisations*, "International Journal of Project Management" 2003, Volume 21, Issue 6, s. 457.	Dojrzałość definiuje się jako stan, w którym organizacja jest w doskonałej kondycji, by osiągnąć wyznaczone sobie cele.

Źródło: opracowanie własne na podstawie wskazanej w tabeli literatury.

W definicjach dojrzałości, m.in. takich autorów, jak Mateusza Juchniewicza i Michała Hałaczkiewcza, pojawia się termin „zdolność" (ang. *capability*), który często występuje w opracowaniach dotyczących dojrzałości w organizacji. Pojęcia te w swojej pracy porównali Amy van Looy, Manu de Backer i Geert Poels[39]. Zauważyli, że termin „dojrzałość" ukierunkowany jest na organizację, na wszystkie procesy w niej zainicjowane. Uważają, że jest to stopień, w jakim organizacja świadomie i konsekwentnie wdraża procesy zgodnie z celami biznesowymi. Dojrzałość można mierzyć ze względu na: komponenty procesów biznesowych, zarządzanie procesami biznesowymi, orientację procesową. Zaś pojęcie „zdolność" jest ukierunkowane na pojedynczy proces. Badacze ci stwierdzają, że jest to umiejętność lub kompetencja organizacji do osiągnięcia zamierzonych rezultatów w wyniku realizacji określonego procesu lub obszaru procesu. „Zdolność" wymaga organizacji, która jest wystarczająco dojrzała, aby ją wspierać.

Z przeprowadzonych studiów literaturowych wynika, iż Tomasz Bartosz Kalinowski[40] podjął próbę uporządkowania rozważań na temat dojrzałości procesowej. Zauważył, że może być ona opisywana w jednym z trzech wymiarów:

[39] A. van Looy, M. Backer, G. Poels, *Defining business process maturity*. *A journey towards excellence*, „Total Quality Management" 2011, Vol. 22, s. 1129.

[40] T.B. Kalinowski, *Dojrzałość procesowa a wyniki organizacji*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2018, s. 49.

1. Dojrzałości procesów (ang. *Business Process Mat*urity).
2. Dojrzałości zarządzania procesowego (ang. *Business Process Management Maturity*).
3. Dojrzałości orientacji procesowej (ang. *Business Process Orientation Maturity*).

T. B. Kalinowski w podsumowaniu łączy te trzy wymiary, stwierdzając, że: „Organizacje, które dążą do osiągnięcia wysokiego poziomu dojrzałości procesowej, w istocie dążą do zarządzania procesami i realizacją założeń koncepcji zarządzania procesowego lub orientacji procesowej na wysokim poziomie (mierzonym np. określonymi miarami wyników działalności)”[41]. Organizacja osiąga wysoki poziom dojrzałości, gdy jest w stanie osiągnąć pożądane cele lub założenia. COBIT[42], w swojej definicji, określa dojrzałość[43] jako stopień wiarygodności i niezawodności organizacji, która uzyskuje pewny poziom dojrzałości na uporządkowanej, zdefiniowanej wcześniej skali. W zbiorze dokumentów ITIL[44] dojrzałość[45] jest miarą: niezawodności, wydajności i skuteczności procesu, funkcji, organizacji itp. Najbardziej dojrzałe procesy i funkcje są formalnie dostosowane do celów biznesowych i strategii oraz wspierane przez ramy ciągłego doskonalenia.

1.1.3. Modele dojrzałości procesowej

Między innymi wymóg ciągłego doskonalenia organizacji, którego celem jest poszukiwanie możliwości podniesienia sprawności i skuteczności wykonywanych działań, przyczynił się do powstania modeli dojrzałości. Według Herberta Stachowiaka[46] modele te upraszczają badany obszar działalności organizacji, wskazując tylko istotne elementy procesów i zachodzące między nimi relacje, oraz oceniają

[41] Ibidem, s. 53.

[42] COBIT (ang. *Control Objectives for Information and related Technology*, pol. Cele kontrolne w zakresie informacji i technik powiązanych) – opracowane przez ISACA dobre praktyki w zakresie ładu informatycznego.

[43] ang. „Maturity – in business, indicates the degree of reliability or dependency that the business can place on a process achieving the desired goals or objectives”, https://www.isaca.org/resources/glossary#glossi, dostęp: 3.08.2023 r.

[44] ITIL (ang. Information Technology Infrastructure Library) – najlepsze praktyki związane procesowym zarządzaniem usługami IT, początkowo opracowywane przez agencję Central Computers and Telecommunications Agency (CCTA), która w późniejszym czasie stała się częścią biura UK Office of Government Commerce (OGC, ang. Office of Government Commerce).

[45] ang. „Maturity – A measure of the reliability, efficiency and effectiveness of a process, function, organization etc. The most mature processes and functions are formally aligned to business objectives and strategy, and are supported by a framework for continual improvement”, https://www.axelos.com/corporate/media/files/glossaries/itil_2011_glossary_gb-v1-0.pdf, s. 36, dostęp: 3.08.2023 r.

[46] H. Stachowiak, *Allgemeine Modelltheorie*, Springer–Verlag, Wien New York 1973, s. 131–132.

dojrzałość procesową. Podobnie Renata Brajer-Marczak oraz Alicja Gębczyńska[47] uważają modele dojrzałości za narzędzia doskonalenia i rozwoju organizacji. Ich zdaniem zarówno badają poziom dojrzałości, jak i pozwalają poprawić wyniki poszczególnych procesów, a co za tym idzie – efektywność całej organizacji.

Mark C. Paulk[48], T. Bartosz Kalinowski[49] w swoich pracach wskazują, iż źródłem idei mierzenia dojrzałości procesów była koncepcja kompleksowego zarządzania jakością TQM (ang. *Total Quality Management*)[50]. Pierwsze próby opracowania modeli oceny dojrzałości procesów zostały podjęte przez Philipa Crosby'ego (QMMG – ang. *Quality Management Maturity Grid*)[51] oraz Waltera A. Shewharta i Williama E. Deminga (koncepcja cyklu PDCA – ang. *Plan, Do, Check,* Act). Philip Crosby swoje podejście oparł na pięciu poziomach dojrzałości – od stanu niepewności, w którym to kierownictwo jest zdezorientowane i niezaangażowane w wykorzystywaniu jakości jako narzędzia zarządzania, do stanu pewności, gdzie zarządzanie jakością jest uważane za absolutnie niezbędną część zarządzania przedsiębiorstwem. Powyższe koncepcje były inspiracją dla Wattsa Humphreya[52] do opracowania jednego z pierwszych kompleksowych podejść w zakresie oceny dojrzałości procesów. Większość modeli dojrzałości[53] (również tych dotyczących bezpieczeństwa informacji) wywodzi się od metody opracowanej przez Software Engineering Institute (SEI) Carnegie Mellon University i MITRE Corporation służącej ocenie dojrzałości firm wytwarzających oprogramowanie dla Departamentu Obrony USA. Prace w SEI, zapoczątkowane przez Wattsa Humphreya, trwały od 1986 r. do 1991 r., kiedy to zaprezentowana została

[47] R. Brajer-Marczak, A. Gębczyńska, *Process Maturity Models as Tools for Organisation Improvement and Development*, [w:] *Education Excellence and Innovation Management: A 2025 Vision to Sustain Economic Development during Global Challenges*, (red.) S. Soliman Khalid, International Business Information Management Association (IBIMA), 2020, s. 10260–10269.

[48] M.C. Paulk, *A History of the Capability Maturity Model for Software*, „ASQ Software Quality Professional" 2009, Vol. 12, No. 1, s. 5–6.

[49] T.B. Kalinowski, *Modele oceny dojrzałości procesów*, „Acta Universitatis Lodziensis. Folia Oeconomica" 2011, nr 258, s. 174.

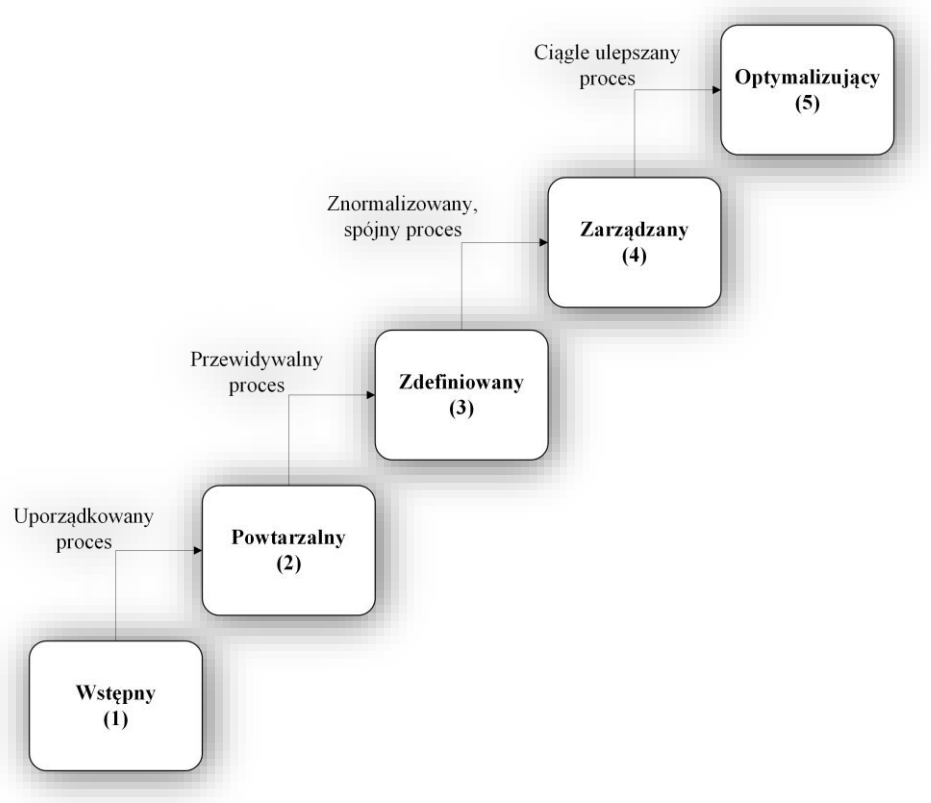
[50] TQM (ang. *Total Quality Management*, pol. kompleksowe zarządzanie przez jakość, kompleksowe zarządzanie jakością, totalne zarządzanie jakością) – według normy ISO 8402:1994 jest to: „sposób zarządzania organizacją skoncentrowany na jakości, oparty na udziale wszystkich członków organizacji i nakierowany na osiągnięcie długotrwałego sukcesu dzięki zadowoleniu klienta oraz korzyściom dla wszystkich członków organizacji i dla społeczeństwa", źródło: J. Penc, *Strategiczny system zarządzania*, Placet, Warszawa 2001, s. 91.

[51] P. Crosby, op. cit.

[52] W.S. Humphrey, *Characterizing the Software Process: A Maturity Framework*, Carnegie Mellon University/Software Engineering Institute, Pittsburgh 1987; W.S. Humphrey, W.L. Sweet, *A method for assessing the software engineering capability of contractors*, Carnegie Mellon University, Software Engineering Institute, Pittsburgh 1987.

[53] A. Kaczmarek, *Wybrane modele dojrzałości zarządzania bezpieczeństwem informacji – analiza porównawcza*, [w:] *Współczesny człowiek wobec wyzwań: szans i zagrożeń w cyberprzestrzeni*, (red.) J. Grubicka, A. Kamińska-Nawrot, Akademia Pomorska w Słupsku, Słupsk 2021, s. 95.

pierwsza wersja koncepcji CMM[54] (ang. *Capability Maturity Model*). Model został zaprojektowany tak, aby pomóc organizacjom programistycznym w wyborze strategii doskonalenia procesu poprzez określenie aktualnej dojrzałości procesu i zidentyfikowanie problemów najbardziej krytycznych dla jakości oprogramowania. Według twórców ciągłe doskonalenie procesu opiera się na wielu małych, ewolucyjnych krokach, a nie na rewolucyjnych zmianach. CMM zapewnia ramy do organizowania tych ewolucyjnych etapów na pięciu poziomach dojrzałości, które stanowią kolejne podstawy ciągłego doskonalenia procesu[55]. Te pięć poziomów dojrzałości definiuje skalę pomiarową dojrzałości procesu tworzenia oprogramowania oraz pomaga organizacji w ustalaniu priorytetów w zakresie doskonalenia – Rysunek 1.1 przedstawia graf z opisaną koncepcją.



Rysunek 1.1. Poziomy dojrzałości według pierwotnej koncepcji CMM.
Źródło: M.C. Paulk, B. Curtis, M.B. Chrissis, C.V. Weber, Capability Maturity Model for Software, version 1.1. CMU/SEI-93-TR-24, Carnegie Mellon University, Software Engineering Institute, Pittsburgh 1993, s. 8.

[54] M.C. Paulk, B. Curtis, M. B. Chrissis, E. L. Averill, J. Bamberger, T. C. Kasse, M. D. Konrad, J. R. Perdue, C.V. Weber, J.V. Withey. *Capability Maturity Model for Software*. CMU/SEI-91-TR-24, Carnegie Mellon University, Software Engineering Institute, Pittsburgh 1991.

[55] M.C. Paulk, B. Curtis, M. B. Chrissis, and C.V. Weber, *Capability Maturity Model for Software, version 1.1. CMU/SEI-93-TR-24*, Pittsburgh: Carnegie Mellon University, Software Engineering Institute, 1993, s. 7.

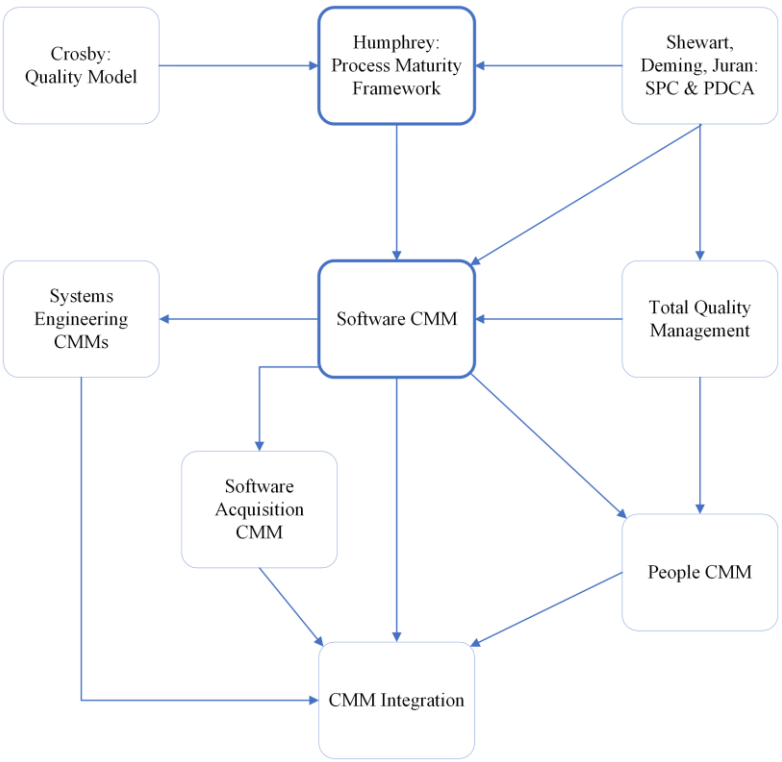
1. „Wstępny (ang. *initial*) – proces tworzenia oprogramowania jest określany *ad hoc,* a czasami nawet chaotycznie. Niewiele procesów jest zdefiniowanych, a sukces zależy od indywidualnego wysiłku.
2. Powtarzalny (ang. *repeatable*) – podstawowe procesy zarządzania projektem są ustalane w celu śledzenia kosztów, harmonogramu i funkcjonalności. Wprowadza się niezbędną dyscyplinę procesu, aby powtórzyć wcześniejsze sukcesy w projektach o podobnych zastosowaniach.
3. Zdefiniowany (ang. *defined*) – proces tworzenia oprogramowania zarówno dla działań zarządczych, jak i inżynieryjnych jest udokumentowany, znormalizowany i zintegrowany ze standardowym procesem tworzenia oprogramowania dla organizacji. Wszystkie projekty wykorzystują zatwierdzoną, dostosowaną do potrzeb wersję standardowego procesu tworzenia oprogramowania organizacji do opracowywania i utrzymywania oprogramowania.
4. Zarządzany (ang. *managed*) – zbierane są szczegółowe miary procesu tworzenia oprogramowania i jakości produktu. Zarówno proces tworzenia oprogramowania, jak i produkty są ilościowo rozumiane i kontrolowane.
5. Optymalizujący (ang. *optimizing*) – ciągłe doskonalenie procesu jest możliwe dzięki ilościowej informacji zwrotnej z procesu oraz pilotowaniu innowacyjnych pomysłów i technologii”[56].

W Carnegie Mellon University na podstawie CMM powstawały modele z innych obszarów zarządzania, m.in.: model do oceny dojrzałości procesów w obszarze pozyskiwania oprogramowania – SA-CMM[57] (ang. *Software Acquisition Capability Maturity Model*) czy model przeznaczony do badania dojrzałości procesów w obszarze zarządzania zasobami ludzkimi – P-CMM[58] (ang. *People Capability Maturity Model*). W 2002 r. postanowiono scalić powstałe modele, tak powstała pierwsza wersja CMMI (ang. *Capability Maturity Model Integration*) –Rysunek 1.2.

[56] M.C. Paulk, B. Curtis, M.B. Chrissis, and C.V. Weber. Capability Maturity Model for Software, version 1.1. CMU/SEI-93-TR-24, Carnegie Mellon University, Software Engineering Institute, Pittsburgh 1993, s. 8–9 (tłumaczenie własne).

[57] J. Cooper, M. Fisher *Software Acquisition Capability Maturity Model (SA-CMM) Version 1.03,* CMU/SEI-2002-TR-010, Carnegie Mellon University, Software Engineering Institute, Pittsburgh 2002, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2002_005_001_14036.pdf (dostęp: 3.08.2023 r.).

[58] B.Curtis, B. Hefley, S. Miller, *People Capability Maturity Model, Version 2 Second Edition*, CMU/SEI-2009-TR-003, Carnegie Mellon University, Software Engineering Institute, Pittsburgh 2009, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2009_005_001_15095.pdf (dostęp: 3.08.2023 r.).



Rysunek 1.2. Genealogia CMM Integration
Źródło: opracowanie własne na podstawie: OMG Document Number: formal/2008-06-01, Business Process Maturity Model (BPMM), https://www.omg.org/spec/BPMM/1.0/PDF, dostęp: 30.03.2021 r.

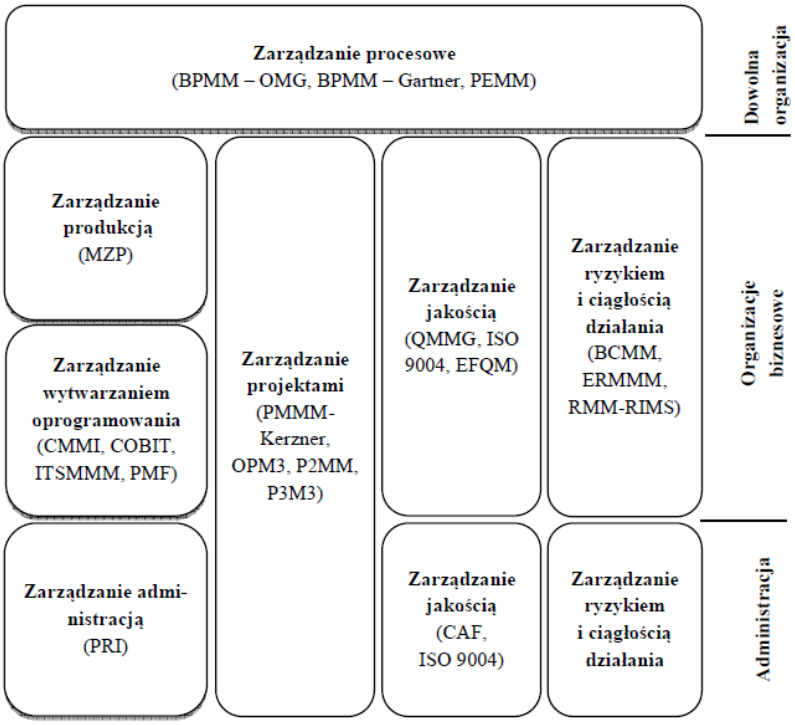
Dalsze prace nad modelem trwały w CMMI Institute, który od 2016 r. znalazł się w strukturach ISACA. Ostatnie wydanie modelu CMMI v3.0 (ang. *Capability Maturity Model Integration*) miało miejsce w kwietniu 2023 r. Osiągnięty sukces spowodował, że zawarte w CMM/CMMI rozwiązania są wymieniane w wielu pracach naukowych, stosowane i ulepszane przez specjalistów[59]. Autorzy artykułu pt. *Analiza porównawcza modeli dojrzałości organizacji*[60] porównali 20 modeli dojrzałości, grupując je w następujące kategorie: zarządzanie procesowe, zarządzanie produkcją, zarządzanie projektami, zarządzanie jakością, zarządzanie ryzykiem i ciągłością działania (Rysunek 1.3). Według badaczy modele, które mogą być wykorzystane przez dowolną organizację w badaniu dojrzałości zarządzania procesowego, to: BPMM – OMG[61] (ang. *Business Process Maturity Model – Object Management Group*), BPMM firmy

[59] T. B. Kalinowski, *Process maturity vs. organisational results*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2017, (463), 173.

[60] J. Smagowicz, A. Kosieradzka, *Analiza porównawcza modeli dojrzałości organizacji*, [w:] *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego*, (red.), M. Ćwiklicki, M. Jabłoński, S. Mazur Stanisław, Fundacja Gospodarki i Administracji Publicznej, Kraków 2016, s. 289.

[61] C. Weber, B. Curtis, T. Gardiner, *Business Process Maturity Model (BPMM)* Version 1.0, 2008, s. 454.

Gartner oraz PEMM. Przeprowadzona analiza wykazała duże podobieństwo modeli pod względem ich budowy oraz wyszczególnionych poziomów dojrzałości. Autorzy przypisują to zjawisko wzorowaniu się przy tworzeniu nowych modeli na wcześniejszych opracowaniach, przy czym osiem badanych rozwiązań wzorowało się bezpośrednio na modelu CMM[62].



Rysunek 1.3. Systematyka badanych modeli dojrzałości
Źródło: J. Smagowicz., A. Kosieradzka, Analiza porównawcza modeli dojrzałości organizacji, [w:] Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego, (red.), M. Ćwiklicki, M. Jabłoński, S. Mazur Stanisław, Fundacja Gospodarki i Administracji Publicznej, Kraków 2016, s. 286.

Mateusz Juchniewicz – w swojej pracy dotyczącej koncepcji doskonalenia organizacji[63] – podaje, iż obecnie na rynku funkcjonuje około 200 modeli dojrzałości w zarządzaniu. Według niego najpopularniejsze modele to: CMMI, BPM Maturity Model, OPM3, The Kerzner PMMM oraz OGC P3M3. Uważa on, że stanowią one obecnie grupę podstawowych narzędzi wdrażania idei ciągłego doskonalenia w organizacjach. W swoim artykule[64], który zawierał wyniki systematycznego przeglądu literatury w temacie modeli dojrzałości procesów biznesowych, badacze

[62] Ibidem, s. 292.
[63] M. Juchniewicz, *Koncepcje doskonalenia organizacji – ewolucja, krytyka, perspektywy rozwoju*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu: Nowe kierunki w zarządzaniu przedsiębiorstwem. Procesy i projekty w zarządzaniu zmianami" 2017 12(463), 2017, s. 34–45.
[64] A. Tarhan, O. Turetken, H. A. Reijers, *Business process maturity models: A systematic literature review*, „Information and Software Technology" 2016, Vol. 75, s. 122–134.

Ayca Tarhan, Oktay Turetken, Hajo A. Reijers uznali 9 modeli jako „wiodących" w odniesieniu do uwagi, jaką zdobyły w badaniach akademickich. Autorzy koncentrowali się na literaturze, która dotyczyła modeli dojrzałości obejmujących zarządzanie organizacją w całości, i nie brali pod uwagę modeli, które odnosiły się tylko do wąskiej, określonej dziedziny.

Jednym z wymienionych w obu publikacjach[65] modeli jest rozwiązanie opracowane przez międzynarodową organizację Object Management Group (OMG) Business Process Maturity Model (BPMM)[66]. Występuje w nim trzydzieści obszarów procesów, przypisanych do pięciu poziomów dojrzałości oraz blisko 350 praktyk szczegółowych. Również rozwiązanie Business Process Management Maturity (BPMM), które zostało opracowane przez międzynarodową firmę konsultingową Gartner, wzoruje się na koncepcji CMM. Model identyfikuje sześć obszarów oceny (organizacja i kultura, kompetencje procesowe, stosowane metody, technika i struktura, metryki i miary, nadzór). Dla każdego z nich opracowano zestaw wskazówek umożliwiających zakwalifikowanie do odpowiedniego z pięciu poziomów dojrzałości.

W obszarze zarządzania projektami brytyjska organizacja Office of Government Commerce[67] (OGC) opracowała model dojrzałości PRINCE2 Maturity Model (P2MM) – oceniający organizacje w aspekcie skutecznego stosowania metodyki PRINCE2, który również opiera się na wytycznych zastosowanych w modelu CMM\CMMI.

Inny podział modeli dojrzałości zaproponowali Jerzy Auksztol i Magdalena Chomuszko. W swojej publikacji wyróżnili cztery grupy[68]:

- Galaktyka modeli opartych na CMM;
- Business Process Maturity Model (BPMM);
- Modele branżowe, często inspirowane przez CMM/CMMI lub BPMM;
- Bardziej ogólne modele organizacji, które zawierają pewne elementy dojrzałości, np. ITIL, który zawiera dedykowaną część związaną z dojrzałością procesową: Process Maturity Framework (PMF).

[65] M. Juchniewicz, op. cit., s. 34–45; A. Tarhan, O. Turetken, H. A. Reijers, op. cit., s. 122–134.

[66] OMG Document Number: formal/2008-06-01, Business Process Maturity Model (BPMM), https://www.omg.org/spec/BPMM/1.0/PDF, dostęp: 30.03.2021 r.

[67] Office of Government Commerce (OGC) było brytyjskim biurem rządowym utworzonym w 2000 r., a zamkniętym w 2011 r. Celem OGC było wspieranie procesu zamówień i przejęć organizacji sektora publicznego w Wielkiej Brytanii poprzez wytyczne dotyczące polityki i procesów oraz negocjacje nadrzędnych ram usług i świadczenia usług. Rozwiązania PRINCE2, ITIL zostały przejęte przez spółką joint venture AXELOS, utworzoną w 2013 r. przez Cabinet Office, źródło: https://www.axelos.com/about-axelos, dostęp: 5.05.2021 r.

[68] J. Auksztol, M. Chomuszko, *Modelowanie organizacji procesowej*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 42–43.

Również tu autorzy zauważyli zjawisko wzorowania się na już istniejących rozwiązaniach, a szczególnie na CMM.

Modele dojrzałości są jednym z narzędzi umożliwiających doskonalenie organizacji[69]. Pozwalają one w procesie ewaluacji przypisać organizację do określonego poziomu rozwoju i na tej podstawie zarekomendować podjęcie działań zmierzających do osiągnięcia wyższego poziomu, doskonalenia kluczowych czynników sukcesu[70] prowadzących do osiągnięcia założonych celów[71]. Modele dojrzałości zyskały uznanie zwłaszcza w zarządzaniu procesami i projektami, jednakże ich zasady działania pozwalają na szerokie zastosowanie w wielu obszarach działalności organizacji, m.in. w doskonaleniu systemów i podsystemów zarządzania w organizacji[72].

1.1.4. System zarządzania i ocena jego dojrzałości

Pojęcie systemu zarządzania wywodzi się z systemowej perspektywy postrzegania organizacji[73]. Badacze zwracają uwagę na integralność celów i spójność wszystkich elementów systemu, którym jest organizacja[74]. Renesis Likert był jednym z pierwszych badaczy, którzy wprowadzili do literatury pojęcie systemu zarządzania. Wyróżnił on występowanie czterech stylów przywódczych, które nazwał systemami[75]: eksploatatorsko-autorytarny (ang. *exploitative authoritative*), paternalistyczny (ang. *benevolent authoritative*), konsultacyjny (ang. *consultative*) oraz partycypacyjny

[69] M. Juchniewicz, op. cit., s. 34–45.

[70] Kluczowe czynniki sukcesu (ang. *critical sucess factors* – CSF): „to kilka kluczowych obszarów działalności, w których korzystne wyniki są absolutnie niezbędne, aby dany menedżer mógł osiągnąć swoje cele".

Tłumaczenie własne definicji: „Critical success factors are the few key areas of activity in which favorable results are absolutely necessary for a particular manager to reach his goals" za: Bullen, J.F. Rockart, *A primer on critical success factors,* Sloan School of Management, Massachusetts Institute of Technology, 1981, s. 3.

„Kluczowymi czynnikami sukcesu są te działania, cechy, kompetencje i umiejętności, które są postrzegane jako krytyczne (niezbędne) warunki wstępne dla sukcesu organizacji w swojej branży w danym momencie" za: A. Niemiec, *Możliwość zastosowania analizy istotności-osiągnięć w identyfikacji i ewaluacji zestawu kluczowych mierników dokonań (KPIs)*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego, nr 873. Finanse, Rynki Finansowe, Ubezpieczenia" 2015, 77, s. 565.

[71] A. van Looy, *Business Process Maturity – A Comparative Study on a Sample of Business Process Maturity Models,* Springer Briefs in Business Process Management, 2014.

[72] PN-EN ISO 9004:2018-06 Zarządzanie jakością – Jakość organizacji – Wytyczne osiągnięcia trwałego sukcesu; J. Smagowicz, A. Kosieradzka, op. cit., s. 289.

[73] L. von Bertallanfy, *Ogólna teoria systemów*. *Podstawy, rozwój, zastosowania*, PWE, Warszawa 1984; G. Bełz, J. Skalik, *Rozumienie systemu zarządzania. Próba definicji*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Kształtowanie i doskonalenie systemu zarządzania w przedsiębiorstwach" 2011, nr 178., s. 9–23.

[74] J. Skalik, A. Barabasz, G. Bełz, *Systemowe uwarunkowania rozwoju metod zarządzania. Przykład modelu Triady*, „Acta Universitatis Lodziensis. Folia Oeconomica" 2010, 234, s. 71–83.

[75] Likert R., *New Patterns of Management*, McGraw–Hill, New York 1961; K. Krzakiewicz, S. Cyfert, *Podstawy zarządzania organizacjami*, University of Economics and Business, Poznań 2020, s. 251–252.

(ang. *participative group*). Systemy Likerta opisują przede wszystkim charakter relacji pomiędzy przełożonymi a podwładnymi. Natomiast Thomas Peters zdefiniował, jakie obszary działalności zwykle obejmuje pojęcie „system zarządzania". Według niego są to: systemy planowania strategicznego i operacyjnego, system podejmowania decyzji inwestycyjnych, system budżetowania i system personalny. Tak zdefiniowany system w połączeniu ze strukturą organizacji to nic innego jak ramy dla niemal wszystkich ważnych interakcji zarządczych. Można w nich kształtować: wartości, kulturę, charakter i kompetencje organizacji. Analizując wewnętrzną budowę systemów, przedstawił komponenty systemu zarządzania, porządkując je w trzy klasy, reprezentujące trzy różne poziomy abstrakcji. Pierwsza klasa to kierunkowskazy (ang. *directional signals*), obejmująca orientację biznesową (ang. *business focus*) oraz normy i wartości stanowiące wytyczne w systemach zarządzania. Druga klasa to fazy procesu (ang. *process phases*). Wyodrębnione zostały następujące fazy: identyfikacja problemu, rozwiązanie problemu, eliminowanie problemu, interpretacja. Zdefiniowanie tej klasy wynika z przekonania T. Petersa, że system zarządzania jest maszyną do rozwiązywania problemów. Trzecią klasą są narzędzia zarządzania (ang. *management tools*), które podzielił na: osobiste działania (ang. *personal actions*), strukturyzowanie forum (ang. *forum structuring*), mechanizmy nagradzania (ang. *reward mechanisms*)[76]. T. Peters przedstawił w swojej pracy tezę, że najważniejszym nośnikiem znaczenia, a tym samym nośnikiem charakteru organizacji, jest pełny zestaw systemów lub procesów zarządzania. Innymi słowy: według niego system zarządzania jest językiem organizacji. Zdaniem Grzegorza Bełzy i Jana Skalika[77] koncepcja zaprezentowana przez T. Petersa jest czymś więcej niż tylko metodą zarządzania, ponieważ obejmuje ona również techniki postępowania kierowniczego, procedury działania oraz kluczowe na poziomie całej organizacji normy i wartości. Należy zauważyć, że w innej publikacji[78], w której T. Peters wspólnie z R. Watermanem i J. Phillipsem przedstawili koncepcję modelu „7-S", zarówno wartości, jak i struktury organizacyjne traktowane są jako odrębne elementy. Autorzy zaś system zarządzania definiują jako zbiór wszystkich procedur formalnych i nieformalnych, które przyczyniają się do funkcjonowania na bieżąco organizacji.

[76] T. Peters, *Management systems: The language of organizational character and competence*, „Organizational Dynamics" 1980, Vol. 9, No. 1, s. 3–26.

[77] G. Bełz, J. Skalik, *Rozumienie*…, op. cit., s. 9–23.

[78] R. Waterman, T. Peters, J. Phillips, *Structure is not organization*, Business Horizons, 1980, s. 14–26.

Andrzej Koźmiński zdefiniował system zarządzania poprzez jego rolę w funkcjonowaniu organizacji oraz przejawy jego działania. Uważał, że funkcjonowanie systemu zarządzania przejawia się istnieniem procesów informacyjno-decyzyjnych oraz że jest on nadrzędny wobec pozostałych podsystemów organizacji. Jego podstawowymi elementami są: mechanizmy ludzkiego zachowania, role społeczne i organizacyjne, systemy informacyjne, mechanizmy kierowania zespołami pracowniczymi, czynniki techniczne[79]. Jerzy Trzcieniecki definiuje system zarządzania jako podsystem organizacji, który jest zbiorem współdziałających ze sobą, wzajemnie powiązanych elementów, służących: zapewnieniu osiągnięcia celów, doborowi metod i środków działania, powiązaniu i zharmonizowaniu działań indywidualnych oraz zespołowych. Autor ten stwierdza również, że zarządzanie można określić jako realizowanie procesu doprowadzenia określonego systemu do wcześniej wyznaczonego nowego stanu przez oddziaływanie na jego zmienne[80]. Podobnie uważał Lech Szybiński – zdefiniował on system zarządzania jako zbiór obiektów zmierzających do spowodowania realizacji przez instytucję określonych celów[81]. Adam Stabryła twierdził, iż system zarządzania może być rozpatrywany w aspekcie zarówno statycznym, to jest: stanowisk kierowniczych, zbiorów uprawnień decyzyjnych czy struktury jednostek organizacyjnych, jak i dynamicznym, gdzie brany jest po uwagę proces zarządzania z jego układami informacyjno-decyzyjnymi i funkcjami zarządzania[82]. Leszek Krzyżanowski uważa, że system zarządzania składa się z warstwy konceptualnej oraz z warstwy materialnej. Do pierwszej z nich należy uporządkowany zbiór instrumentów, reguł i procedur zarządzania. Drugą warstwę tworzy aparat zarządzający organizacją oraz wyposażenie materialno-techniczno-informatyczne[83]. W warstwie konceptualnej L. Krzyżanowski rozróżnia instrumenty zarządzania: bezpośrednie – wpływające wprost na zachowania pracowników oraz pośrednie – zorientowane na kształtowanie hierarchii wartości, postaw lub interesów, a za ich pośrednictwem wywierające wpływ na organizacyjne zachowania uczestników. Autor dzieli reguł zarządzania na zasady konstruowania i modyfikacji planów oraz reguły kształtowania formalnej struktury organizacji i podziału ról organizacyjnych. Ten sam

[79] A. K. Koźmiński, *Zarządzanie systemowe*, PWE, Warszawa 1971.

[80] J. Trzcieniecki, *Projektowanie systemów zarządzania*, PWN, Warszawa 1980.

[81] L. Szybiński, *Projektowanie organizacji i systemu zarządzania, cz. I*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 1984.

[82] A. Stabryła, *Analiza systemowa procesu zarządzania*, PAN, Zakład Narodowy im. Ossolińskich, Wrocław 1984.

[83] L. Krzyżanowski, *Podstawy nauk o zarządzaniu*, Wydawnictwo Naukowe PWN, Warszawa 1994.

badacz wyróżnia następujące procedury: podejmowania i optymalizacji decyzji kierowniczych; technologiczne, technologiczno-organizacyjne i technologiczno-ekonomiczne; organizacyjne i organizatorskie; kadrowo-płacowe; inne procedury i techniki badania zachowań organizacyjnych, wpływania na zachowania, ujawniania i rozwiązywania konfliktów organizacyjnych[84]. Z kolei Jan M. Myszewski uważa, że „zarządzanie jest działaniem systemowym". Zaproponował on model cybernetyczny zarządzania, w którym wyszczególnił podsystem zarządzający i podsystem zarządzany. W swoim modelu podsystem zarządzający utożsamił z systemem sterującym. Sterowanie systemem zdefiniował jako oddziaływanie na dany system, którego celem jest osiągnięcie i utrzymanie zamierzonych właściwości[85].

Grzegorz Bełz, Jan Skalik zaproponowali przyjęcie definicji, „według której system zarządzania to całokształt: wartości i celów, regulacji i struktur, metod i praktyk zarządzania oraz wynikających z mechanizmów regulacyjnych relacji między nimi, który to całokształt warunkuje sposób realizacji procesu zarządzania. Proces zarządzania rozumiany jest w tym kontekście jako ciągły i zorganizowany zespół wszelkich działań informacyjno-decyzyjnych i koordynacyjnych służących osiąganiu celów organizacji"[86].

Według Międzynarodowej Organizacji Standaryzacyjnej (ang. *International Organization for Standardization,* skrót: ISO), która odegrała kluczową rolę w standaryzacji różnych systemów zarządzania poprzez wydawanie międzynarodowych norm, systemem zarządzania jest: „sposób, w jaki organizacja zarządza wzajemnie powiązanymi częściami swojej działalności, aby osiągnąć swoje cele. Cele te mogą odnosić się do wielu różnych tematów, w tym: jakości produktu lub usługi, efektywności operacyjnej, efektywności środowiskowej, bezpieczeństwa i higieny pracy w miejscu pracy i wielu innych. Poziom złożoności systemu będzie zależał od specyficznego kontekstu każdej organizacji. W przypadku niektórych organizacji, szczególnie mniejszych, może to po prostu oznaczać posiadanie silnego przywództwa, zapewniającego jasną definicję oczekiwań wobec każdego pracownika i tego, w jaki sposób przyczynia się on do osiągania ogólnych celów organizacji, bez konieczności stosowania obszernej dokumentacji. Bardziej złożone przedsiębiorstwa, działające na przykład w sektorach podlegających ścisłym regulacjom, mogą potrzebować obszernej

[84] Ibidem, s. 226.

[85] J.M. Myszewski, *Zarządzanie zmiennością. Systemowe spojrzenie na metody statystyczne w zarządzaniu jakością*, Orgmasz, Warszawa 1998, s. 18.

[86] G. Bełz, J. Skalik, *Rozumienie*…, op. cit., s. 9–23.

dokumentacji i kontroli, aby wywiązać się ze swoich obowiązków prawnych i osiągnąć cele organizacyjne”[87].

Z przedstawionych powyżej definicji pojęcia systemu zarządzania wynika, że procesy są jednym z komponentów systemu zarządzania[88]. Z możliwości pomiaru dojrzałości procesów, opisanej w podrozdziale 1.1.2 dysertacji, wynika, że ocenie dojrzałości może podlegać również system zarządzania. W polskiej literaturze przedmiotu występują prace poświęcone badaniom dojrzałości systemów zarządzania. W swojej publikacji[89], porównującej modele dojrzałości, Anna Kosieradzka i Justyna Smagowicz zastosowały podział odnoszący się do różnych obszarów zarządzania, uwzględniający m.in. zarządzanie ryzykiem i ciągłością działania, zarządzanie administracją. Również Katarzyna Hys[90] czy Radosław Wolniak[91] w swoich pracach opisują metody mierzenia dojrzałości systemów zarządzania. Obie publikacje dotyczą pomiaru dojrzałości systemu zarządzania jakością opartego na standardzie 9001[92]. Radosław Wolniak przeprowadził badania w ponad 500 polskich organizacjach. Wnioskował z nich, że najniższy poziom dojrzałości organizacje uzyskują w zarządzaniu zasobami ludzkimi i w obszarze przywództwa.

[87] https://www.iso.org/management-system-standards.html, dostęp: 10.03.2024 r.

Definicja normy ISO 22000:2018, 3.25: „System zarządzania – zestaw wzajemnie powiązanych lub wzajemnie oddziałujących elementów organizacji (3.27) w celu ustanowienia polityk (3.30) i celów (3.26) oraz procesów (3.32) służących osiągnięciu tych celów.
Uwaga 1: System zarządzania może dotyczyć jednej lub kilku dyscyplin.
Uwaga 2: Elementy systemu obejmują strukturę organizacji, role i obowiązki, planowanie i działanie.
Uwaga 3: Zakres systemu zarządzania może obejmować całą organizację, określone i zidentyfikowane funkcje organizacji, określone i zidentyfikowane sekcje organizacji lub jedną lub więcej funkcji w całej grupie organizacji.
Uwaga 4: Odpowiednie dyscypliny to na przykład: system zarządzania jakością lub system zarządzania środowiskiem” (tłumaczenie własne tekstu z ang.: Management System – set of interrelated or interacting elements of an organization (3.27) to establish policies (3.30) and objectives (3.26) and processes (3.32) to achieve those objectives.
Note 1 to entry: A management system can address a single discipline or several disciplines.
Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning and operation.
Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.
Note 4 to entry: Relevant disciplines are, for example, a quality management system or an environmental management system).

[88] G. Bełz, J. Skalik, *Rozumienie*…, op. cit., s. 9–23; T. Peters, *Management systems: The language of organizational character and competence*, „Organizational Dynamics” 1980, Vol. 9, No. 1, s. 3–26.

[89] J. Smagowicz, A. Kosieradzka, op. cit., s. 289.

[90] K. Hys, *Wybrane modele dojrzałości systemu zarządzania jakością w organizacji*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu: Sieci międzyorganizacyjne, procesy i projekty w erze paradoksów, 2016, 5(421).

[91] R. Wolniak, *The level of maturity of quality management systems in Poland-Results of empirical research*, Sustainability (Switzerland), 2019, 11(15).

[92] PN-EN ISO 9001:2015-10 – Systemy zarządzania jakością – Wymagania.

Jak napisał Radosław Haffer: „o dojrzałości systemu zarządzania decyduje nie tyle wdrożenie w przedsiębiorstwie konkretnego podejścia do zarządzania, standardu zarządzania, metodyki usprawnienia procesów, modelu samooceny czy technologii informatycznej, ile właściwe dopasowanie wszystkich tych elementów do modelu biznesowego”[93].

1.2. Bezpieczeństwo informacji, bezpieczeństwo systemów informatycznych oraz systemy zarządzania bezpieczeństwem informacji

1.2.1. Bezpieczeństwo informacji

W erze cywilizacji przemysłowej[94] rozwój gospodarczy wiązał się z eksploatacją pracownika i zasobów naturalnych, prymatem techniki oraz kapitałem finansowym. W XXI w. rozwój ekonomiczny, polityczny i kulturalny społeczeństw uzależniony jest przede wszystkim od informacji, wiedzy i komunikacji[95].

Termin informacja pochodzi od łacińskiego czasownika *in-formare*. Myśliciele, tacy jak Cyceron i Augustyn z Hippony, używali go w kontekście teorii idei (inaczej: teorii form) Platona. W starożytności i średniowieczu termin „informacja” używany był przede wszystkim w opisie i wyjaśnianiu poznania, oznaczał treść poznawczą pochodzącą od rzeczy. Informacja była rozumiana jako rezultat czynności „in-formowania”, czyli formułowania treści poznawczych[96]. W XX w., wraz z wynalezieniem maszyn cyfrowych i rozwojem technik komputerowych, informacja przestała być wiązana wyłącznie z poznaniem. Na przestrzeni wieków stała się nie tylko

[93] R. Haffer, *Samoocena i pomiar wyników działalności w systemach zarządzania przedsiębiorstw: w poszukiwaniu doskonałości biznesowej*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2011.

[94] A. Toffler, *Trzecia fala*, Książka i Wiedza, Warszawa 1986, s. 38–39.

[95] M. Muraszkiewicz, *Społeczeństwo informacyjne i praca*, [w:] *Społeczeństwo informacyjne i jego technologie*, (red.) B. Sosińska-Kalata, K. Materska, W. Gliński, Wydawnictwo SBP, Warszawa 2004, s. 13–25; P.F. Drucker, *Knowledge-Worker Productivity: THE BIGGEST CHALLENGE*, „California Management Review” 1999, Vol. 41(2), s. 79–94; P.F. Drucker, *Information, Communications, and Understanding*, Routledge 2017; J. Borbinha, D. Proença, *Information Security Management Systems – A Maturity Model Based on ISO/IEC 27001*, [w:] *Business Information Systems*, (red.) Abramowicz W., Paschke A., BIS 2018. Lecture Notes in Business Information Processing, vol. 320, Springer, Cham 2018, s. 102–114.

[96] P. Adriaans, J. Benthem, *Introduction: Information is What Information Does*, [w:] *Philosophy of Information*, (red.) Adriaans P., Benthem J., Elsevier 2008, s. 5–28.

przedmiotem teorii filozoficznych[97], ale również matematycznych i informatycznych (ang. *computer science*), np. teoria informacji[98] czy złożoność Kołmogorowa[99].

Pojęcie informacji ściśle wiąże się z terminem danych, które to są surowymi i niepoddanymi analizie wartościami lub zbiorami wartości przekazującymi opis faktów i zdarzeń[100]. Informacja wraz z danymi stanowi wiedzę. W podobny sposób opisywał zależności między wymienionymi pojęciami Bogdan Stefanowicz[101]: „Dane stanowią poziom niższy w stosunku do informacji. Terminy te nie mogą więc być stosowane zamiennie, jako synonimy. Poziom jeszcze wyższy tworzy wiedza. A nad nią dominuje mądrość". Rusesell L. Ackoff pisał, że z mądrości wywodzi się zrozumienie, wiedza, informacja, a na samym dole plasują się dane. Nie mają one żadnej wartości, dopóki nie zostaną przetworzone w użyteczną, odpowiednią formę. Dlatego różnica między danymi a informacją ma charakter funkcjonalny, a nie strukturalny. Dane zwykle ulegają zmniejszeniu, gdy są przekształcane w informacje. Zrozumienie relacji prowadzi od danych do informacji, zrozumienie wzorców skutkuje wiedzą, a zrozumienie zasad prowadzi do mądrości[102].

Według Petera J. Denninga[103] informacja to osąd osoby lub grupy osób, że pewne dane odpowiadają na stawiane pytania. Innymi słowy: informacja to znaczenie, jakie ktoś przypisuje danym[104]. Informacja istnieje zatem w oczach odbiorcy – te same dane mogą być nieważne dla jednej osoby, a bardzo ważne dla innej. Wiesław Flakiewicz[105] zdefiniował informację jako czynnik, który zwiększa naszą wiedzę o otaczającej nas rzeczywistości, natomiast Jerzy Kisielnicki i Henryk Sroka[106] jako rodzaj zasobu, który pozwala na zwiększenie naszej wiedzy o nas i otaczającym nas świecie. Ikujirō Nonaka

[97] M. G. Murphey, *The Development of Peirce's Philosophy*, Harvard University Press: Cambridge, MA, USA, 1961.

[98] C. Shannon. *A Mathematical Theory of Communication*, „Bell System Technical Journal" 1948, 27, s. 379–423.

[99] A. N. Kolmogorov, *Three approaches to the quantitative definition of information*, „International Journal of Computer Mathematics" 1968, 2:1–4, s. 157–168; A.N. Kolmogorov, *On Tables of Random Numbers*, „Theoretical Computer Scienc" (1998) [1963], 207 (2), s. 387–395.

[100] W. M. Grudzewski, I. K. Hejduk, *Zarządzanie wiedzą w przedsiębiorstwach*, Difin, Warszawa 2004, s. 75; M. Dembowska, *Słownik terminologiczny informacji naukowej*, Zakład Narodowy im. Ossolińskich, Wrocław–Warszawa–Kraków–Gdańsk 1979, s. 36.

[101] B. Stefanowicz, *Informacja*, Oficyna Wydawnicza SGH, Warszawa 2004.

[102] R.L. Ackoff, *From Data to Wisdom*, „Journal of Applied Systems Analysis" 1989, Vol. 16, s. 3–9.

[103] P.J. Denning, *The IT Schools Movement*, „Communications of ACM" 2001, Vol. 44, No. 8, s. 19–22.

[104] R. van der Spek, A. Spijkervet, *Knowledge Management: Dealing Intelligently with Knowledge*, CIBIT, Utrecht 1997; C.W. Choo, D. Detlor, D. Turnbull, *Web Work: Information Seeking and Knowledge Work on the World Wide Web*, Kluwer, Dordrecht 2000.

[105] W. Flakiewicz, *Pojęcie informacji w technologii multimedialnej*, SGH, Warszawa 2005.

[106] J. Kisielnicki, H. Sroka, *Systemy informacyjne biznesu*, Placet, Warszawa 2005.

i Hirotaka Takeuchi, podsumowując swoje badania nad wykorzystaniem informacji i wiedzy w strukturach organizacyjnych, zdefiniowali wiedzę jako dynamiczny ludzki proces uzasadniania osobistych przekonań co do „prawdy”[107].

Norma ISO/IEC 2382:2015-2121271 mówi[108] o informacji jako o wiedzy dotyczącej obiektów, takich jak: fakty, zdarzenia, rzeczy, procesy lub idee. Według norm z rodziny ISO/IEC 27k[109] informacje to ważne aktywa organizacji, niezbędne do jej działania. Mogą one przyjmować formę: dokumentu pisanego odręcznie, wydruku papierowego, pliku cyfrowego (np. dokument elektroniczny, plik wideo), wypowiedzi ustnej [ISO/IEC 27000:2018-3.2.2][110]. Elżbieta Niedzielska[111] stwierdziła, że: „informacja jest specyficznym dobrem niematerialnym, które w miarę postępu gospodarczego oraz rozwoju środków i form komunikowania się społecznego nabiera coraz większego znaczenia, przeobrażając oblicze wielu tradycyjnie zorganizowanych gospodarek świata”.

Rozwój technik komunikacyjnych – od połączeń telefonicznych do Internetu i systemów informatycznych – przyczynił się do wzrostu znaczenia i wpływu informacji na gospodarkę, jak również na społeczne, polityczne i prywatne aspekty życia ludzi. Ochrona informacji m.in. przed niepowołanym dostępem, na każdym etapie jej przetwarzania, jest wymaganiem stawianym przed organizację w celu zapewnienia prywatności osób, których dane są w jej posiadaniu, czy utrzymania konkurencyjności przedsiębiorstw.

Bezpieczeństwo informacji według ISACA zapewniane jest wtedy, gdy w ramach organizacji informacje są chronione przed ujawnieniem ich nieupoważnionym użytkownikom, niewłaściwą modyfikacją oraz brakiem dostępu w razie potrzeby. W zamieszczonej definicji bezpieczeństwa informacji w normie ISO/IEC 27000:2018[112] stwierdzono, że oprócz zachowania poufności, integralności i dostępności

[107] I. Nonaka, H. Takeuchi, *The Knowledge-Creating Company*, Oxford University Press, Oxford, UK 1995.

[108] ISO/IEC 2382:2015-2121271 Information technology — Vocabulary (tłumaczenie PKN: Technika informatyczna – Terminologia).

[109] Normy serii ISO/IEC 27k to normy z zakresu bezpieczeństwa teleinformatycznego i ochrony informacji, prezentujące m.in. model systemu zarządzania bezpieczeństwem informacji (SZBI).

[110] ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary (odpowiednik krajowy: Polska norma PN-EN ISO/IEC 27000:2020-07 – wersja angielska: Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia).

[111] E. Niedzielska (red.), *Informatyka ekonomiczna*, AE we Wrocławiu, Wrocław 1998, s. 20.

[112] ISO/IEC 27000:2018 – 3.28.

(ang. *confidentiality, integrity, availability,* skrót: CIA)[113] można dodatkowo uwzględnić takie cechy informacji, jak: autentyczność, rozliczalność, niezawodność i niezaprzeczalność[114]. Według normy bezpieczeństwo informacji (ang. *information security*, skrót: IS) można osiągnąć poprzez wdrożenie odpowiedniego zbioru zabezpieczeń, którego elementy można ustalić w procesie zarządzania ryzykiem[115]. Te zabezpieczenia następnie należy: wdrożyć, monitorować, przeglądać i doskonalić. W zbiorze publikacji ITIL[116] zarządzanie bezpieczeństwem informacji zdefiniowane jest jako proces odpowiedzialny za zapewnienie: poufności, integralności i dostępności aktywów, informacji, danych i usług informatycznych organizacji, odpowiadający uzgodnionym potrzebom biznesu.

W wielu badaniach[117], jak również w tej dysertacji bezpieczeństwo informacji oparte jest na tak zwanej triadzie CIA lub jej rozszerzonej wersji (np.: na autentyczności, rozliczalności, niezawodności i niezaprzeczalności)[118]. Są jednak prace krytykujące to podejście. Jedną z nich jest artykuł Björna Lundgrena i Niklasa Möllera, którzy uważają, że definicja CIA nie jest wystarczająco elastyczna, aby uwzględniać każdą sytuację i zróżnicować wymagania dotyczące różnych informacji, systemów lub organizacji. Nie uwzględnia również wpływu człowieka na bezpieczeństwo, zwłaszcza

[113] Poufność (ang. *confidentiality*, ISO/IEC 27000:2018-3.10) – właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom; integralność (ang. *integrity*, ISO/IEC 27000:2018-3.36) – właściwość polegająca na zapewnieniu dokładności i kompletności; dostępność (ang. *availability*, ISO/IEC 27000:2018-3.7) – właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu.

[114] Autentyczność (ang. *authenticity*, ISO/IEC 27000:2018-3.6) – właściwość, która polega na tym, że podmiot jest tym, za kogo się podaje; rozliczalność (ang. *accountability*, ISO/IEC 2382:2015-2126250) – zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz że wywołał je dany podmiot; niezawodność (ang. *reliability* – ISO/IEC 27000:2018-3.55) – właściwość oznaczająca spójne, zamierzone zachowanie i skutki; niezaprzeczalność (ang. *non-repudiation* – ISO/IEC 27000:2018-3.48) – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.

[115] ISO/IEC 27000:2018-4.5.5.

[116] ITIL (ang. *Information Technology Infrastructure Library*) – najlepsze praktyki związane procesowym zarządzaniem usługami IT, początkowo opracowywane przez agencję Central Computers and Telecommunications Agency (CCTA), która w późniejszym czasie stała się częścią biura UK Office of Government Commerce (OGC, ang. *Office of Government Commerce*).

[117] S.V. Thakare, D.V. Gore, *Comparative study of CIA and revised-CIA algorithm*, Proceedings – 2014, 4th International Conference on Communication Systems and Network Technologies, CSNT 2014, art. no. 6821492, s. 713–718; R.A. Haraty, M. Naous, *Modeling and validating the clinical information systems policy using alloy*, „Lecture Notes in Computer Science" (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2013, 7798 LNCS, s. 1–17; S.N. Shah, *Understanding medical practice cybersecurity risks: Mitigations for the digital health era* [w:] Risk Management, Liability Insurance, and Asset Protection Strategies for Doctors and Advisors: Best Practices from Leading Consultants and Certified Medical Planners, CRC Press 2015, s. 245–263.

[118] J.S. Tiller, B.D. Fish, *Packet sniffers and network monitors*, [w:] *Information security management handbook* 5th ed., (red.) H.F. Tipton, M. Krause, Boca Raton, Auerbach 2004, s. 223; M. Bishop, *Introduction to computer security*, Addison-Wesley, Boston 2005; K.S. Wilson, *Conflicts among the pillars of information assurance* (2013) IT Professional, 15 (4), no. 6152082, s. 44 – 49.

w sposób, który analitycznie pozwala określić, na czym polega naruszenie lub kiedy ono następuje; nie dostarcza też niezbędnych podstaw do zapewnienia bezpieczeństwa. Autorzy zaproponowali definicję „odpowiedniego dostępu”[119] (ang. *Appropriate Access*, skrót: AA) jako nowe podejście do bezpieczeństwa informacji: „Informacja I jest bezpieczna dla interesariusza H wtedy i tylko wtedy, gdy: dla każdego agenta A i każdej części P informacji I, agent A ma odpowiedni dostęp do części P w stosunku do interesariusza H”[120]. W definicji termin „agent” odnosi się do dowolnego podmiotu (technicznego, oprogramowania, człowieka itp.), który może posiadać jakiś rodzaj dostępu do jakiejś części informacji, której bezpieczeństwo jest rozważane.

W celu uniknięcia lub zmniejszenia częstości występowania incydentów dotyczących bezpieczeństwa informacji podejmuje się działania, mające na celu zidentyfikowanie zagrożeń oraz oszacowanie ryzyka wystąpienia naruszeń bezpieczeństwa aktywów. Incydenty to pojedyncze niepożądane lub niespodziewane zdarzenia lub serie takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji[121]. Zagrożenia[122], którym podlegają informacje będące w posiadaniu i przetwarzane w organizacji, mogą wynikać z przyczyn naturalnych (np. pożar, powódź) lub być wywołane przez człowieka. Zagrożeniem mogą być: błędy popełnione przez uprawnionych użytkowników, atak celowy, dobrze przygotowany, wykorzystujący elementy socjotechniki, jak również atak zautomatyzowany przy użyciu specjalistycznego oprogramowania.

Zagrożenia wywołują szkody w organizacji, jeżeli istnieją podatności[123] odpowiadające tym zagrożeniom. Podatnościami mogą być błędy w strukturze organizacyjnej, w obsadzie stanowisk oraz wady i luki w wykorzystywanych systemach informatycznych oraz brak świadomości zagrożeń. Mikko T. Siponen[124] definiuje świadomość bezpieczeństwa informacji jako wiedzę jednostki na temat poszczególnych zagrożeń bezpieczeństwa i potencjalnych środków zaradczych wobec tych zagrożeń.

[119] B. Lundgren, N. Möller, *Defining Information Security*, „Sci Eng Ethics” 2019, Vol. 25, s. 419–441.

[120] Ibidem.

[121] ISO/IEC 27000:2018-3.31.

[122] Zagrożenie (ang. *threat*, ISO/IEC 27000:2018-3.74) – potencjalna przyczyna niepożądanego incydentu, który może spowodować szkodę dla systemu lub organizacji.

[123] Podatność (ang. *vulnerability*, ISO/IEC 27000:2018-3.77) – słabość aktywu lub zabezpieczenia, która może być wykorzystana przez co najmniej jedno zagrożenie.

[124] M. Siponen, *A conceptual foundation for organizational information security awareness*, „Information Management & Computer Security” 2000, nr 8(1), 31–41.

Joanna Chmura w swoim artykule[125] podkreśla istotę i znaczenie świadomości bezpieczeństwa informacji w organizacji oraz zajmuje się analizą wybranych metod kształtowania świadomości pracowników w zakresie bezpieczeństwa informacji.

1.2.2. Bezpieczeństwo systemów informatycznych

Bezpieczeństwo systemów informatycznych[126] stało się współcześnie ważnym zagadnieniem dla organizacji, ponieważ większość działań, w tym procesy związane z przetwarzaniem informacji, uzależniona jest od technik informatycznych i komunikacyjnych (ang. *Information and Communication Technologies* – ICT)[127]. Opracowano wiele narzędzi i mechanizmów obejmujących różne aspekty bezpieczeństwa systemów informatycznych. Ich skuteczność uzależniona jest od świadomości zagrożeń użytkowników tych systemów. Liczba incydentów związanych z bezpieczeństwem i wynikające z nich straty finansowe stale rosną – zarówno pod względem rozmiarów, jak i dotkliwości[128].

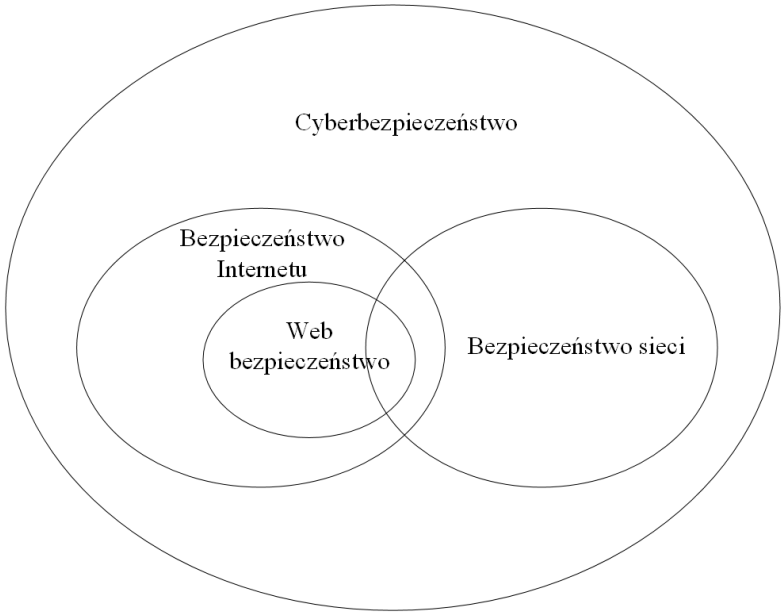
[125] J. Chmura, *Forming the Awareness of Employees in the Field of Information Security*, „Journal of Positive Management" 2017, nr 8(1), s. 78.

[126] System informacyjny (ang. *information system*, ISO/IEC 2382:2015-2121292) – »fundamentalne terminy« system przetwarzania informacji, wraz z powiązanymi zasobami organizacyjnymi, takimi jak zasoby ludzkie, techniczne i finansowe, który dostarcza i rozpowszechnia informacje (tłumaczenie własne tekstu ang.: information system »fundamental terms« information processing system, together with associated organizational resources such as human, technical, and financial resources, that provides and distributes information); system przetwarzania informacji/system informatyczny (ang. *information processing system*, ISO/IEC 2382:2015-2121291) – jeden lub więcej takich systemów i urządzeń do przetwarzania danych, jak sprzęt biurowy i komunikacyjny, które przetwarzają informacje (tłumaczenie własne tekstu ang.: information processing system – one or more data processing systems and devices, such as office and communication equipment, that perform information processing).

[127] Rozwinięcie angielskiego skrótu ICT – Information and Communication Technologies tłumaczone jest na język polski jako „Technologie informacyjno-komunikacyjne", np. definicja Głównego Urzędu Statystycznego: „Technologie informacyjno-komunikacyjne (synonimy: Technologie teleinformacyjne, ICT – ang.: Information and Communication Technologies). Definicja: Rodzina technologii przetwarzających, gromadzących i przesyłających informacje w formie elektronicznej", https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1893,pojecie.html, dostęp: 17.11.2020 r. Między innymi D. Lisiak-Felicka i M. Szmit. (D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, European Association For Security, Kraków 2016) oraz Zbigniew Łucki (Zbigniew Łucki, *Proszę… nie mówmy „technologia" na technikę!* Biuletyn Informacyjny Pracowników Akademii Górniczo-Hutniczej) w swoich publikacjach wyjaśniają, iż prawidłowym tłumaczeniem angielskiego terminu „technology" na język polski jest „technika". Pojęcie „technika" jest używane w polskich tłumaczeniach norm ISO/IEC z serii 27k.

[128] NASK/CERT Polska, Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2019 z działalności CERT Polska 2020, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf, dostęp: 1.09.2020 r.; https://www.statista.com/topics/9918/cyber-crime-and-the-financial-industry-in-the-united-states/#topicOverview, dostęp: 12.05.2024 r.

W XXI w. w opracowaniach praktycznych coraz częściej pojawia się termin cyberbezpieczeństwo. Norma ISO/IEC 27032:2023[129] obejmuje podstawowe praktyki bezpieczeństwa dla interesariuszy w cyberprzestrzeni[130] oraz wyjaśnia związki między cyberbezpieczeństwem a innymi rodzajami bezpieczeństwa (Rysunek 1.4), a ponadto definiuje interesariuszy i ich role. Termin „cyberbezpieczeństwo"[131] zdefiniowany w niej został jako ochrona ludzi, społeczeństwa, organizacji i narodów przed zagrożeniami cybernetycznymi, przy czym ochrona oznacza utrzymywanie ryzyka cybernetycznego na tolerowanym poziomie.



Rysunek 1.4. Związek między cyberbezpieczeństwem a innymi rodzajami bezpieczeństwa
Źródło: ISO/IEC 27032:2023, Definicje pojęć: 3.6 ***Cyberbezpieczeństwo*** *(ang. Cybersecurity) – ochrona ludzi, społeczeństwa, organizacji i narodów przed zagrożeniami cybernetycznymi. Uwaga 1 do wpisu: Ochrona oznacza utrzymywanie ryzyka cybernetycznego na tolerowanym poziomie. [Źródło: ISO/IEC TS 27100:2020, 3.2]; 3.12* ***Bezpieczeństwo Internetu*** *(ang. Internet security) – zachowanie poufności, integralności i dostępności informacji przez Internet (3.11). Uwaga 1 do wpisu: Ponadto w grę mogą wchodzić inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Uwaga 2 do wpisu: Należy odnieść się do definicji poufności, integralności, dostępności, autentyczności, rozliczalności, niezaprzeczalności i niezawodności w ISO/IEC 27000:2018, klauzula 3;* ***Web***

[129] ISO/IEC 27032:2023 Cybersecurity – Guidelines for Internet security (pol. Cyberbezpieczeństwo – Wytyczne dotyczące bezpieczeństwa Internetu).

[130] Cyberprzestrzeń – wzajemnie połączone środowisko cyfrowe sieci, usług, systemów, ludzi, procesów, organizacji i tego, co znajduje się w środowisku cyfrowym lub przez nie przechodzi.

Uwaga 1: Połączone środowisko cyfrowe, które przebiega przez infrastrukturę publiczną, np. Internet, a nie części wewnętrznej sieci organizacji lub szczelne środowiska cyfrowe, które mogą nie przechodzić przez infrastrukturę publiczną (tłumaczenie własne tekstu ang.: *cyberspace* – interconnected digital environment of networks, services, systems, people, processes, organizations, and that which resides on the digital environment or traverses through it.

Note 1 to entry: Interconnected digital environment that traverses public infrastructure e.g. the internet, rather than parts of the organisation's internal network or air-gapped digital environments that may not traverse public infrastructure), źródło: ISO/IEC TS 27100:2020 - 3.5.

[131] „Cybersecurity – safeguarding of people, society, organizations and nations from cyber risks Note 1 to entry: Safeguarding means to keep cyber risk at a tolerable level. [SOURCE:ISO/IEC TS 27100:2020 - 3.2]".

bezpieczeństwo *(ang. Web security) – bezpieczeństwo informacji i usług w uniwersum sieci (ISO/IEC 27032:2023, s. 6);* ***Bezpieczeństwo sieci*** *(ang. Network security) – bezpieczeństwo wszystkich rodzajów sieci istniejących w organizacji, w tym sieć lokalna, sieć rozległa, sieć bezprzewodowa. Sieci te mogą obejmować takie komponenty, jak: routery, koncentratory, okablowanie, kontrolery telekomunikacyjne, kluczowe centra dystrybucji i techniczne urządzenia sterujące (ISO/IEC 27032:2023, s. 6).*

Powszechne wykorzystywanie mediów społecznościowych, urządzeń mobilnych, chmury obliczeniowej, sztucznej inteligencji[132] oraz realizacje koncepcji „internetu rzeczy"[133] (ang. *Internet of Things*) „e-administracji"[134] (ang. *E-government*) i „inteligentnych miast"[135] (ang. *Smart Cities*) wpłynęło na to, że zagrożenia związane z cyberbezpieczeństwem stają się coraz bardziej różnorodne i stanowią duże wyzwanie dla utrzymania celów biznesowych, społecznych i politycznych. Badacze R. Kour, R. Karim, A. Thaduri[136] podkreślają, że cyberataki stają się coraz częstsze i bardziej dotkliwe. Rosną zaawansowane zagrożenia cyberbezpieczeństwa w wielu obszarach działalności organizacji, takich jak np.: finanse, zdrowie, handel detaliczny, administracja publiczna, telekomunikacja, transport. Kraje, organizacje i ogół społeczeństwa narażone są na błędne decyzje, utratę reputacji, straty finansowe i zdrowotne. Rządy państw określają w swoich dokumentach strategicznych, co rozumieją przez bezpieczeństwo cyberprzestrzeni[137]. W polskim prawie, w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity, skrót:

[132] A.A. Rakowska, *Human-Robot Interactions in the Workplace – Key Challenges and Concerns*, „Annales Universitatis Mariae Curie-Skłodowska, sectio H – Oeconomia" 2022, 56, 1, s. 95-106.

[133] Internet rzeczy (ang. *Internet of Things* - IoT) – „samokonfigurująca się, adaptacyjna, złożona sieć, która łączy »rzeczy« z Internetem za pomocą standardowych protokołów komunikacyjnych. Połączone rzeczy mają fizyczną lub wirtualną reprezentację w świecie cyfrowym, zdolność wykrywania/uruchamiania, funkcję programowalności i są jednoznacznie identyfikowalne. Reprezentacja ta zawiera informacje, w tym tożsamość, status, lokalizację lub wszelkie inne istotne informacje biznesowe, społeczne lub prywatne. Rzeczy oferują usługi, z interwencją człowieka lub bez, poprzez wykorzystanie unikalnej identyfikacji, przechwytywania danych i komunikacji oraz możliwości uruchamiania. Usługa jest wykorzystywana za pomocą inteligentnych interfejsów i jest udostępniana w dowolnym miejscu, o każdej porze i dla każdego, z uwzględnieniem bezpieczeństwa".
H. Minn, M. Zeng, V. Bhargava, *Towards a definition of the Internet of Things (IoT)*, „IEEE Internet Initiative" 2015, s. 74.

[134] M. Zioło, P. Niedzielski, E. Kuzionko-Ochrymiuk, J. Marcinkiewicz, K. Łobacz, K. Dyl, R. Szanter, *E-Government Development in European Countries: Socio-Economic and Environmental Aspects*, „Energies" 2022, 15, 8870.

[135] Inteligentne miasta – „przestrzeń, która wykorzystuje technologie informacyjno-komunikacyjne w celu zwiększenia interaktywności i wydajności infrastruktury miejskiej i jej komponentów składowych, a także do podniesienia świadomości mieszkańców. Miasto może być traktowane jako „inteligentne", gdy podejmuje inwestycje w kapitał ludzki i społeczny oraz infrastrukturę komunikacyjną, w celu aktywnego promowania zrównoważonego rozwoju gospodarczego i wysokiej jakości życia, w tym mądrego gospodarowania zasobami naturalnymi, przez partycypację obywatelską", *IoT w polskiej gospodarce. Raport Grupy Roboczej do spraw Internetu Rzeczy przy Ministerstwie Cyfryzacji*, Ministerstwo Cyfryzacji, Warszawa 2018, s. 33.

[136] R. Kour, R. Karim, A. Thaduri, *Cybersecurity for railways – A maturity model*, Proceedings of the Institution of Mechanical Engineers. Part F-Journal of Rail and Rapid Transit, 2019, Article Number: UNSP 0954409719881849.

[137] M. Lehto, J. Limnell, *Cyber Security Capability and the Case of Finland*, Proceedings of the 15th European Conference on Cyber Warfare and Security (Eccws 2016), 2016, s. 182–190.

t.j. Dz. U. z 2023 r., poz. 913 z późn. zm.) termin cyberbezpieczeństwo zdefiniowano jako: „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy". Jak określa to artykuł 3 powołanej ustawy, celem powstania krajowego systemu cyberbezpieczeństwa jest: „zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów". W wymienionej ustawie, powstałej i uchwalonej w wyniku wdrożenia dyrektywy Parlamentu Europejskiego i Rady Unii Europejskiej 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[138], definiując pojęcie cyberbezpieczeństwa, ustawodawca nie odwołuje się do pojęcia cyberprzestrzeni. W preambule wymienionej dyrektywy pojawia się termin cyberprzestrzeń, jednakże w tekście aktu nie podano jego definicji. Określenie: „Cyberprzestrzeń to przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[139], wraz z powiązaniami między nimi oraz relacjami z użytkownikami" zamieszczona jest w art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[140] oraz w innych ustawach[141]. Kwestia ewolucji pojęć „cyberbezpieczeństwo" i „cyberprzestrzeń" w polskim prawie została szerzej omówiona w pracy A. Szmit i M. Szmita „O normatywnych definicjach cyberbezpieczeństwa"[142].

[138] Dz. Urz. UE. L. z 2016 r. Nr 194.

[139] T.j. Dz. U. z 2024 r., poz. 307.

[140] T.j. Dz. U. z 2022 r., poz. 2091.

[141] Art. 2 ust. 1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j. Dz. U. z 2017 r., poz. 1928), art. 3 ust. 1 pkt 4 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (t.j. Dz. U. z 2017 r., poz. 1897), uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M. P. z 2019 r., poz. 1037).

[142] M. Szmit, A. Szmit, *O normatywnych definicjach cyberbezpieczeństwa*, [w:] K. Załęski, P. Polko (red.), *Bezpieczeństwo Polski w drugiej dekadzie XXI wieku*, Akademia WSB, Dąbrowa Górnicza 2019, s. 113–122.

W unijnym dokumencie[143] z 2019 r., zwanym aktem o cyberbezpieczeństwie, definiuje się je: „jako działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników tych systemów oraz innych osób przed cyberzagrożeniami", gdzie: „cyberzagrożenie oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób"[144].

Międzynarodowy Związek Telekomunikacyjny (ang. *International Telecommunication Union,* skrót: ITU)[145] definiuje cyberbezpieczeństwo jako „zbiór: narzędzi, polityk, koncepcji bezpieczeństwa, zabezpieczeń, wytycznych, podejść do zarządzania ryzykiem, działań, szkoleń, najlepszych praktyk, gwarancji i technik, które mogą być wykorzystane do ochrony środowiska cybernetycznego oraz organizacji i zasobów użytkownika"[146]. Według dokumentu ITU-T środowisko cybernetyczne: „obejmuje: użytkowników, sieci, urządzenia, całe oprogramowanie, procesy, informacje w trakcie przechowywania lub przesyłu, aplikacje, usługi i systemy, które mogą być podłączone bezpośrednio lub pośrednio do sieci"[147]. Amerykański Narodowy Instytut Standardów i Technik (ang. *National Institute of Standards and Technology,* skrót: NIST) definiuje cyberbezpieczeństwo jako: „zdolność do ochrony lub obrony działalności w cyberprzestrzeni przed cyberprzestępczością"[148]. Z kolei cyberprzestrzeń

[143] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie).

[144] Ibidem.

[145] Międzynarodowy Związek Telekomunikacyjny (skrót: ITU) jest wyspecjalizowaną agencją ONZ z siedzibą w Szwajcarii, założoną w 1865 r., która zajmuje się opracowywaniem i publikowaniem zaleceń dotyczących systemów radiowych (ITU-R), telekomunikacji (ITU-T) oraz pomocy na rzecz rozwoju (ITU-D). Odpowiedzialny jest również za przydzielanie globalnych częstotliwości radiowych i orbit satelitarnych.

[146] Recommendation ITU-T X.1205 (18 April 2008).

3.2.5 cybersecurity: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets, https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items, dostęp: 19.11.2020 r.

[147] Recommendation ITU-T X.1205 (18 April 2008).

3.2.4 cyber environment: This includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks,
https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items, dostęp: 19.11.2020 r.

[148] NIST: National Institute of Standards and Technology (2013). Security and privacy controls for federal information systems and organizations. NIST Special Publication, 800-53 Rev. 4 (Publikacja wycofana z serii technicznej NIST dnia 23.09.2021 r.). Cyber Security – The ability to protect or defend

określana jest jako: „globalna przestrzeń w środowisku informacyjnym składająca się z współzależnej sieci infrastruktur systemów informacyjnych, w tym Internetu, sieci telekomunikacyjnych, systemów komputerowych oraz wbudowanych procesorów i kontrolerów”[149]. Inna instytucja Stanów Zjednoczonych Ameryki – Komitet ds. Systemów Bezpieczeństwa Narodowego (ang. *Committee on National Security Systems,* skrót: CNSS) – definiuje cyberbezpieczeństwo jako: „zapobieganie szkodom, ochrona i przywracanie sprawności komputerów, systemów łączności elektronicznej, usług łączności elektronicznej, łączności przewodowej i łączności elektronicznej, w tym informacji w nich zawartych, w celu zapewnienia ich dostępności, integralności, uwierzytelniania, poufności i niezaprzeczalności”[150]; a cyberprzestrzeń jako: „współzależną sieć infrastruktury informatycznej, obejmującą Internet, sieci telekomunikacyjne, systemy komputerowe oraz wbudowane procesory i kontrolery w krytycznych branżach”[151].

W wymienionych przykładach definicji terminu „cyberbezpieczeństwo” można zauważyć, że jeżeli nie odwołują się one bezpośrednio do pojęcia „cyberprzestrzeń”, to w części zwanej *definiens* mówią o elementach tej przestrzeni, takich jak systemy informatyczne, informacje itd. Cyberbezpieczeństwo definiowane jest jako zbiór narzędzi lub działań, ale także jako stan lub posiadanie odpowiednich cech (np. odporność, zdolność).

Nie we wszystkich definicjach terminu „cyberprzestrzeń” wymieniony jest użytkownik jako element tej przestrzeni (np. w definicji NIST), definicje skupiają się na

---

the use of cyberspace from cyber attacks. Źródłem powyższej definicji jest dokument CNSSI No. 4009 w wersji z 2010 r., https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, s. 86, dostęp: 19.11.2020 r.

[149] NIST: National Institute of Standards and Technology (2013). Security and privacy controls for federal information systems and organizations. NIST Special Publication, 800-53 Rev. 4.

Cyberspace – A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers,

źródłem powyższej definicji jest dokument CNSSI No. 4009 w wersji z 2010 r.,

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, s. 86, dostęp: 19.11.2020 r.

[150] Glossary Committee on National Security Systems CNSSI No. 4009, kwiecień 2015.

Cybersecurity – Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation, https://www.cnss.gov/CNSS/issuances/Instructions.cfm, dostęp: 19.11.2020 r.

[151] Glossary Committee on National Security Systems CNSSI No. 4009, kwiecień 2015.

Cyberspace – The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries, https://www.cnss.gov/CNSS/issuances/Instructions.cfm, dostęp: 19.11.2020 r.

wykorzystywanej technice w cyberprzestrzeni. Według R. Solmsa i J. Niekerka[152] cyberbezpieczeństwo i bezpieczeństwo informacji w znacznym stopniu się pokrywają, ale te dwa pojęcia nie są całkowicie tożsame. Twierdzą, że cyberbezpieczeństwo wykracza poza granice tradycyjnego bezpieczeństwa informacji, ponieważ obejmuje nie tylko ochronę zasobów informacyjnych, ale również innych zasobów, w tym samej osoby. Ludzie są potencjalnymi celami ataków cybernetycznych, mogą być również nieświadomymi uczestnikami cyberataku. Ten dodatkowy wymiar ma konsekwencje etyczne dla całego społeczeństwa, ponieważ ochrona niektórych wrażliwych grup społecznych, na przykład dzieci czy osób chorych, może być postrzegana jako odpowiedzialność społeczna.

1.2.3. Systemy zarządzania bezpieczeństwem informacji

System zarządzania bezpieczeństwem informacji stanowi podsystem systemu zarządzania całą organizacją, stwierdzono związek pomiędzy bezpieczeństwem informacji a ładem organizacyjnym[153]. Pojęcie podsystemu wywodzi się z podejścia systemowego w teorii organizacji, gdzie podstawą jest uznanie całej organizacji za system i opisanie jej w kategoriach systemowych[154]. Siłą sprawczą pojawiania się kolejnych koncepcji i kierunków badawczych w teorii organizacji i zarządzania są potrzeby oraz wyzwania praktyki zarządzania organizacjami[155]. Jedną z ważniejszych koncepcji dla systemów zarządzania bezpieczeństwem informacji jest Business Process Reengineering (BPR). Jego twórcy, M. Hammer i J. Champy, zdefiniowali reengering jako: „fundamentalne przemyślenie od nowa i radykalne przeprojektowanie procesów w firmie prowadzące do przełomowej poprawy według krytycznych, współczesnych miar osiągania wyników (takich jak: koszty, jakość, serwis, szybkość)”[156]. Uważali oni, że zmiana sytuacji, jaka zaszła w II połowie XX w., wymagała od firm porzucenia dotychczasowych, wyuczonych sposobów działania.

W obszarze zagadnień związanych z zarządzaniem i jakością szczególną rolę pełnią najlepsze praktyki znormalizowane przez Międzynarodową Organizację

[152] R. von Solms, J. van Niekerk, *From information security to cyber security*, „Computers & Security” 2013, 38(0), s. 97–102.

[153] S. Al Ghamdi, K. Win, E. Vlahu-Gjorgievska, *Information security governance challenges and critical success factors: Systematic review*, „Computers and Security” 2020, Vol. 99.

[154] A.K. Koźmiński, D. Latusek-Jurczak, *Rozwój teorii organizacji. Od systemu do sieci*, Poltex, Warszawa 2017, s. 45.

[155] Ibidem.

[156] M. Hammer, J. Champy, *Reengineering w przedsiębiorstwie*, Neumann Management Institute, Warszawa 1996, s. 45–49.

Standaryzacyjną, która – między innymi – upowszechniła koncepcję wyodrębniania z całościowego systemu zarzadzania jego poszczególnych podsystemów, takich jak na przykład: system zarządzania jakością, system zarządzania środowiskowego, system zarządzania ciągłością działania czy system zarządzania bezpieczeństwem informacji (Załącznik 5. Standardy systemów zarządzania Międzynarodowej Organizacji Normalizacyjnej – ISO). Wspólną ich podstawą są: podejście probabilistyczne, opierające się na zarządzaniu ryzykiem, podejście systemowe, podejście procesowe czy wymóg ciągłego doskonalenia. W zbiorze dokumentów ITIL zauważa się konieczność istnienia w organizacji spójnej koncepcji (spójnego podejścia do zarządzania) w poszczególnych podsystemach zarządzania w celu uniknięcia powielania działań oraz koncentracji na głównych celach organizacji. Stwierdza się, że podsystemy zarządzania muszą ze sobą współdziałać, na przykład zarządzanie ciągłością usług informatycznych powinno być zbieżne z zarządzaniem ciągłością działania organizacji itp.[157]

W dysertacji używane jest pojęcie systemu zarządzania bezpieczeństwa informacji (ang. *Information Security Management System, skrót:* ISMS) w rozumieniu definicji zawartej w normie ISO/IEC 27000:2018-4.2.1. SZBI składa się z polityk, procedur, wytycznych oraz powiązanych zasobów i działań, które zapewniają organizacji możliwość osiągnięcia celów zarządzania bezpieczeństwem informacji. SZBI jest bazującym na szacowaniu ryzyka i poziomach akceptacji ryzyka systematycznym podejściem do: ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu utrzymania i doskonalenia bezpieczeństwa informacji i osiągnięcia założeń biznesowych. Podejście to zostało przyjęte przez wiele organizacji na całym świecie, ceniony jest również certyfikat zgodności ISMS z wymaganiami ISO/IEC 27001.

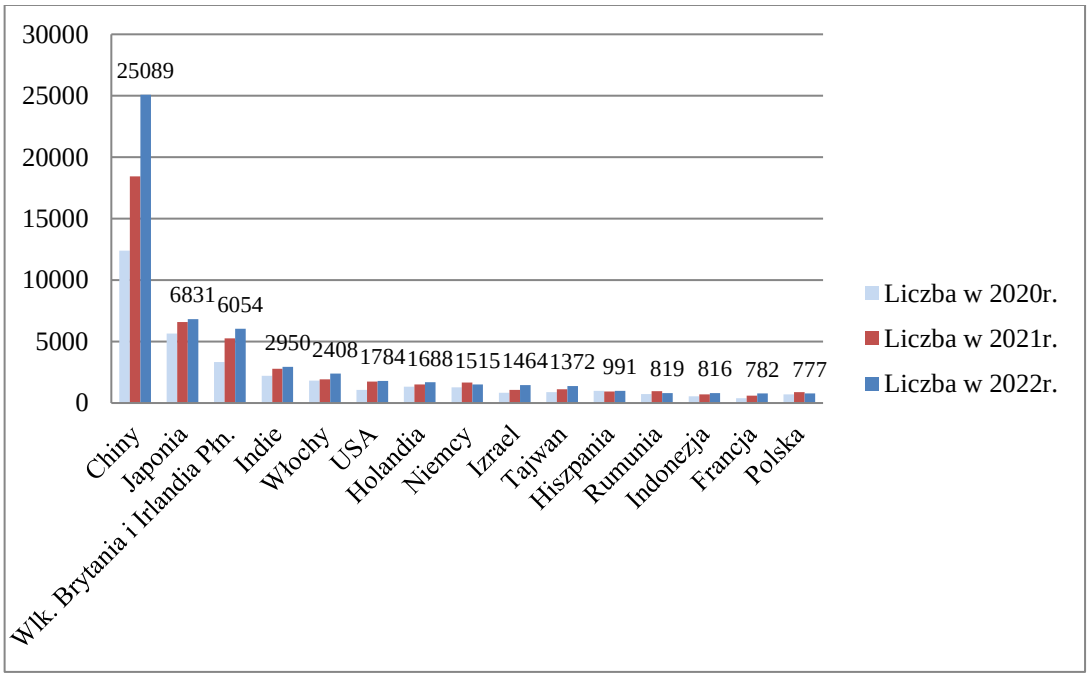
Według badaczy[158] głównym motywem, dla którego organizacje decydują się na dostosowanie zarządzania bezpieczeństwem informacji do normy, jest zwiększenie poziomu bezpieczeństwa informacji przez podnoszenie świadomości pracowników w zakresie bezpieczeństwa informacji oraz zmniejszenie ryzyka naruszeń bezpieczeństwa. Zauważają również, że dla organizacji z sektora ICT głównymi motywami są: wymagania interesariuszy, presja ze strony konkurencji, zdobywanie

[157] J. Clinch, „ITIL v3 and Information Security", Axelos Global Best Practices, May 2009, s. 7.

[158] M. Mirtsch, K. Blind, C. Koch, G. Dudek, *Information security management in ICT and non-ICT sector companies: A preventive innovation perspective*, „Computers & Security" 2021, Vol. 109, s. 1–23; M. Podrecca, G. Culot, G. Nassimbeni, M. Sartor, *Information security and value creation: The performance implications of ISO/IEC 27001*, „Computers in Industry" 2022, 142, 103744; M. Mirtsch, *Adoption of the information security management system standard ISO/IEC 27001: a study among German organizations*, „International Journal for Quality Research" 2023, 17(3), s. 747–768.

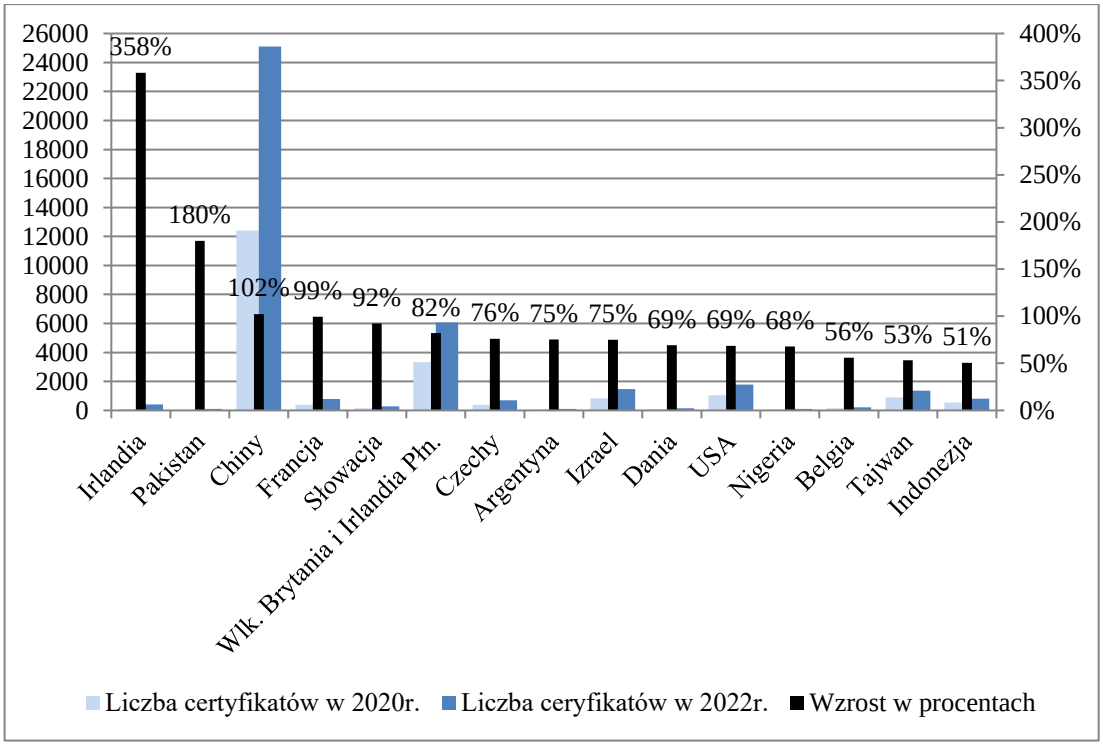
dostępu do rynku i poprawa swojego wizerunku, czyli brane są pod rozwagę korzyści ekonomiczne. Głównym powodem uzyskania certyfikatów ISO/IEC 27001 przez organizacje spoza sektora ICT jest zapewnienie zgodności z obowiązującymi regulacjami prawnymi.

W Polsce w 2022 r. zarejestrowanych było 777 ważnych certyfikatów ISO/IEC 27001. Ważny certyfikat to taki, który został wydany przez jednostkę certyfikacyjną akredytowaną przez jednego z członków międzynarodowego porozumienia między jednostkami akredytującymi w sprawie wzajemnego uznawania akredytacji IAF (ang. *International Accreditation Forum*) MLA (ang. *Multilateral Recognition Arrangements*) w roku przeglądu lub w ciągu dwóch poprzedzających go lat. W załączniku nr 4 zebrano informacje o liczbie certyfikatów zgodności z wymaganiami normy ISO/IEC 27001:2013 w poszczególnych krajach w latach 2020–2022. Najwięcej organizacji posiadających certyfikat w 2022 r. pochodziło z Chin. Polska znalazła się wśród piętnastu państw z największą liczbą aktualnych certyfikatów – Rysunek 1.5.



Rysunek 1.5. Piętnaście państw z największą liczbą aktualnych certyfikatów zgodności ISMS z wymaganiami ISO/IEC 27001:2013 w 2022 r.
Źródło: opracowanie własne na podstawie danych zawartych na stronie internetowej https://www.iso.org/the-iso-survey.html, ***dostęp****: 4.04.2024 r.*

Irlandia jest państwem, w którym nastąpił w 2022 r. największy przyrost liczby certyfikatów zgodności ISMS z wymaganiami ISO/IEC 27001:2013 w stosunku do liczby certyfikatów w 2020 r. – Rysunek 1.6. W Polsce w tym okresie nastąpił dziewięcioprocentowy wzrost certyfikatów: z 710 w 2020 r. do 777 w 2022 r.



Rysunek 1.6. Piętnaście państw z największym wzrostem liczby aktualnych certyfikatów zgodności ISMS z wymaganiami ISO/IEC 27001:2013 do roku 2022 (po usunięciu z zestawienia państw z ogólną liczbą certyfikatów poniżej 20)
Źródło: opracowanie własne na podstawie danych zawartych na stronie internetowej https://www.iso.org/the-iso-survey.html, dostęp: 4.04.2024 r.

Krajową jednostką akredytującą upoważnioną do akredytacji jednostek oceniających zgodność ISMS z wymogami ISO/IEC 27001 jest Polskie Centrum Akredytacji (PCA), którego ramy działania określa ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r., poz. 1854). Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającym wymagania w zakresie akredytacji i nadzoru rynku odnoszącym się do warunków wprowadzania produktów do obrotu PCA zostało wskazane jako jedyna krajowa jednostka akredytująca. Na dzień 4 kwietnia 2024 r. czternaście podmiotów w Polsce[159] posiada ważny certyfikat akredytacji systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001. Podmioty te mają również możliwość wydawania certyfikatów dla innych systemów zarządzania, np. dla Systemu Zarządzania Jakością ISO 9001.

Normy ISO dotyczące systemów zarządzania są opracowane tak, aby wspierać wspólne wdrożenie i eksploatację, charakteryzuje je podejście procesowe oraz posiadają

[159] https://www.pca.gov.pl/akredytowane-podmioty/akredytacje-aktywne/jednostki-certyfikujace-systemy/, dostęp: 4.04.2024 r.

one spójne zasady nadzorowania dokumentów, prowadzenia audytów i definiowania działań korygujących oraz zapobiegawczych. We wprowadzeniu do ISO/IEC 27001:2022 znajduje się zalecenie, aby SZBI był zintegrowany z innymi systemami zarządzania w organizacji, oraz oświadczenie, iż w tej normie zastosowano strukturę dokumentu, tytuły podrozdziałów, wspólne terminy oraz podstawowe definicje określone w Załączniku SL do dyrektyw ISO/IEC, Część 1, Skonsolidowany Suplement ISO – Procedury specyficzne dla ISO[160]. W wyniku czego zachowano zgodność z innymi normami dotyczącymi systemów zarządzania, co jest ułatwieniem dla członków organizacji wdrażających SZBI. Przedstawione standardy wspierają zarządzanie i pełnienie funkcji kierowniczych na wszystkich poziomach. Normy te mają zastosowanie w organizacjach rozmaitych typów i wielkości oraz w różnych warunkach kulturowych i społecznych. Aby organizacja mogła uzyskać certyfikat zgodności ISMS z normą ISO/IEC 27001, potrzebuje dowodów, że spełnia jej wymagania. Takie gromadzenie dowodów odbywa się poprzez przeprowadzenie audytu[161] zewnętrznego przez podmiot akredytowany.

Badania[162] wykazały, że formalizacja wymagana przez normę ISO 27001 może spowodować nadmierną biurokrację i potencjalną utratę elastyczności, co ostatecznie może wpłynąć negatywnie na wydajność certyfikowanych organizacji. Badane organizacje postrzegały wdrożenie normy jako kosztowne w porównaniu z innymi

[160] ISO/IEC Directives Part 1 and Consolidated ISO Supplement – Procedures specific to ISO (tłum. PKN: Dyrektywy ISO/IEC, Część 1, Skonsolidowany Suplement ISO – Procedury specyficzne dla ISO) 13th edition, 2022 – Oficjalne procedury, które należy przestrzegać przy opracowywaniu i utrzymywaniu Międzynarodowej Normy oraz procedury specyficzne dla ISO, https://www.iso.org/sites/directives/current/consolidated/index.xhtml, dostęp: 17.06.2022 r.

[161] Audyt – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów audytu i obiektywnej ich oceny w celu ustalenia stopnia spełnienia kryteriów audytu.

Uwaga 1: Audyt może być audytem wewnętrznym (pierwsza strona) lub audytem zewnętrznym (strona druga lub trzecia), może to być audyt łączony (łączący dwie lub więcej dyscyplin).

Uwaga 2: Audyt wewnętrzny przeprowadza sama organizacja lub w jej imieniu strona zewnętrzna.

Uwaga 3: „Dowody audytu" i „kryteria audytu" są zdefiniowane w normie ISO 19011.

Tłumaczenie własne definicji: ISO/IEC 27000:2018-3.3. audit – „systematic, independent and documented process (3.54) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the organization itself, or by an external party on its behalf.

Note 3 to entry: „Audit evidence" and „audit criteria" are defined in ISO 19011".

[162] A. Annarelli, F. Nonino, G. Palombi, *Understanding the management of cyber resilient systems*, Computers & Industrial Engineering, 2020, Vol. 149, 106829; R. van Wessela, X. Yangb, H.J. de Vriesa, *Implementing international standards for Information Security Management in China and Europe: A comparative multi-case study*, Technology Analysis & Strategic Management, 2011, Vol. 23/8, s. 865–879.

wydatkami na IT. Jednakże z badań[163] wynika, że korzyści z zastosowania normy ISO/IEC 27001 przewyższają potencjalne wady, a efekty poprawy wydajności procesów przesunięte są w czasie. Badacze zajmujący się bezpieczeństwem informacji w organizacji wskazują na pozytywny związek pomiędzy posiadaniem certyfikatu ISO 27001 a wydajnością procesów związanych z zarządzaniem bezpieczeństwem informacji i wynikami finansowymi w organizacji.

W normach oraz metodykach dotyczących systemów zarządzania bezpieczeństwem informacji, jak i w literaturze przedmiotu[164], stwierdzono, że w coraz większym zakresie organizacje muszą zajmować się kwestiami związanymi z bezpieczeństwem informacji. Wynika to z konieczności zapewnienia bezpiecznej realizacji procesów biznesowych lub specjalistycznych zadań z wykorzystaniem technik informatycznych – zarówno w trybie offline, jak i online.

Różne podmioty podjęły się zadania opracowania standardów zarządzania bezpieczeństwem informacji oraz zbiorów najlepszych praktyk w tym zakresie. Należą do nich: Międzynarodowa Organizacja Normalizacyjna (ang. *International Organization for Standardization*) i Międzynarodowa Komisja Elektrotechniczna (ang. *International Electrotechnical Commission*), Federalny Urząd ds. Bezpieczeństwa Informacji w Niemczech (niem. *Bundesamt für Sicherheit in der Informationstechnik*, skrót: BSI), Narodowy Instytut Standardów i Technik (ang. *National Institute of Standards and Technology*, skrót: NIST). Oprócz standardów krajowych, takich jak seria NIST SP 800 w USA czy wytyczne bezpieczeństwa IT Federalnego Urzędu ds. Bezpieczeństwa Informacji w Niemczech, istnieją opracowania w zakresie tworzenia i funkcjonowania systemu zarządzania bezpieczeństwem informacji wykorzystywane w rozmaitych organizacjach działających w różnych krajach. Wiele źródeł[165] uznaje

[163] M. Podrecca, G. Culot, G. Nassimbeni, M. Sartor, op. cit., s. 9; A. Annarelli, F. Nonino, G. Palombi, op. cit.; R. van Wessela, X. Yangb, H.J. de Vriesa, op. cit.

[164] BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-1-Managementsysteme-fuer-Informationssicherheit/bsi-standard-200-1-managementsysteme-fuer-informationssicherheit_node.html, s. 5, dostęp: 20.09.2021 r.; X.Y. Ge, Y.Q. Yuan, L.L. Lu, *An information security maturity evaluation mode*, Procedia Engineering, 2011, 24, s. 335.

[165] M.G. Pinheiro, M. Misaghi, *Proposal of a Framework of Lean Governance and Management of Enterprise IT*, Proceedings of the 16th International Conference on Information Integration and Web-Based Applications & Services – IiWAS '14, 2014, s. 554–558; C. Calvache, M. Piattini, F. Garcia, F. Pino, M. Baldassarre, *A 360-degree process improvement approach based on multiple models*, „Revista Facultad de Ingenieria", 2015, Vol. 1(77), s. 95–105; European Union Agency For Network And Information Security, *Definition of Cybersecurity – Gaps and overlaps in standardisation v1.0*, 2015, s. 23; M. Stoll, *An Information Security Model for Implementing the New ISO 27001*, [w:] Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications, edited by Information

ISO 27k za najszerzej akceptowany standard bezpieczeństwa informacji obok takich inicjatyw, jak COBIT i ITIL.

1.2.4. Rodzina norm ISO/IEC 27k

Międzynarodowa Organizacja Normalizacyjna (ang. skrót: ISO) i Międzynarodowa Komisja Elektrotechniczna (ang. skrót: IEC) utworzyły wspólny komitet techniczny – ISO/IEC JTC 1. W ramach podkomitetu SC 27 działa grupa robocza WG 1, która zajmuje się opracowywaniem i wprowadzaniem międzynarodowych standardów dla systemów zarządzania bezpieczeństwem informacji. Normy dotyczące ISMS mają zastosowanie do wszystkich typów i rozmiarów organizacji oraz są często przywoływane w literaturze przedmiotu[166]:

1. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary (tłumaczenie PKN: ISO/IEC 27000:2018 Technika informatyczna — Techniki bezpieczeństwa — Systemy zarządzania bezpieczeństwem informacji — Przegląd i terminologia).

Zawiera wprowadzenie do systemów zarządzania bezpieczeństwem informacji, podstawowe terminy i definicje oraz przegląd rodziny norm dotyczących ISMS.

2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements (tłumaczenie własne: ISO/IEC 27001:2022 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności — Systemy zarządzania bezpieczeństwem informacji – Wymagania).

ISO/IEC 27001:2022 jest podstawową normą w rodzinie norm 27k. Przedstawia wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji. Według normy przyjęcie SZBI jest decyzją strategiczną dla organizacji. Na jego ustanowienie i wdrożenie w organizacji mają wpływ: jej potrzeby oraz cele, wymagania dotyczące bezpieczeństwa, stosowane procesy, wielkość i struktura organizacji. SZBI przyczynia się do zachowania

Resources Management Association, IGI Global, 2019, s. 219–242; M. Podrecca, G. Culot, G. Nassimbeni, M. Sartor, op. cit., s. 9; R. van Wessela, X. Yangb, H. J. de Vriesa, *Implementing international standards for Information Security Management in China and Europe: A comparative multi-case study*, „Technology Analysis & Strategic Management" 2011, Vol. 23/8, s. 865–879.

[166] G. Culot, G. Nassimbeni, M. Podrecca, M. Sartor, *The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda*, „The TQM Journal", 2021, Vol. 33, s. 76–105.

poufności, integralności i dostępności informacji poprzez zastosowanie procesu zarządzania ryzykiem oraz daje pewność interesariuszom, że ryzyko jest odpowiednio zarządzane. W dokumencie zwraca się uwagę na konieczność integracji SZBI z innymi systemami zarządzania, występującymi w organizacji[167]. Wymaga się, aby bezpieczeństwo informacji było uwzględniane przy projektowaniu nowych procesów, systemów informacyjnych i zabezpieczeń. Wymagania są sformułowane w sposób ogólny, tak aby pasowały do wszystkich organizacji, niezależnie od ich wielkości, celów, modelu biznesowego czy lokalizacji.

W załączniku normatywnym (Rysunek 1.7) wymieniono 93 zabezpieczenia (ang. *controls*)[168], które to zmniejszają ryzyko związane z bezpieczeństwem informacji. Zaleca się, aby decyzję o wyborze zabezpieczeń podjąć po przeprowadzonej ocenie ryzyka. Wybór zabezpieczeń powinien również uwzględniać dotyczące organizacji przepisy i regulacje krajowe czy międzynarodowe.

Zabezpieczenia podzielone są na:

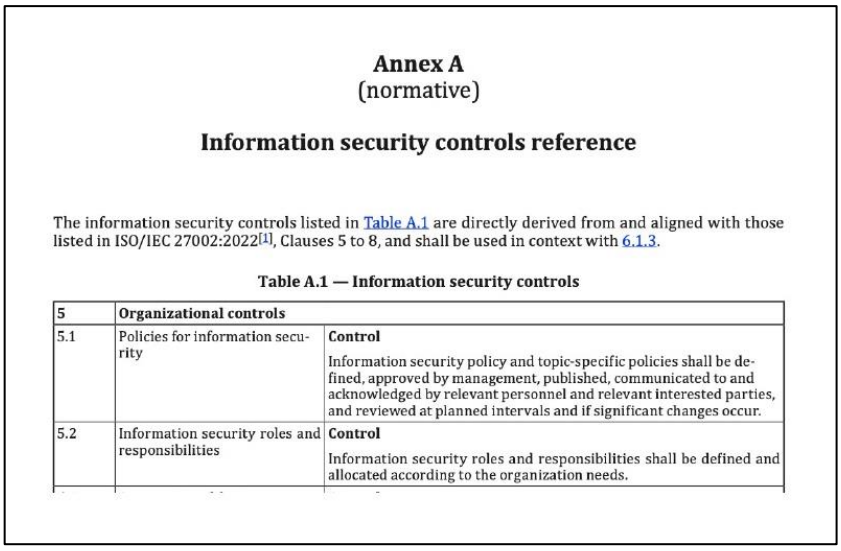
a) ludzkie, jeśli dotyczą osób,
b) fizyczne, jeśli dotyczą obiektów fizycznych,
c) techniczne, jeśli dotyczą wykorzystywanych technik,
d) organizacyjne.

[167] ISO/IEC 27001:2022-0.1; N. Góra, *Zintegrowane systemy zarządzania w ujęciu teoretyczno-praktycznym*, Management and Quality, 2021, t. 3, nr 2, s. 7–19.

[168] ISO/IEC 27000:2018 3.14 „zabezpieczenie – środek, który modyfikuje ryzyko.

Uwaga 1: Zabezpieczenia obejmują procesy, politykę, urządzenia, praktyki lub inne działania modyfikujące ryzyko.

Uwaga 2: Zabezpieczenia nie zawsze wywierają zamierzony wpływ" (tłumaczenie PN-ISO/IEC 27000:2014-11-2.16).



Annex A
(normative)

Information security controls reference

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022[1], Clauses 5 to 8, and shall be used in context with 6.1.3.

Table A.1 — Information security controls

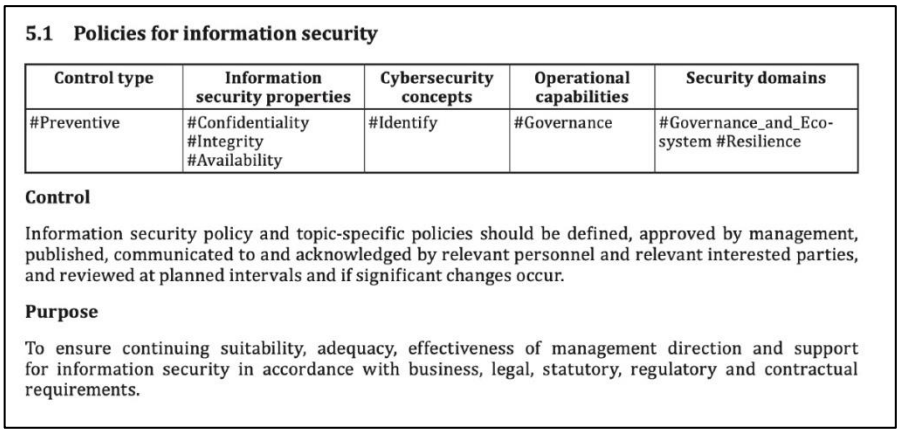
5	Organizational controls	
5.1	Policies for information security	**Control** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
5.2	Information security roles and responsibilities	**Control** Information security roles and responsibilities shall be defined and allocated according to the organization needs.

Rysunek 1.7. Przykład zabezpieczeń organizacyjnych zawartych w załączniku do normy ISO/IEC 27001:2022
Źródło: ISO/IEC 27001:2022, s. 11.

Każde zabezpieczenie opisane jest pięcioma atrybutami (Rysunek 1.8)[169]:

1) Typ zabezpieczenia (prewencyjny, wykrywający, korygujący).
2) Właściwości bezpieczeństwa informacji (poufność, integralność, dostępność).
3) Koncepcje cyberbezpieczeństwa (identyfikacja, ochrona, wykrywanie, reagowanie i odzyskiwanie).
4) Zdolności operacyjne – atrybut umożliwiający przeglądanie zabezpieczeń z perspektywy praktyka. Przykładowe wartości atrybutu: ład, zarządzanie zasobami, bezpieczeństwo, bezpieczeństwo aplikacji, bezpieczeństwo konfiguracji.
5) Domeny bezpieczeństwa (ład i ekosystem, ochrona, obrona, odporność).

[169] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, s. 8.



5.1 Policies for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

Control

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.

Rysunek 1.8. Przykład opisania zabezpieczenia w normie ISO/IEC 27002:2022
Źródło: ISO/IEC 27002:202, s. 9.

3. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls (tłumaczenie własne: ISO/IEC 27002:2022 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności — Zabezpieczenia bezpieczeństwa informacji).

Norma ta wspiera w wyborze i we wdrażaniu zabezpieczeń opisanych w ISO/IEC 27001 w celu ustanowienia działającego systemu zarządzania bezpieczeństwem informacji i osadzenia go w organizacji. Stanowi zestaw referencyjny zabezpieczeń. Zawarte w niej zalecenia przeznaczone są przede wszystkim dla kadry zarządzającej. Wdrożenie zaleceń dotyczących bezpieczeństwa zawartych w normie ISO/IEC 27002 jest jedną z możliwości spełnienia wymagań normy ISO/IEC 27001.

4. ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation (tłumaczenie PKN: ISO/IEC 27004:2016 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie bezpieczeństwem informacji – Monitorowanie, pomiary, analiza i ocena).

Norma ISO/IEC 27004:2016 zawiera wytyczne mające na celu pomoc organizacjom w ocenie działania w zakresie bezpieczeństwa informacji oraz skuteczności systemu zarządzania bezpieczeństwem informacji. Wskazuje możliwości monitorowania i pomiaru skuteczności systemu zarządzania bezpieczeństwem informacji, w tym jego procesów i mechanizmów kontrolnych.

5. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks (tłumaczenie własne: ISO/IEC 27005:2022 Bezpieczeństwo informacji,

cyberbezpieczeństwo i ochrona prywatności — Wytyczne zarządzania ryzykiem w bezpieczeństwie informacji).

Norma ta zawiera ramowe zalecenia dotyczące zarządzania ryzykiem w zakresie bezpieczeństwa informacji. Między innymi wspiera wdrażanie zaleceń z normy ISO/IEC 27001. Nie określa jednak konkretnej metody zarządzania ryzykiem. Norma ta jest głównie oparta na normie ISO 31000:2018 Risk management — Guidelines (tłumaczenie PKN: ISO 31000:2018 Zarządzanie ryzykiem – Wytyczne).

1.2.5. Seria NIST SP 800

Amerykański Narodowy Instytut Standaryzacji i Technologii jest agencją federalną odpowiedzialną m.in. za opracowywanie standardów, które są wiążące dla agencji rządowych USA. W specjalnej serii publikacji 800[170] (ang. *NIST SP 800 series*) NIST regularnie publikuje dokumenty dotyczące poszczególnych tematów z zakresu bezpieczeństwa informacji (kryptografia, cloud computing itp.). Seria, wydawana od 1990 r., obejmuje: wytyczne, zalecenia, specyfikacje techniczne i roczne raporty z działalności NIST. Publikacje zawierają również informacje z działań w zakresie współpracy pomiędzy przemysłem, rządem i organizacjami akademickimi. Wydawane przez NIST dokumenty są wykorzystywane przez międzynarodową społeczność osób odpowiedzialnych za bezpieczeństwo informacji w organizacjach[171].

Jedna z publikacji – „SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations" (tłumaczenie własne: „Mechanizmy kontroli bezpieczeństwa i prywatności dla systemów informacyjnych i organizacji") – zawiera katalog mechanizmów kontroli bezpieczeństwa i ochrony prywatności dla systemów informatycznych i organizacji w celu ochrony: działań oraz aktywów organizacji, osób, innych organizacji i narodu przed różnorodnymi zagrożeniami i ryzykiem, w tym: wrogimi atakami, błędami ludzkimi, katastrofami naturalnymi, awariami strukturalnymi, działaniami obcych wywiadów oraz ryzykiem związanym z ochroną prywatności. Zawarte w dokumencie mechanizmy kontrolne są elastyczne i można je dostosować do potrzeb każdej jednostki oraz mogą być wdrażane jako część ogólnoorganizacyjnego procesu zarządzania ryzykiem. Dotyczą różnorodnych wymagań wynikających z: misji i potrzeb biznesowych, rozporządzeń, dyrektyw,

[170] https://csrc.nist.gov/publications/sp800, dostęp: 21.09.2021 r.

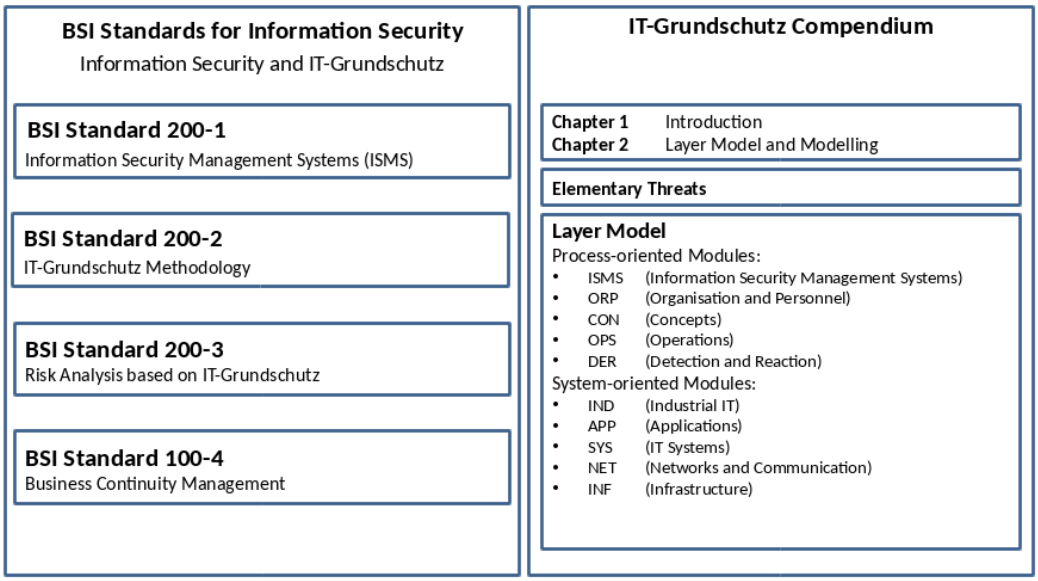
[171] https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information, dostęp: 21.09.2021 r.

regulacji, polityk, standardów i wytycznych. Skonsolidowany katalog mechanizmów kontrolnych odnosi się do bezpieczeństwa i prywatności z uwzględnieniem funkcjonalności i wiarygodności tych mechanizmów.

W celu pomocy organizacjom w poznaniu zbieżności i rozbieżności w stosowaniu środków kontrolnych, przedstawionych w różnych publikacjach, NIST opublikował dokumenty zawierające mapowania 800-53 Rev. 5 na inne ramy i standardy: NIST Cybersecurity Framework i NIST Privacy Framework; ISO/IEC 27001[172].

1.2.6. Normy BSI

IT-Grundschutz (tłumaczenie własne: IT – ochrona podstawowa) jest metodyką organu rządu federalnego odpowiedzialnego za bezpieczeństwo w cyberprzestrzeni oraz za kształtowanie bezpiecznej cyfryzacji w Niemczech (Bundesamt für Sicherheit in der Informationstechnik, skrót: BSI). Rozwijana jest ona od 1994 r. Charakteryzuje się holistycznym podejściem do wdrażania rozwiązań dotyczących bezpieczeństwa informacji. Dzięki podziałowi na podejścia podstawowe, standardowe i kluczowe do zabezpieczeń IT-Grundschutz oferuje możliwość dostosowania zabezpieczeń dotyczących bezpiecznego przetwarzania informacji dla każdego typu i wielkości organizacji. Rysunek 1.9 ilustruje strukturę dokumentów IT-Grundschutz.



Rysunek 1.9. Struktura dokumentów IT-Grundschutz
Źródło: BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-1-Managementsysteme-fuer-Informationssicherheit/bsi-standard-200-1-managementsysteme-fuer-informationssicherheit_node.html, s. 5, dostęp: 20.09.2021 r.

[172] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final, dostęp: 21.09.2021 r.

Seria norm BSI, dotyczących bezpieczeństwa informacji, składa się z norm:

200-1 Systemy zarządzania bezpieczeństwem informacji (ISMS)

Norma definiuje ogólne wymagania dla ISMS. Opisano w niej, jakie zabezpieczenia mogą być stosowane do ogólnego inicjowania, kontrolowania i monitorowania bezpieczeństwa informacji w organizacji. Norma BSI 200-1 jest całkowicie zgodna z normą ISO/IEC 27001, a ponadto uwzględnia terminy zdefiniowane w normie ISO/IEC 27000 oraz zalecenia zawarte w normie ISO/IEC 27002.

200-2 Metodyka IT-Grundschutz

Metodyka IT-Grundschutz wyjaśnia, w jaki sposób system zarządzania bezpieczeństwem informacji może być ustanowiony i stosowany w praktyce. Ważnymi tematami w tym zakresie są zadania związane z zarządzaniem bezpieczeństwem informacji oraz projekt struktury organizacyjnej dla bezpieczeństwa informacji. Metodyka IT-Grundschutz omawia, w jaki sposób w praktyce można opracować politykę bezpieczeństwa, jak wybrać odpowiednie wymagania bezpieczeństwa oraz na co należy zwrócić uwagę przy wdrażaniu polityki bezpieczeństwa, wskazuje również, jak utrzymać i poprawić bezpieczeństwo informacji.

Opierając się na normie BSI 200-2, IT-Grundschutz interpretuje ogólne wymagania bezpieczeństwa wyżej wymienionych norm ISO 27001 i 27002 oraz wspiera użytkowników w praktycznej implementacji poprzez dostarczanie informacji ogólnych i przykładów.

200-3 Analiza ryzyka na podstawie IT-Grundschutz

BSI opracowało metodę analizy ryzyka na podstawie IT-Grundschutz. Norma BSI 200-3 opisuje, w jaki sposób na bazie metodyki IT-Grundschutz można przeprowadzić uproszczoną analizę ryzyka dla przetwarzania informacji.

100-4 Zarządzanie ciągłością działania

W normie BSI 100-4 wyjaśniona jest metoda tworzenia i utrzymywania zarządzania ciągłością działania w całej organizacji.

Kompendium IT-Grundschutz[173] zawiera moduły procesowe z następujących obszarów i warstw:

[173] *IT-Grundschutz-Compendium*, Federal Office for Information Security (BSI), Bonn, Germany 2022.

– ISMS: systemy zarządzanie bezpieczeństwem informacji,
– ORP: organizacja i personel,
– CON: koncepcje i podejścia (np. koncepcja kryptograficzna, rozwój oprogramowania),
– OPS: operacje (np. ochrona przed złośliwym oprogramowaniem, cloud computing),
– DER: wykrywanie i reagowanie (zarządzanie incydentami, zarządzanie ciągłością działania).

Ponadto kompendium IT-Grundschutz zawiera następujące moduły systemowe:

– INF: infrastruktura (np. budynki, centrum komputerowe),
– SYS: systemy informatyczne (np. serwery, klienci),
– NET: sieci i komunikacja (np. architektura oraz projektowanie sieci),
– APP: aplikacje (np. poczta elektroniczna i przeglądarka),
– IND: informatyka przemysłowa (np. technologia operacyjna i kontrolna oraz centrum kontroli).

Każdy moduł zawiera krótki opis tematu i celu, który ma być osiągnięty poprzez jego wdrożenie oraz przegląd specyficznych dla tematu zagrożeń. Wymagania bezpieczeństwa dla zabezpieczeń podstawowych, standardowych i kluczowych tworzą rdzeń każdego modułu. Wymagania dla modułu ISMS, dotyczącego zarządzania bezpieczeństwem, rozpoczynają się od określenia odpowiedzialności za wdrażanie i utrzymanie rozwiązań. Według kompendium IT-Grundschutz za spełnienie wymagań odpowiada Dyrektor ds. Bezpieczeństwa Informacji (ang. *Chief Information Security Office*r, skrót: CISO), ważną rolę pełnią również najwyższe kierownictwo i bezpośredni przełożeni.

Na podstawie kompendium w module ISMS w każdej organizacji w trybie priorytetowym powinny zostać spełnione następujące podstawowe wymagania:

ISMS.1.A1 Przyjęcie ogólnej odpowiedzialności za bezpieczeństwo informacji przez najwyższe kierownictwo.

ISMS.1.A2 Zdefiniowanie celów i strategii.

ISMS.1.A3 Opracowanie polityki bezpieczeństwa.

ISMS.1.A4 Powołanie Dyrektora ds. Bezpieczeństwa Informacji.

ISMS.1.A5 Podpisanie umowy z zewnętrznym Dyrektorem ds. Bezpieczeństwa Informacji, jeżeli roli CISO nie może odgrywać pracownik.

ISMS.1.A6 Utworzenie odpowiedniej struktury organizacyjnej ds. bezpieczeństwa informacji.

ISMS.1.A7 Definicja zabezpieczeń dla wszystkich aspektów przetwarzania informacji.

ISMS.1.A8 Włączenie wszystkich pracowników w proces bezpieczeństwa.

ISMS.1.A9 Zintegrowanie bezpieczeństwa informacji z procedurami i procesami obowiązującymi w całej organizacji.

W kompendium IT-Grundschutz zaleca się, aby wymagania standardowe również były wdrażane we wszystkich organizacjach:

ISMS.1.A10 Opracowanie koncepcji bezpieczeństwa dla każdego zakresu (domeny) informacji.

ISMS.1.A11 Zapewnienie ciągłości bezpieczeństwa informacji w organizacji.

ISMS.1.A12 Raportowanie najwyższemu kierownictwu o stanie bezpieczeństwa informacji.

ISMS.1.A13 Udokumentowanie procesu bezpieczeństwa.

ISMS.1.A14 (Wymóg został wyeliminowany).

ISMS.1.A15 Opłacalne wykorzystanie zasobów na rzecz bezpieczeństwa informacji.

Ostatnią grupą są wymagania w przypadku zwiększonych potrzeb organizacji w zakresie bezpieczeństwa informacji. Wybór wymagań powinien odbywać się na podstawie przeprowadzonej analizy ryzyka.

ISMS.1.A16 Tworzenie polityk bezpieczeństwa zorientowanych na grupę docelową.

ISMS.1.A17 Zawarcie ubezpieczenia od ryzyk rezydualnych.

1.2.7. Dobre praktyki biblioteki ITIL

ITIL (ang. *IT Infrastructure Library*) to zbiór dobrych praktyk dotyczących zarządzania usługami IT[174], w tym również zarządzania bezpieczeństwem informacji[175].

[174] Definicja terminu „usługa" (ang. *service*) – usługa to sposób dostarczania wartości odbiorcy poprzez umożliwienie mu uzyskania oczekiwanych przez niego wyników. Odbiorca nie bierze na siebie specyficznych kosztów i ryzyk powiązanych z dostarczaniem usługi. Termin usługa używany jest czasem jako synonim usługi podstawowej, usługi informatycznej lub pakietu usług.

Definicja terminu „usługa IT/usługa informatyczna" (ang. *IT service*) – usługa świadczona przez dostawcę usług informatycznych. Usługa informatyczna składa się z połączenia technologii informatycznych, ludzi i procesów. Zorientowana jest na odbiorcę i bezpośrednio wspiera procesy biznesowe jednego lub więcej odbiorców. Docelowy poziom świadczenia usług powinien być zdefiniowany w umowie SLA (ang. *service level agreement* – umowa o gwarantowanym poziomie świadczenia usług). Inne usługi informatyczne, zwane usługami wspierającymi, nie są bezpośrednio wykorzystywane przez organizację biznesową, ale są wymagane przez dostawcę usług do dostarczenia usług zorientowanych na odbiorcę.

Został on opracowany w latach 80. XX w. przez brytyjskie Office of Government Commerce (OGC) w celu zwiększenia wydajności tych usług, podniesienia jakości i zmniejszenia nakładów finansowych. ITIL zajmuje się zarządzaniem usługami informatycznymi (ang. *Information Technology Service Management*, skrót: ITSM) z punktu widzenia dostawcy usług informatycznych. Dostawcą usług IT może być zarówno wewnętrzny dział IT, jak i zewnętrzny dostawca. Wersja druga biblioteki została udostępniona w 2000 r., wersja trzecia w 2007 r. Na kanwie ITIL wydano normę ISO/IEC 20000, która może być podstawą do certyfikacji systemu zarządzania usługami. Ostatnia aktualizacja ITIL miała miejsce w 2019 r.

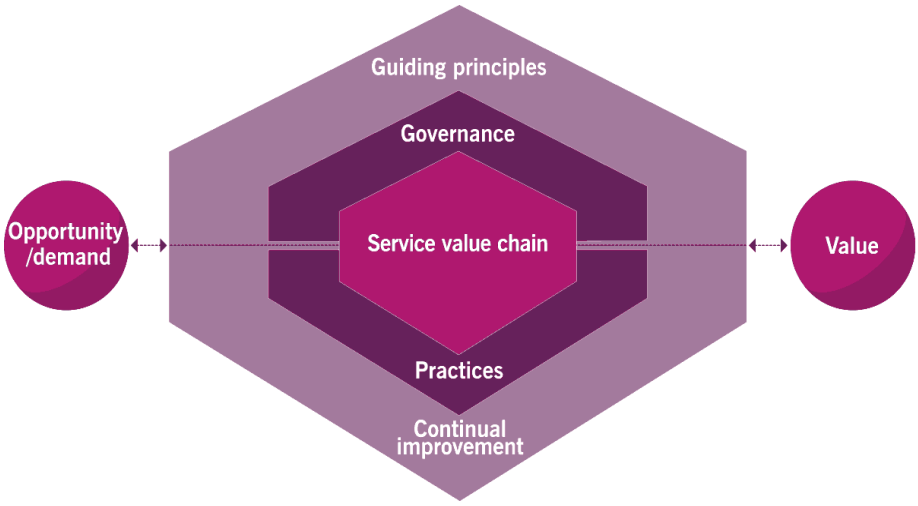
Usługa, zgodnie z definicją ITIL, to akt „dostarczania wartości odbiorcy". W ostatniej wersji biblioteki odbiorca, obok dostawcy, zaczął odgrywać ważną rolę w tworzeniu usługi. Wartość jest współtworzona poprzez aktywną współpracę pomiędzy dostawcami i odbiorcami. ITIL 4 zaleca, aby dostawcy dążyli do ustanowienia wzajemnie korzystnych, interaktywnych relacji z ich odbiorcami, upoważniając ich do bycia kreatywnymi współpracownikami[176].

Kluczowym elementem ITIL 4 jest system wartości usług (ang. *Service Value System,* skrót SVS), który ma umożliwiać koordynację i integrację elementów oraz działań organizacyjnych w celu tworzenia wartości (Rysunek 1.10).

Źródło powyższych definicji: Polski glosariusz ITIL®, wersja 1.0, z dnia 15 grudnia 2011 oparty na angielskim glosariuszu, wersja 1.0, z dnia 29 lipca 2011 r. Glosariusz ITIL® wraz ze skrótami Polski, s. 72, 114.

[175] K. Haufe, R. Colomo-Palacios, S. Dzombeta, K. Brandis, V. Stantchev, *A process framework for information security management*, „International Journal of Information Systems and Project Management" 2016, 4, s. 27; J. Clinch, *ITIL v3 and Information Security*, *Axelos Global Best Practices*, May 2009, s. 5; H. Susanto, M. Nabil Almunawar, Y. Tuan, *Information Security Management System Standards: A Comparative Study of the Big Five*, „International Journal of Engineering and Computer Science" 2011, 11, s. 23.

[176] ITIL® Foundation, ITIL 4 edition. Norwich: TSO (The Stationery Office), 2019, s. 4.



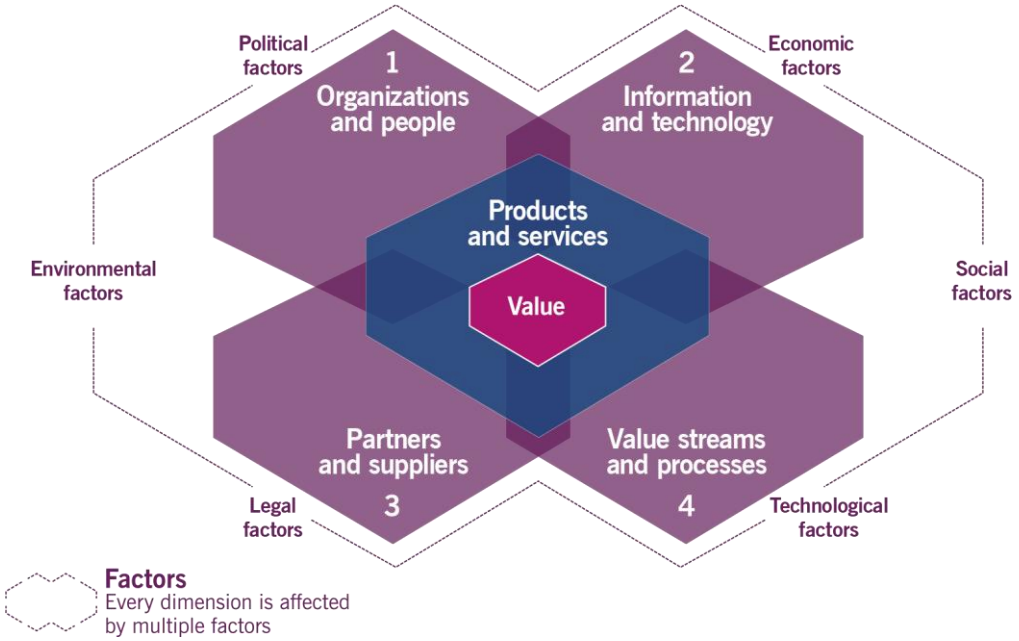
Rysunek 1.10. Elementy systemu wartości usług
Źródło: ITIL® Foundation, ITIL 4 edition. Norwich: TSO (The Stationery Office), 2019, s. 15.

Podstawową częścią SVS jest łańcuch wartości usług (ang. *Service Value Chain*, skrót: SVC). Jest to elastyczny model operacyjny, który definiuje sześć kluczowych działań, które mogą być łączone na różne sposoby, tworząc wiele strumieni wartości:

1) Planowanie (ang. *Plan*),
2) Ulepszanie (ang. *Improve*),
3) Zaangażowanie (ang. *Engage*),
4) Projektowanie i Przekazywanie (ang. *Design and Transition*),
5) Pozyskiwanie i Rozwijanie (ang. *Obtain/ Build*),
6) Dostarczanie i Wspieranie (ang. *Deliver and Support*).

Zdolność adaptacyjna łańcucha wartości usług ma umożliwiać organizacjom reagowanie na zmieniające się wymagania swoich interesariuszy w najbardziej efektywny i skuteczny sposób. SVC powinien zapewniać tworzenie, dostarczanie i ciągłe doskonalenie usług.

W celu wparcia holistycznego podejścia do zarządzania usługami IT w ITIL 4 zostały zdefiniowane cztery wymiary zarządzania (Rysunek 1.11). Mają one kluczowe znaczenie dla skutecznego i wydajnego tworzenia wartości dla interesariuszy.



Rysunek 1.11. Cztery wymiary zarządzania usługami
Źródło: ITIL® Foundation, ITIL 4 edition. Norwich: TSO (The Stationery Office), 2019, s. 39.

1) Organizacje i ludzie (ang. *Organizations and people*) – zapewnienie, że sposób, w jaki organizacja jest zorganizowana i zarządzana, zasady przydzielania ról i odpowiedzialności, systemy uprawnień i komunikacji, są dobrze zdefiniowane i wspierają strategię oraz model operacyjny organizacji.
2) Informacja i techniki (ang. *Information and technology*) – wymiar ten obejmuje informacje i wiedzę niezbędną do zarządzania usługami, jak również wymagane techniki. Obejmuje on również relacje pomiędzy różnymi komponentami SVS, takie jak wejścia i wyjścia działań oraz praktyk.
3) Partnerzy i dostawcy (ang. *Partners and suppliers*) – wymiar ten obejmuje relacje organizacji z innymi organizacjami, które są zaangażowane w: projektowanie, rozwój, wdrażanie, dostarczanie, wspieranie i doskonalenie usług. Obejmuje on również umowy pomiędzy organizacją a jej partnerami lub dostawcami.
4) Strumienie wartości i procesy (ang. *Value streams and processes*) – wymiar ten skupia się na tym, jakie działania podejmuje organizacja i jak są one zorganizowane, aby umożliwić tworzenie wartości poprzez produkty i usługi.

Na każdy wymiar mają wpływ różne czynniki zewnętrzne, tj.: prawne, techniczne, polityczne, ekonomiczne czy społeczne.

ITIL SVS obejmuje czternaście ogólnych praktyk zarządzania, siedemnaście praktyk zarządzania usługami i trzy praktyki zarządzania technicznego – wszystkie

podlegają czterem wymiarom zarządzania usługami. W ITIL praktyka zarządzania to zbiór zasobów organizacyjnych przeznaczonych do realizacji zadań lub osiągnięcia celu[177].

Jedną z ogólnych praktyk zarządzania jest zarządzanie bezpieczeństwem informacji (ang. *Information Security Management*, skrót: ISM). Praktyka ta została wprowadzone w wersji 3 biblioteki ITIL. Obejmuje szacowanie i zarządzanie ryzykiem dla poufności, integralności i dostępności informacji, a także inne aspekty bezpieczeństwa informacji[178]. Aby wspierać zarządzanie bezpieczeństwem informacji w organizacji, potrzebnych jest wiele procesów i procedur. Należą do nich:

- proces zarządzania incydentami związanymi z bezpieczeństwem informacji,
- proces zarządzania ryzykiem,
- proces przeglądu i audytu,
- proces zarządzania tożsamością i dostępem,
- zarządzanie zdarzeniami,
- procedury testów penetracyjnych, skanowania podatności itp.
- procedury zarządzania zmianami związanymi z bezpieczeństwem informacji, np. zmianami w konfiguracji zapory ogniowej.

Zauważono, że zarządzanie bezpieczeństwem informacji powinno wchodzić w interakcje ze wszystkimi innymi trzynastoma ogólnymi praktykami oraz że powinno być zaangażowane we wszystkie komponenty SVS[179]. Bezpieczeństwo informacji jest zależne od zachowania ludzi w całej organizacji. Pracownicy, którzy zostali dobrze przeszkoleni i zwracają uwagę na polityki bezpieczeństwa informacji i inne zabezpieczenia, mogą pomóc w wykrywaniu, zapobieganiu i usuwaniu incydentów związanych z bezpieczeństwem informacji.

[177] ITIL® Foundation, ITIL 4 edition. Norwich: TSO (The Stationery Office), 2019, s. 246.
[178] Niezaprzeczalność – zapewnienie, że ktoś nie może zaprzeczyć, że podjął jakieś działanie.
[179] D. Berger, N. Shashidhar and C. Varol, *Using ITIL 4 in Security Management*, 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, s. 1–6.

1.2.8. ISACA[180] COBIT 2019

Ramy najlepszych praktyk zarządzania informacją i techniką COBIT są publikowane przez ISACA od 1996 r. W listopadzie 2018 r. ukazała się najnowsza wersja ram COBIT 2019. Aktualizacja COBIT ma na celu ułatwienie wdrożenia zarządzania organizacją w zakresie technik informatycznych (ang. *Enterprise Governance of Information Technology* – EGIT), bardziej elastycznego i dostosowanego do potrzeb. W porównaniu z poprzednią wersją COBIT 5: zaktualizowano kaskadę celów (ang. *goals cascade*), wprowadzono trzy nowe procesy (APO14 – Dane zarządzane; BAI11 – Projekty zarządzane; MEA04[181] – Zarządzane zapewnienie – Rysunek 1.12), koncepcję obszarów zainteresowania (ang. *focus areas*) oraz przedstawiono czynniki projektowe (ang. *design factors*).

Według koncepcji kaskady celów potrzeby interesariuszy muszą zostać przekształcone w cele nadzoru i zarządzania organizacją. Następuje to kaskadowo, potrzeby interesariuszy brane są pod uwagę w określaniu priorytetowych celów organizacji, następnie określane są priorytetowe cele dostosowania wszystkich działań z zakresu IT do celów organizacji. Końcowym efektem są cele nadzoru i zarządzania wpływające na system zarządzania organizacją.

Obszar zainteresowania opisuje określony temat, dziedzinę lub problem ładu organizacyjnego, którymi można się zająć poprzez wyznaczenie celów nadzoru i zarządzania oraz ich komponentów. Obszarami zainteresowania mogą być na przykład: małe i średnie przedsiębiorstwa, cyberbezpieczeństwo, transformacja cyfrowa, przetwarzanie w chmurze, prywatność. Obszary tematyczne mogą zawierać kombinację ogólnych komponentów zarządzania i wariantów niektórych komponentów dostosowanych do tematu danego obszaru. Nowe obszary tematyczne mogą być

[180] ISACA (ang. *Information Systems Audit and Control Association*, pol. Stowarzyszenie Audytu i Kontroli Systemów Informatycznych) – międzynarodowe stowarzyszenie osób zajmujących się zawodowo zagadnieniami dotyczącymi audytu, kontroli, bezpieczeństwa oraz innymi aspektami zarządzania systemami informatycznymi. ISACA opracowała Standard COBIT 2019 (ang. *Control Objectives for Information and related Technology*, pol. Cele kontrolne w zakresie informacji i technologii powiązanych) – dobre praktyki w zakresie ładu informatycznego.

[181] Opis MEA04: Planowanie, określanie zakresu i realizacja inicjatyw związanych z zapewnieniem zgodności z: wymogami wewnętrznymi, przepisami prawa, regulacjami i celami strategicznymi. Umożliwianie kierownictwu dostarczania odpowiedniego i trwałego zapewnienia w organizacji poprzez przeprowadzanie niezależnych przeglądów i działań w zakresie zapewnienia (tłum. własne), źródło: COBIT 2019, Framework: Governance and Management Objectives, ISACA 2019, s. 289; Assurance – zapewnienie/audyt (tłum. ISACA Glossary of Terms English-Polish, źródło: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/isaca-glossary-english-polish_0320.pdf?la=en&hash=7D1019A7B0C29BB10AF3E3A73712E2993CB2A4DA, dostęp: . 21.09.2021 r.

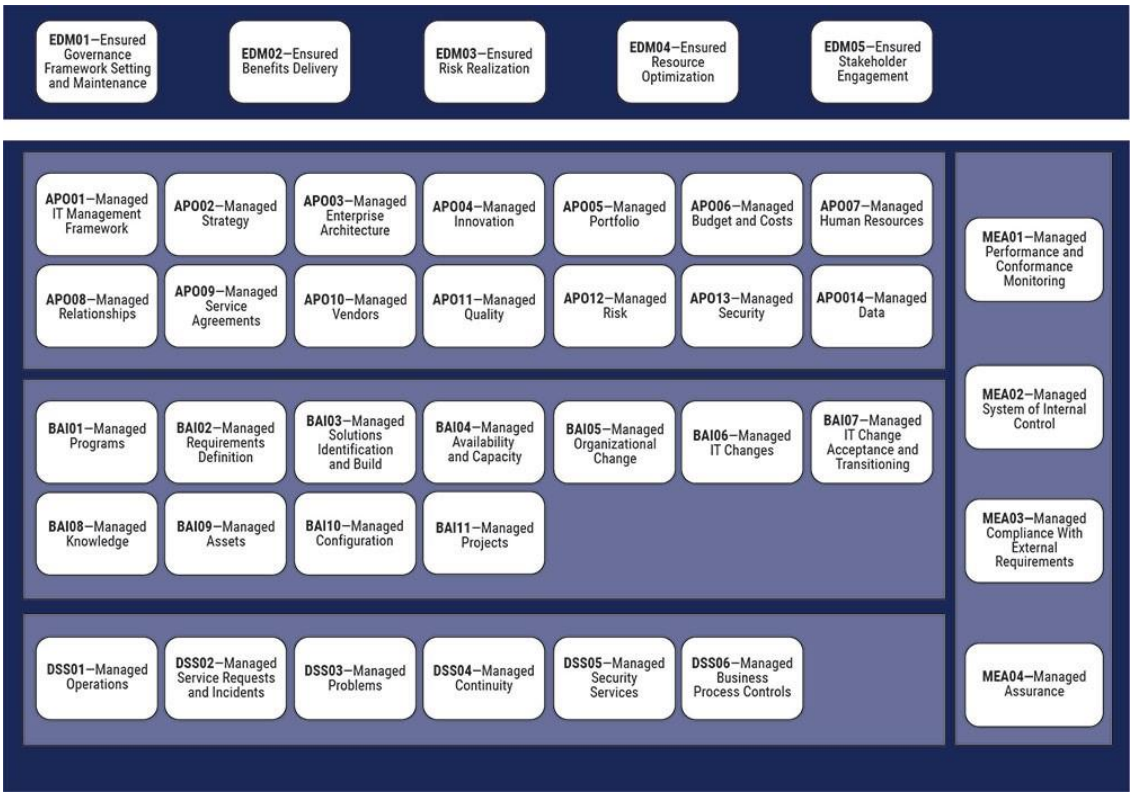
dodawane w miarę potrzeb lub w miarę jak eksperci i praktycy przyczyniają się do rozwoju otwartego modelu COBIT. To właśnie sprawia, że COBIT ma charakter otwarty.

Czynniki projektowe to takie, które mogą wpływać na projektowanie systemu zarządzania organizacją i zapewnić jej sukces w korzystaniu z IT. Mogą obejmować dowolną kombinację następujących czynników: ogólna strategia organizacji, cele wspierające strategię, profil ryzyka organizacji, doświadczenie organizacji związane z incydentami, wymogi zgodności z przepisami prawnymi, rola odgrywana przez techniki informatyczne w organizacji, metody pozyskiwania i wdrażania tych technik, wielkość organizacji.

Ewolucja ram COBIT jest odpowiedzią na istotne zmiany związane z IT w organizacjach, m.in.: ewoluujące modele zaopatrzenia w usługi IT, przeobrażające się modele biznesowe z powodu transformacji cyfrowej, zmieniający się krajobraz regulacyjny[182].

COBIT 2019 uznaje IT za istotny element organizacji w zakresie realizacji jej celów i wymaga, aby cele strategii organizacji zostały włączone do celów IT oraz aby świadczone usługi spełniały wymagania jakościowe procesów. Podobnie jak ITIL, COBIT opiera się na ukierunkowanych, zoptymalizowanych procesach IT. Wprowadza aspekt potencjału procesowego, który odnosi się do stopnia, w jakim organizacja jest w stanie osiągnąć wymagane cele w sposób niezawodny i trwały. Przegląd dojrzałości wszystkich 40 obszarów procesowych, zgrupowanych w pięciu domenach, może być wykorzystany do określenia dojrzałości wspierających je procesów IT. Opracowując COBIT, autorzy wzorowali się na istniejących standardach dotyczących tematyki zarządzania bezpieczeństwem, w szczególności na normie ISO/IEC 27002. Rysunek 1.12 przedstawia Model COBIT z celami nadzoru i zarządzania.

[182] D. Steuperaert, *COBIT 2019: A Significant Update*, EDPACS, 2019, 59(1), s. 14–18.



Rysunek 1.12. Model COBIT
Źródło: https://www.isaca.org/resources/news-and-trends/industry-news/2020/using-cobit-2019-to-plan-and-execute-an-organization-transformation-strategy, dostęp. 21.09.2021 r.

Cele nadzoru i zarządzania w COBIT są zgrupowane w pięciu domenach (Rysunek 1.12).

Celem nadzoru jest:

– Ocenianie, kierowanie i monitorowanie (ang. *Evaluate, Direct and Monitor* – EDM).

Cele zarządzania są zgrupowane w czterech domenach:

– Dostosowanie, planowanie i organizowanie (ang. *Align, Plan and Organize* – APO) dotyczy całej organizacji, strategii i działań wspierających IT.
– Tworzenie, nabywanie i wdrożenie (ang. *Build, Acquire and Implement* – BAI) zajmuje się definiowaniem, nabywaniem i wdrażaniem rozwiązań IT oraz ich integracją w procesach biznesowych.
– Dostawa, serwis i wsparcie (ang. *Deliver, Service and Support* – DSS) zajmuje się dostarczaniem i wsparciem operacyjnym usług IT, w tym ochroną.
– Monitorowanie, ocenianie i szacowanie (ang. *Monitor, Evaluate and Assess* – MEA) dotyczy monitorowania wydajności i zgodności IT z wewnętrznymi normami bezpieczeństwa.

Aby spełnić cele w zakresie nadzoru i zarządzania, każda organizacja musi ustanowić, dostosować i utrzymać system zarządzania, składający się z wielu komponentów. Te ostatnie to czynniki, które indywidualnie i zbiorowo przyczyniają się do dobrego funkcjonowania systemu zarządzania. COBIT 2019 wymienia następujące jego komponenty:

- Procesy – zestaw praktyk i działań mających na celu osiągnięcie określonych celów.
- Struktury organizacyjne – odpowiedzialność, nadzór.
- Zasady, polityki i ramy – przełożenie pożądanych zachowań na praktyczne wskazówki.
- Informacja – wszystkie informacje wytwarzane i wykorzystywane przez organizację niezbędne do efektywnego funkcjonowania systemu zarządzania, przepływ informacji.
- Kultura, etyka i zachowanie jednostek oraz organizacji – czynniki wpływające na powodzenie działań związanych z nadzorem i zarządzaniem w organizacji.
- Ludzie, umiejętności i kompetencje – komponent niezbędny do podejmowania dobrych decyzji, realizacji działań.
- Usługi, infrastruktura i aplikacje – komponent zapewniający organizacji możliwość ukształtowania i zarządzania systemem informatycznym.

Komponenty zarządzania bezpieczeństwem informacji opisane są w domenie „Dostosowanie, planowanie i organizowanie", cel oznaczony jest w dokumentacji COBIT 2019[183] symbolem APO13. Zdefiniowanie, obsługa i monitorowanie systemu zarządzania bezpieczeństwem informacji ma zapewnić utrzymanie występowania incydentów związanych z bezpieczeństwem informacji na poziomie akceptowalnego ryzyka w organizacji. W podrozdziale 1.3.1 COBIT PM przedstawione są zaproponowane w APO13 komponenty wpływające na bezpieczeństwo informacji. Są one podstawą do utworzenia modelu oceny dojrzałości systemów zarządzania bezpieczeństwem informacji.

[183] COBIT® 2019 Framework: Governance and Management Objectives, s. 12, www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19fim, dostęp: 20.05.2020 r.

1.3. Ocena dojrzałości ukierunkowana na zarządzanie bezpieczeństwem informacji – wybrane modele

Ocena dojrzałości zarządzania bezpieczeństwem informacji stała się istotną częścią oceny kompetencji organizacji w zakresie zarządzania wszystkimi jej aspektami. Istotność ta wynika z faktu, iż znajdujemy się obecnie w okresie cywilizacyjnym zwanym informacyjnym[184], w którym to rozwój techniki umożliwił organizacjom zastąpienie izolowanych systemów informatycznych systemami pozwalającymi na swobodną wymianę informacji z otoczeniem. Procesy zarządzania bezpieczeństwem informacji powinny zapewnić poufność, integralność i dostępność przetwarzanej informacji. Tworzone modele dojrzałości składają się z różnorodnych narzędzi i praktyk, które badając stopień osiągniętej dojrzałości, umożliwiają doskonalenie kluczowych czynników prowadzących do osiągnięcia założonych celów. Odpowiednie zarządzanie bezpieczeństwem informacji prowadzi do osiągnięcia m.in. takich celów, jak ciągłość i dostępność usług związanych z główną działalnością, zarządzanie ryzykiem organizacji oraz ochrona danych osobowych.

Mikko Siponen mówi o modelach dojrzałości jako o spuściźnie list kontrolnych (ang. *check-list*). Twierdzi on, że każdą listę kontrolną i każdy standard zarządzania, dotyczący bezpieczeństwa informacji, można przekształcić w kryterium dojrzałości poprzez podzielenie ich na poziomy dojrzałości. M. Siponen dzieli modele na te, które są zorientowane na ocenę dojrzałości zarządzania bezpieczeństwem informacji oraz na modele, których kryteria zorientowane są na bezpieczeństwo informatyczne[185]. Niniejsza praca dotyczy pierwszej grupy modeli.

Z przeprowadzonego przeglądu literatury wynika[186], że wzorem dla wielu modeli dojrzałości, dotyczących zarządzaniem bezpieczeństwem informacji, był CMM opracowany przez Software Engineering Institute Carnegie Mellon University i MITRE Corporation dla Departamentu Obrony USA. W rozdziale zaprezentowane zostaną trzy modele, dwa z nich reprezentują rodzinę modeli wywodzących się z CMM, trzeci reprezentuje odmienne spojrzenie na temat oceny zarządzania bezpieczeństwem informacji.

[184] J. Bieńkowska, C. Sikorski, *Ewolucja zarządzania. Dyktat struktury, strategii i kultury*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2016, s. 79, 101.

[185] M. Siponen, *Towards*…, op. cit.

[186] A. Kaczmarek, op. cit., s. 95

1.3.1. COBIT PM

Model dojrzałości CPM[187] (ang. *COBIT Performance Management*), opracowany przez ISACA, jest składową ram COBIT 2019, w dużej mierze pokrywa się on z modelem CMMI Development V2.020. Zdefiniowanych jest w nim sześć poziomów dojrzałości dla procesów (Tabela 1.2), dodatkowo zdefiniowane są poziomy dojrzałości jako mierniki wydajności w danym obszarze zainteresowania. Obszar zainteresowania opisuje pewien temat, dziedzinę lub zagadnienie związane z zarządzaniem, które może być zbiorem celów nadzoru (np. zarządu, rady nadzorczej) i zarządzania (np. kierowników). Przykładowe obszary tematyczne obejmują: transformację cyfrową, bezpieczeństwo cybernetyczne, przetwarzanie w chmurze, prywatność.

Tabela 1.2. Poziomy zdolności dla procesów w modelu dojrzałości CPM

Poziomy dojrzałości	**Opis poziomu dla procesów**	**Opis poziomu dla obszaru zainteresowania**
Poziom 0	Brak jakichkolwiek podstawowych zdolności: – niewystarczające podejście do realizacji celów w zakresie nadzoru i zarządzania, – mogą lub nie muszą być zgodne z intencją jakichkolwiek praktyk procesowych.	Niekompletny – praca może, ale nie musi być zakończona w celu osiągnięcia celów nadzoru oraz zarządzania w obszarze zainteresowania.
Poziom 1.	Proces w mniejszym lub większym stopniu osiąga swój cel poprzez zastosowanie niepełnego zestawu czynności, który można określić jako wstępny lub intuicyjny – niezbyt zorganizowany.	Wstępny – praca jest ukończona, ale nie osiągnięto jeszcze pełnego celu i intencji obszaru zainteresowania.
Poziom 2.	Proces osiąga swój cel poprzez zastosowanie podstawowego, ale kompletnego zestawu czynności, które można określić jako	Zarządzane – planowanie i pomiar wydajności mają miejsce, choć jeszcze nie w sposób znormalizowany.

[187] COBIT 2019 Framework: Introduction and Methodology, www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19fim, dostęp: 20.05.2020 r.

Poziomy dojrzałości	Opis poziomu dla procesów	Opis poziomu dla obszaru zainteresowania
	wykonywane.	
Poziom 3.	Proces ten osiąga swój cel w znacznie bardziej zorganizowany sposób, wykorzystując zasoby organizacyjne. Procesy zazwyczaj są dobrze zdefiniowane.	Zdefiniowane – normy zapewniają wytyczne dla całej organizacji.
Poziom 4.	Proces osiąga swój cel, jest dobrze zdefiniowany, a jego wydajność jest mierzona (ilościowo).	Ilościowy – organizacja opiera się na analizie danych, z wdrożoną ilościową poprawą wydajności.
Poziom 5.	Proces osiąga swój cel, jest dobrze zdefiniowany, a jego wydajność jest mierzona w celu poprawy wydajności i ciągłego doskonalenia.	Optymalizacja – organizacja jest nastawiona na ciągłe doskonalenie.

Źródło: opracowanie własne na podstawie COBIT 2019 Framework: Introduction and Methodology, www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19fim, dostęp: 20.05.2020 r.

Ocena dojrzałości procesów związanych z zarządzaniem bezpieczeństwem informacji opiera się na ocenie podejmowanych działań w ramach praktyk zarządczych opisanych w domenie „Dostosowanie, planowanie i organizowanie" w celach zarządzania APO13 (Podrozdział 1.2.8 ISACA COBIT 2019).

W komponencie *Proces* zaproponowane są następujące praktyki zarządcze:

1) APO13.01 Ustanowić i utrzymywać system zarządzania bezpieczeństwem informacji.

   Ustanowienie i utrzymanie SZBI, który zapewnia praktyczne, formalne i ciągłe podejście do zarządzania bezpieczeństwem informacji, używając bezpiecznych technik i procesów, które są dostosowane do wymagań organizacji. Przykładowym miernikiem realizacji praktyki może być stopień zadowolenia interesariuszy z wdrożonych rozwiązań dotyczących bezpieczeństwa informacji w organizacji.

2) APO13.02 Zdefiniowanie i zarządzanie planem postępowania z ryzykiem dotyczącym bezpieczeństwa informacji i prywatności.

   Utrzymanie planu bezpieczeństwa informacji, który opisuje sposób zarządzania ryzykiem w zakresie bezpieczeństwa informacji i jest dostosowany do strategii oraz struktury organizacji. Liczba pracowników, którzy pomyślnie ukończyli szkolenie dotyczące świadomości bezpieczeństwa informacji, może być miernikiem realizacji tej praktyki.

3) APO13.03 Monitorowanie i przegląd systemu zarządzania bezpieczeństwem informacji.

   Informowanie o potrzebie i korzyściach płynących z ciągłego doskonalenia w zakresie bezpieczeństwa informacji. Zbieranie i analizowanie danych dotyczących SZBI oraz poprawianie jego skuteczności. Korygowanie nieprawidłowości w celu zapobiegania ich ponownemu wystąpieniu. Przykładami mierników powyższej praktyki są częstotliwość planowanych przeglądów bezpieczeństwa oraz liczba incydentów związanych z nieprzestrzeganiem zasad bezpieczeństwa informacji obowiązujących w organizacji.

Do wszystkich powyższych praktyk zarządczych wskazano działania, którym przypisano poziom dojrzałości COBIT PM.

Wszystkie działania dla praktyki APO13.01 osiągają maksymalnie poziom dojrzałości 2., są one następujące:

1. Określenie zakresu i granic systemu zarządzania bezpieczeństwem informacji (ISMS) w odniesieniu do: charakterystyki przedsiębiorstwa, organizacji, jej lokalizacji, aktywów i technologii. Należy podać szczegóły i uzasadnienie wszelkich wyłączeń z zakresu.
2. Zdefiniowanie ISMS zgodnie z polityką przedsiębiorstwa i kontekstem, w którym działa przedsiębiorstwo.
3. Dostosowanie ISMS do ogólnego podejścia przedsiębiorstwa do zarządzania bezpieczeństwem.
4. Uzyskanie upoważnienia kierownictwa do wdrożenia i obsługi lub zmiany ISMS.
5. Przygotowanie i utrzymywanie oświadczenia o stosowalności, które opisuje zakres ISMS.

6. Zdefiniowanie i zakomunikowanie ról oraz obowiązków związanych z zarządzaniem bezpieczeństwem informacji.
7. Komunikowanie strategii ISMS.

Sześć pierwszych działań dla praktyki APO13.02 jest na poziomie dojrzałości 3. Jeżeli realizowane jest ostatnie siódme działanie (i wszystkie poprzedzające działania), proces może osiągnąć poziom 4.:

1. Sformułowanie i utrzymywanie planu postępowania z ryzykiem związanym z bezpieczeństwem informacji, dostosowanego do celów strategicznych i architektury przedsiębiorstwa. Zapewnienie, że plan identyfikuje odpowiednie i optymalne praktyki zarządzania i rozwiązania w zakresie bezpieczeństwa wraz z powiązanymi zasobami, obowiązkami oraz priorytetami w zakresie zarządzania zidentyfikowanym ryzykiem bezpieczeństwa informacji.
2. Utrzymywanie w ramach architektury korporacyjnej wykazu komponentów rozwiązań, które są stosowane do zarządzania ryzykiem związanym z bezpieczeństwem.
3. Opracowanie propozycji wdrożenia planu postępowania z ryzykiem związanym z bezpieczeństwem informacji, popartych odpowiednimi przypadkami biznesowymi, które obejmują rozważenie finansowania i alokacji ról oraz obowiązków.
4. Zapewnienie wkładu w projektowanie i rozwój praktyk zarządzania oraz rozwiązań wybranych z planu postępowania z ryzykiem bezpieczeństwa informacji.
5. Wdrażanie programów szkoleniowych i uświadamiających w zakresie bezpieczeństwa informacji i prywatności.
6. Integracja planowania, projektowania, wdrażania i monitorowania procedur bezpieczeństwa informacji i prywatności oraz innych środków kontroli umożliwiających szybkie zapobieganie, wykrywanie zdarzeń związanych z bezpieczeństwem i reagowanie na incydenty związane z bezpieczeństwem.
7. Określenie sposobu pomiaru skuteczności wybranych praktyk zarządzania.

Pierwsze działanie dla praktyki APO13.03 jest na poziomie dojrzałości 4, pozostałe na poziomie dojrzałości 5, najwyższym:

1. Przeprowadzanie regularnych przeglądów skuteczności ISMS. Obejmują one realizację polityki i celów ISMS oraz przegląd praktyk w zakresie bezpieczeństwa i prywatności.
2. Przeprowadzanie audytów ISMS w zaplanowanych odstępach czasu.
3. Regularne przeprowadzanie kierowniczego przeglądu SZBI w celu zapewnienia adekwatności zakresu i identyfikacji usprawnień w procesie SZBI.
4. Rejestrowanie działań i zdarzeń, które mogą mieć wpływ na skuteczność lub wydajność ISMS.
5. Zapewnienie wkładu w utrzymanie planów bezpieczeństwa w celu uwzględnienia ustaleń z monitorowania i przeglądu działań.

Każda praktyka posiada informacje o mapowaniu na powiązane normy, ramy, wytyczne (np. ISO/IEC 27001:2013, ITIL V3, NIST Special Publication 800-37, Revision 2 (Draft), maj 2018 r.) innych organizacji zajmujących się tworzeniem wytycznych do zarządzania bezpieczeństwem informacji.

W komponencie „Struktura organizacyjna" przedstawiona jest propozycja podziału ról w organizacji ze wskazaniem osób odpowiedzialnych (symbol: R) i osób rozliczanych (symbol: A) za realizację jednej z wymienionych powyżej praktyk zarządczych. W komponencie „Przepływy i pozycje informacji" wskazane są informacje, jakie są potrzebne na wejściu, a jakie na wyjściu danej praktyki, jakie jest źródło, a jakie przeznaczenie danej informacji. W części dotyczącej „Ludzi, umiejętności i kompetencji" wymieniono bezpieczeństwo informacji, opracowanie strategii bezpieczeństwa informacji. Pierwszą umiejętność muszą zdobyć wszyscy pracownicy w organizacji, druga osoby odpowiedzialne za opracowanie strategii. Wskazane są również dokumenty, z których można czerpać wiedzę na temat wymienionych umiejętności. W komponencie „Polityk i procedur" wymieniona jest regulacja wewnętrzna: Polityka bezpieczeństwa informacji i ochrony prywatności. W części „Kultura, etyka i zachowanie" jako kluczowe elementy wskazano: ustanowienie kultury świadomości bezpieczeństwa i prywatności, która ma pozytywnie wpłynąć na pożądane zachowania i codzienną praktykę zachowania bezpieczeństwa informacji i prywatności; opracowanie wytycznych dotyczących bezpieczeństwa i prywatności; wskazanie liderów w dziedzinie bezpieczeństwa i prywatności; proaktywne wspieranie i komunikowanie o zadaniach z zakresu bezpieczeństwa i prywatności. W komponencie „Usługi, infrastruktura i aplikacje" są podane typy narzędzi i usług niezbędnych do realizacji wymienionych praktyk zarządczych.

Wszystkie wskazane komponenty są istotne w ocenie dojrzałości procesów zarządzania bezpieczeństwem informacji.

1.3.2. C2M2

Departament Energii Stanów Zjednoczonych Ameryki (ang. *Department of Energy* – DOE), we współpracy z Carnegie Mellon University, opublikował w 2012 r. model dojrzałości i zdolności w dziedzinie bezpieczeństwa cybernetycznego (ang. *Cybersecurity Capability Maturity Model* – C2M2). Model C2M2 miał wspierać tworzenie nowy regulacji dotyczących cyberbezpieczeństwa w organizacji lub oceniać dojrzałość, a następnie wspierać ulepszanie istniejących zasad. Ostatnia wersja (2.1) modelu[188], wydana w czerwcu 2022 r., została opracowana w ramach współpracy między organizacjami sektora publicznego i prywatnego, a finansowana była przez DOE, Radę Koordynacyjną Podsektora Energii Elektrycznej (ESCC) oraz Radę Koordynacyjną Podsektora Ropy Naftowej i Gazu Ziemnego (ONG SCC). Model dostarcza przede wszystkim zalecenia o charakterze opisowym, a nie normatywnym. Opracowany jest na wysokim poziomie abstrakcji, dzięki czemu może być stosowany przez organizacje o różnych typach, strukturach i rozmiarach.

Model ten jest zorganizowany w dziesięć domen, każda z nich jest logicznym zgrupowaniem praktyk z zakresu bezpieczeństwa cybernetycznego. Praktyki w ramach każdej domeny są zorganizowane w zadania, które reprezentują cele w ramach danej domeny. Domeny, cele i zadania wymienione są poniżej (Tabela 1.3).

Tabela 1.3. Domeny, cele i zadania C2M2

Domeny	**Cele (ang. *proposes*)**	**Zadania (ang. *objectives*)**
Zarządzanie aktywami, zmianami i konfiguracją (ZASOBY)	Zarządzanie zasobami IT[189] i OT[190] organizacji, w tym zarówno sprzętem, jak i oprogramowaniem, oraz zasobami informacyjnymi współmiernymi do ryzyka dla	1. Zarządzanie inwentaryzacją zasobów IT i OT 2. Zarządzanie inwentaryzacją zasobów informacyjnych 3. Zarządzanie konfiguracją

[188] Cybersecurity Capability Maturity Model (C2M2), Version 2.1, 2022, DOE, https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf, dostęp: 2.02.2023 r.

[189] IT – skrót od ang. *Information Technology* (tłum.: techniki informacyjne). W ogólnym znaczeniu obejmuje ona przetwarzanie i przesyłanie danych w różnych formatach z punktu A do punktu B.

[190] OT – skrót od ang. *Operational Technology* (tłum.: technika operacyjna). W przeciwieństwie do IT obejmuje ona wykorzystanie sprzętu i oprogramowania w środowisku przemysłowym, często w produkcji lub w sektorze energetycznym. OT wykorzystywane jest również w systemach zarządzania budynkami i w sektorze medycznym.

Domeny	Cele (ang. *proposes*)	Zadania (ang. *objectives*)
	infrastruktury krytycznej i celów organizacyjnych.	zasobów IT i OT 4. Zarządzanie zmianami w zasobach IT i OT 5. Działania związane z zarządzaniem dla domeny ZASOBY
Zarządzanie zagrożeniami i podatnościami (ZAGROŻENIA)	Ustanowienie i utrzymywanie planów, procedur i technologii w celu: wykrywania, identyfikowania, analizowania, zarządzania i reagowania na zagrożenia i słabości cyberbezpieczeństwa, współmiernie do ryzyka dla infrastruktury organizacji (takiej jak krytyczna, IT i operacyjna) oraz celów organizacyjnych.	1. Zmniejszenie podatności na zagrożenia cybernetyczne 2. Reagowanie na zagrożenia i udostępnianie informacji o zagrożeniach 3. Działania związane z zarządzaniem domeną ZAGROŻENIA
Zarządzanie ryzykiem (RYZYKO)	Ustanowienie, obsługa i utrzymanie programu zarządzania ryzykiem cybernetycznym w przedsiębiorstwie w celu identyfikacji, analizy i reagowania na ryzyko cybernetyczne, na które narażona jest organizacja, w tym: jej jednostki biznesowe, podmioty zależne, powiązana infrastruktura i interesariusze.	1. Ustanowienie i utrzymanie strategii i programu zarządzania ryzykiem cybernetycznym 2. Identyfikacja ryzyka cybernetycznego 3. Analiza ryzyka cybernetycznego 4. Reagowanie na ryzyko cybernetyczne 5. Zarządzanie działaniami w domenie RYZYKO
Zarządzanie tożsamością i dostępem (DOSTĘP)	Tworzenie tożsamości i zarządzanie nimi dla podmiotów, które mogą uzyskać logiczny lub fizyczny dostęp do zasobów organizacji. Kontrola dostępu do zasobów organizacji, współmierna do ryzyka dla infrastruktury krytycznej i celów organizacyjnych.	1. Ustanowienie tożsamości i zarządzanie uwierzytelnianiem 2. Kontrola dostępu logicznego 3. Kontrola dostępu fizycznego 4. Działania związane z zarządzaniem domeną DOSTĘP
Świadomość sytuacyjna (SYTUACJA)	Ustanowienie i utrzymanie działań i technik w celu: gromadzenia, monitorowania, analizowania, alarmowania, raportowania i wykorzystywania informacji	1. Wykonywanie rejestrowania 2. Monitorowanie 3. Ustanowienie i utrzymanie świadomości sytuacyjnej 4. Działania związane z

Domeny	Cele (ang. *proposes*)	Zadania (ang. *objectives*)
	operacyjnych, dotyczących bezpieczeństwa i zagrożeń, w tym informacji o stanie i podsumowań z innych domen modelu, w celu ustanowienia świadomości sytuacyjnej zarówno dla stanu operacyjnego organizacji, jak i stanu cyberbezpieczeństwa.	zarządzaniem dla domeny SYTUACJA
Reakcja na zdarzenia i incydenty, ciągłość działania (REAKCJA)	Ustanowienie i utrzymywanie planów, procedur i technik w celu: wykrywania, analizowania, łagodzenia, reagowania i odzyskiwania danych po zdarzeniach i incydentach związanych z cyberbezpieczeństwem oraz w celu podtrzymywania działań podczas incydentów związanych z cyberbezpieczeństwem, współmiernie do ryzyka dla infrastruktury krytycznej i celów organizacyjnych.	1. Wykrywanie zdarzeń związanych z cyberbezpieczeństwem 2. Analizowanie zdarzeń cyberbezpieczeństwa i zgłaszanie incydentów 3. Reagowanie na incydenty cyberbezpieczeństwa 4. Uwzględnianie cyberbezpieczeństwa w ciągłości działania 5. Działania zarządcze dla domeny REAKCJA
Zarządzanie ryzykiem stron trzecich (STRONY TRZECIE)	Ustanowienie i utrzymanie mechanizmów kontrolnych w celu zarządzania ryzykiem cybernetycznym wynikającym z działalności dostawców i innych stron trzecich, współmiernie do ryzyka dla infrastruktury krytycznej i celów organizacyjnych.	1. Identyfikacja i priorytetyzacja stron trzecich 2. Zarządzanie ryzykiem stron trzecich 3. Działania w zakresie zarządzania dla domeny STRONY TRZECIE
Zarządzanie pracownikami (PRACOWNICY)	Ustanowienie i utrzymanie planów, procedur, technik i mechanizmów kontrolnych w celu stworzenia kultury cyberbezpieczeństwa oraz zapewnienia ciągłej przydatności i kompetencji personelu, współmiernych do ryzyka dla infrastruktury krytycznej i celów organizacyjnych.	1. Wdrożenie mechanizmów kontroli pracowników 2. Zwiększenie świadomości w zakresie cyberbezpieczeństwa 3. Przypisanie odpowiedzialności za cyberbezpieczeństwo 4. Rozwój umiejętności pracowników w obszarze cyberbezpieczeństwa 5. Działania związane z zarządzaniem dla domeny

Domeny	Cele (ang. *proposes*)	Zadania (ang. *objectives*)
		PRACOWNICY
Architektura cyberbezpieczeństwa (ARCHITEKTURA)	Ustanowienie i utrzymanie struktury i zachowanie organizacyjnej architektury cyberbezpieczeństwa, w tym: mechanizmów kontrolnych, procesów, technik i innych elementów, współmiernych do ryzyka dla infrastruktury krytycznej i celów organizacyjnych.	1. Ustanowienie i utrzymanie strategii i programu architektury cyberbezpieczeństwa. 2. Wdrożenie ochrony sieci jako elementu architektury cyberbezpieczeństwa 3. Wdrożenie zabezpieczeń zasobów IT i OT jako elementu architektury cyberbezpieczeństwa 4. Wdrożenie zabezpieczeń oprogramowania jako elementu architektury cyberbezpieczeństwa 5. Wdrożenie bezpieczeństwa danych jako elementu architektury cyberbezpieczeństwa 6. Działania związane z zarządzaniem dla domeny ARCHITEKTURA
Zarządzanie programem cyberbezpieczeństwa (PROGRAM)	Ustanowienie i utrzymanie programu cyberbezpieczeństwa organizacji, który zapewnia nadzór, planowanie strategiczne i finansowanie działań organizacji w zakresie cyberbezpieczeństwa w sposób, który dostosowuje cele cyberbezpieczeństwa – zarówno do celów strategicznych organizacji, jak i ryzyka dla infrastruktury krytycznej.	1. Ustanowienie strategii programu cyberbezpieczeństwa 2. Ustanowienie i utrzymanie programu cyberbezpieczeństwa 3. Działania zarządcze dla domeny PROGRAM

Źródło: opracowanie własne na podstawie Cybersecurity Capability Maturity Model (C2M2), Version 2.1, 2022, DOE, https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf, dostęp: 2.02.2023 r.

Model definiuje cztery poziomy wskaźników dojrzałości (MIL): od MIL0 do MIL3 (Tabela 1.4), które mają zastosowanie niezależnie do każdej domeny w modelu. W rezultacie organizacja korzystająca z modelu może działać na różnych poziomach MIL w różnych domenach. Aby zdobyć MIL w danej domenie, organizacja musi wykonać wszystkie praktyki na tym poziomie oraz wszystkie z poprzedzających poziomów.

Tabela 1.4. Poziomy dojrzałości C2M2

Poziom dojrzałości (MIL)	**Opis poziomu**
MIL0	Praktyki nie są wykonywane.
MIL1	Wstępne praktyki są wykonywane, ale mogą być doraźne.
MIL2	– Praktyki są udokumentowane. – Zapewnione są odpowiednie zasoby wspierające proces. – Praktyki są bardziej kompletne lub zaawansowane niż w MIL1.
MIL3	– Działaniami kierują polityki (lub inne dyrektywy organizacyjne). – Odpowiedzialność, rozliczalność i uprawnienia do wykonywania praktyk są przypisane. – Personel wykonujący praktyki posiada odpowiednie umiejętności i wiedzę. – Skuteczność działań jest oceniana i monitorowana. – Praktyki są bardziej kompletne lub zaawansowane niż w MIL2.

Źródło: opracowanie własne na podstawie CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2), Version 2.1, https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf, s. 25, dostęp: 2.02.2023 r.

C2M2 zawiera w sumie 356 praktyk cyberbezpieczeństwa – są one przypisane do zadania oraz do poziomu dojrzałości, który organizacja osiągnie, kiedy dane praktyki będą realizowane. Na przykład, dla zadania nr 1. Ustanowienie strategii programu cyberbezpieczeństwa w domenie PROGRAM wskazane są następujące praktyki:

Na poziomie **MIL1**

a. Organizacja posiada strategię programu cyberbezpieczeństwa, która może być rozwijana i zarządzana w sposób doraźny.

Na poziomie **MIL2**

b. Strategia programu cyberbezpieczeństwa definiuje cele i zadania dla działań organizacji w zakresie cyberbezpieczeństwa.
c. Strategia i priorytety programu cyberbezpieczeństwa są udokumentowane i dostosowane do misji organizacji, celów strategicznych i ryzyka dla infrastruktury krytycznej.
d. Strategia programu cyberbezpieczeństwa określa podejście organizacji do zapewnienia nadzoru nad programem i zarządzania działaniami w zakresie cyberbezpieczeństwa.

e. Strategia programu cyberbezpieczeństwa określa strukturę i organizację programu cyberbezpieczeństwa.
f. Strategia programu cyberbezpieczeństwa określa standardy i wytyczne, których program ma przestrzegać.
g. Strategia programu cyberbezpieczeństwa określa wszelkie obowiązujące wymogi zgodności, które muszą być spełnione przez program.

Na poziomie **MIL3**

h. Strategia programu cyberbezpieczeństwa jest okresowo aktualizowana zgodnie ze zdefiniowanymi czynnikami, takimi jak zmiany organizacyjne, w środowisku operacyjnym i w profilu zagrożeń.

Twórcy zalecają ustanowienie docelowego MIL dla każdej domeny jako skuteczną strategię wykorzystania modelu do zarządzania doskonaleniem programu cyberbezpieczeństwa. Osiągnięcie dojrzałości na danym poziomie MIL powinno być zgodne z celami organizacji oraz strategią programu cyberbezpieczeństwa. W dokumentach C2M2 podkreślane jest to, że dążenie do osiągnięcia najwyższego MIL we wszystkich domenach może nie być optymalne. Model został zaprojektowany tak, że każda organizacja, niezależnie od wielkości, powinna być w stanie osiągnąć MIL1 we wszystkich domenach.

1.3.3. FAM/ISFAM

Model FAM[191] (ang. *Focus Area Maturity*) różni się od większości modeli dojrzałości tym, że nie jest stałopoziomowy. Według twórców FAM modele stałopoziomowe dobrze nadają się do benchmarkingu, umieszczając organizację na poziomie dojrzałości poprzez ocenę stopnia wdrażanych procesów, ale są mniej odpowiednie dla stopniowego doskonalenia procesów. Spowodowane jest to tym, że nie mogą one wyrażać współzależności pomiędzy procesami składającymi się na poziomy dojrzałości. Do ciągłego doskonalenia domen funkcjonalnych bardziej odpowiednie są tzw. modele dojrzałości obszaru zainteresowania. Model FAM opiera się na koncepcji kilku obszarów zainteresowań, które należy opracować, aby osiągnąć dojrzałość w domenie funkcjonalnej. Model definiuje dla domeny funkcjonalnej serię etapów rozwoju w postaci stopniowego osiągania zdolności (ang. *capability*). Są one

[191] M. van Steenbergen, R. Bos, S. Brinkkemper, I. van de Weerd, W. Bekkers, *The Design of Focus Area Maturity Models*, Global Perspectives on Design Science Research, 5th International Conference, DESRIST 2010, St. Gallen, Switzerland, June 4–5, 2010. Proceedings. 6105, s. 317–332., dostęp: 19.05.2020 r.

specyficzne dla zidentyfikowanych obszarów zainteresowania. Jest to odejście od ustalonej liczby ogólnych poziomów dojrzałości, na których opierają się modele dojrzałości o stałym poziomie. Według zwolenników podejścia zróżnicowanie poziomów, które można zauważyć pomiędzy różnymi stałopoziomowymi modelami dojrzałości, sugeruje, że założenie istnienia ogólnych poziomów dojrzałości jest zbyt uproszczone. Porównując zdolności wszystkich obszarów zainteresowań w stosunku do siebie, definiuje się zrównoważoną, przyrostową ścieżkę rozwoju, biorąc pod uwagę wszystkie obszary zainteresowań. To zestawienie realizuje się poprzez umieszczenie zdolności w macierzy (Rysunek 1.13), która jest przykładem modelu dojrzałości obszarów zainteresowań w domenie funkcjonalnej architektury korporacyjnej. Obszary zainteresowań są podane w lewej kolumnie, zdolności w obszarze zainteresowania są przedstawione za pomocą liter od A do D, które oznaczają stopniowe osiąganie zdolności, kolejne poziomy dojrzałości są zapisane w pierwszym wierszu. Rzeczywista dojrzałość danej organizacji może być przedstawiona poprzez pokolorowanie komórek aż do następnej, niewdrożonej jeszcze zdolności.

Maturity Scale / Focus Area	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Development of architecture		A			B			C						
Use of architecture			A			B				C				
Alignment with business		A				B				C				
Alignment with the development process			A				B		C					
Alignment with operations					A			B			C			
Relationship to the as-is state					A				B					
Roles and responsibilities				A		B					C			
Coordination of developments							A			B				
Monitoring				A		B		C		D				
Quality management								A		B			C	
Maintenance of the architectural process							A		B		C			
Maintenance of architectural deliverables					A			B					C	
Commitment and motivation		A					B		C					
Architectural roles and training				A		B			C			D		
Use of an architectural method				A						B				C
Consultation			A		B				C					
Architectural tools							A				B			C
Budgeting and planning				A							B		C	

Rysunek 1.13. Przykładowa macierz z modelem FAM z dziedziny funkcjonalnej architektury korporacyjnej
Źródło: M. van Steenbergen, R. Bos, S. Brinkkemper, I. van de Weerd, W. Bekkers, The Design of Focus Area Maturity Models, Global Perspectives on Design Science Research, 5th International Conference, DESRIST 2010, St. Gallen, Szwajcaria, 2010.

Model ISFAM[192] (ang. *Information Security Focus Area Maturity*) wykorzystuje założenia FAM. Został on stworzony w celu poprawy dojrzałości bezpieczeństwa informacji w zorganizowany i efektywny sposób. ISFAM składa się z czterech grup

[192] M. Spruit, M. Roeling, *ISFAM: The information security focus area maturity model*, [w] Proceedings of the European Conference on Information Systems (ECIS) 2014,Tel Aviv, Izrael 2014.

obszarów tematycznych, które skupiały początkowo 13, a w wersji drugiej[193] modelu 14 obszarów zainteresowań. Zostały one określone na podstawie analizy literatury, głównie rodziny norm ISO/IEC 27k:

Organizacyjne:

1) zarządzanie ryzykiem,
2) polityka bezpieczeństwa,
3) organizacja bezpieczeństwa informacji,
4) bezpieczeństwo zasobów ludzkich,
5) zgodność z wymaganiami prawnymi i własnymi standardami,
6) zarządzanie łańcuchem dostaw (dodany w ISFAM 2.0).

Techniczne:

7) pozyskiwanie, rozwój i utrzymanie systemów informatycznych,
8) kontrola dostępu.

Organizacyjne i techniczne:

9) zarządzanie incydentami związanymi z bezpieczeństwem informacji,
10) zarządzanie ciągłością działania,
11) zarządzanie zmianami.

Wsparcie:

12) bezpieczeństwo fizyczne i środowiskowe,
13) zarządzanie zasobami,
14) architektura.

Na podstawie analizy literatury i przeprowadzonych wywiadów z ekspertami w dziedzinie bezpieczeństwa informacji został przygotowany zestaw pytań zamkniętych (tak/nie). Według twórców metody, za ich pomocą w krótkim czasie można dokonać przeglądu aktualnego stanu organizacji, określić poziom dojrzałości oraz zidentyfikować istniejące braki w zakresie bezpieczeństwa informacji.

W obszarze tematycznym *organizacja bezpieczeństwa informacji* zostały określone przedstawione poniżej wymagania i zadania dla osiągnięcia poszczególnych zdolności[194]:

A. – zaangażowanie kierownictwa w bezpieczeństwo informacji;

[193] M. Spruit, G. Slot, *ISFAM 2.0: Revisiting the Information Security Assessment Model*, [w] *Security Risks: Assessment, Management and Current Challenges*, Springer: Cham, Szwajcaria, 2017.

[194] M. Spruit, M. Roeling, *ISFAM: The information security focus area maturity model*, [w] Proceedings of the European Conference on Information Systems (ECIS) 2014,Tel Aviv, Izrael 2014.

– kierownictwo przydziela zasoby w celu zapewnienia bezpieczeństwa informacji;
– kierownictwo jest formalnie odpowiedzialne za politykę bezpieczeństwa informacji.

B. – koordynacja aspektów bezpieczeństwa informacji w całej organizacji;
– wysokopoziomowe zdefiniowanie ról i obowiązków w zakresie bezpieczeństwa informacji;
– podpisanie umów o poufności ze wszystkimi pracownikami.

C. – dostępny proces autoryzacji przetwarzania informacji;
– kontakt z władzami w sprawie prawa i przepisów;
– zdobywanie wiedzy poprzez bierne uczestnictwo w specjalnych grupach zainteresowań.

D. – zdobywanie wiedzy poprzez aktywne uczestnictwo w specjalnych grupach zainteresowań;
– regularny przegląd stanu bezpieczeństwa informacji;
– ryzyko związane z podmiotami zewnętrznymi jest regularnie identyfikowane i aktualizowane.

ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management				A		B		C			D		
Policy Development			A		B						C		
Organizing Information Security		A			B					C		D	
Human Resource Security				A		B		C		D			
Compliance				A		B						C	
Supply Chain Management				A		B		C			D		
Technical													
Identity and access management					A		B		C		D		
Secure software development					A		B			C		D	
Organizational and Technical													
Incident management			A			B			C			D	
Business Continuity Management				A		B		C			D		E
Change Management				A		B		C		D			
Support													
Physical and environmental security						A		B		C			D
Asset Management			A				B			C		D	
Architecture				A		B			C		D		
	Design					*Implementation*		*Operational Effectiveness*			*Monitoring*		

Rysunek 1.14. Macierz modelu ISFAM 2.0. (ang. Information Security Focus Area Maturity)
Źródło: M. Spruit, G. Slot, ISFAM 2.0: Revisiting the Information Security Assessment Model, [w] Security Risks: Assessment, Management and Current Challenges, Springer: Cham, Szwajcaria 2017.

Rysunek 1.14 przedstawia narzędzie modelu i przykładowe wyniki badań. Organizacja w obszarze *organizacji bezpieczeństwa informacji* osiągnęła wymagania dla zdolności na poziomie C i dziesiąty poziom dojrzałości – jest to jeden z lepiej rozwiniętych obszarów. W *zarządzaniu zasobami* badanej organizacji nie udało się osiągnąć zdolności na poziomie A, również poziom dojrzałości w tym obszarze był najniższy (poziom 1.).

Omawiana metoda określa różne skale poziomów dojrzałości dla odmiennych obszarów zainteresowania. Ich pogrupowanie i zestawienie w macierzy z innymi obszarami daje możliwość zrównoważonego i stopniowego doskonalenia procesów związanych z bezpieczeństwem informacji. Według zwolenników metody takie podejście zmniejsza ryzyko skupienia się na rozwoju jednego obszaru zainteresowania.

1.3.4. Porównanie modeli oceny dojrzałości bezpieczeństwa informacji

Przedstawione w niniejszym podrozdziale modele dojrzałości reprezentują trzy typy modeli występujące w literaturze. COBIT PM i C2M2 to modele wzorujące się na CMM. Pomimo różnic w liczbie poziomów najniższy poziom w obu to brak odpowiednich działań lub wykonywanie ich w sposób doraźny, natomiast najwyższy poziom charakteryzuje się pełną kontrolą nad procesami oraz wdrożonymi mechanizmami doskonalenia. Główna różnica pomiędzy tymi modelami polega na obszarze, na którym się koncentrują. Pierwszy z nich kładzie nacisk na ocenę podejmowanych działań w ramach praktyk zarządczych i zorientowany jest na ocenę dojrzałości zarządzania bezpieczeństwem informacji w organizacji. Drugi koncentruje się na bezpieczeństwie technicznym[195], cyberbezpieczeństwie. To bezpieczeństwo infrastruktury krytycznej jest w centrum uwagi C2M2, co wynika między innymi z faktu, że organizacje, takie jak DOE, ONG SCC, mają wpływ na pracę nad modelem.

Trzeci model to przykład odmiennego podejścia do oceny dojrzałości. ISFAM, bez zdefiniowanych stałych poziomów, zapewnia bardzo zindywidualizowane podejście, umożliwiające zidentyfikowanie luk, w celu poprawy bezpieczeństwa informacji organizacji[196]. Wadą modelu jest utrudnienie w ustaleniu przez zewnętrznych interesariuszy, czy organizacja reprezentuje akceptowalny poziom bezpieczeństwa.

[195] M. Siponen, *Towards*…, op. cit., s. 210–224; A. Kaczmarek, op. cit.

[196] B. Yigit Ozkan, M. Spruit, R. Wondolleck, V. Burriel Coll, *Modelling adaptive information security for SMEs in a cluster*, Journal of Intellectual Capital, 2019, Vol. 21, No. 2, s. 235–256.

Z analizy literatury[197] wynika, że występuje zainteresowanie naukowców, praktyków opisanymi modelami oraz że są one ciągle rozwijane i dostosowywane do zmieniającego się otoczenia.

Najczęściej wymieniane w literaturze są modele opracowane i finansowane przez podmioty państwowe i międzynarodowe organizacje normalizacyjne (COBIT PM, C2M2). COBIT PM[198] jest z kolei najczęściej cytowanym modelem dojrzałości w zakresie zarządzania bezpieczeństwem informacji w organizacjach, które nie zarządzają tzw. infrastrukturą krytyczną. Mając to na uwadze, w przeprowadzonym badaniu sądów administracyjnych zastosowano podejście oparte na tym modelu.

[197] B. Yiğit Özkan, S. Lingen, M. Spruit, *The Cybersecurity Focus Area Maturity (CYSFAM) Model*, Journal of Cybersecurity and Privacy, 2021, Vol. 1. s. 119–139; A. Kaczmarek, op. cit.; A.M. Rea-Guaman, T. San Feliu, J.A. Calvo-Manzano, I.D. Sanchez-Garcia, *Comparative Study of Cybersecurity Capability Maturity Models*, Conference: International Conference on Software Process Improvement and Capability Determination, September 2017.; N. Qodarsih, S.B. Yudhoatmojo and A.N. Hidayanto, *Master Data Management Maturity Assessment: A Case Study in the Supreme Court of the Republic of Indonesia*, 2018 6th International Conference on Cyber and IT Service Management (CITSM), Parapat, Indonesia, 2018, s. 1-7; Ch. Schmitz, M. Schmid, D. Harborth, S. Pape, *Maturity Level Assessments of Information Security Controls: An Empirical Analysis of Practitioners Assessment Capabilities*, „Computers & Security" 2021, 108, 102306.

[198] S. Al Ghamdi, K. Win, E. Vlahu-Gjorgievska, op. cit.

2. Organizacyjno-kulturowe uwarunkowania zarządzania bezpieczeństwem informacji

2.1. Organizacja i organizowanie

„Organizacja to twór społeczny, złożony z ludzi, którzy łączą swe wysiłki w urzeczywistnieniu wspólnych celów”[199]. Organizacja jest podstawowym pojęciem w naukach o zarządzaniu i jakości. Nadal, biorąc pod uwagę sformułowane ponad 30 lat temu stwierdzenie Charlsa Perrowa[200], można powiedzieć, że współcześnie żyjemy w „świecie organizacji”. Przybierają one różne formy, stopnie złożoności, mają rozmaite cele oraz są obecne w różnorakich obszarach życia społecznego. Jednostki organizują się, między innymi po to, aby osiągnąć rezultaty, których nie można osiągnąć, działając samodzielnie, aby utrwalić wyniki swojej działalności. „Nauka, wiedza, technologia, cywilizacja – wszystko to są zorganizowane sposoby radzenia sobie ludzi z rzeczywistością, przekazywane w zorganizowany sposób z miejsca na miejsce i z pokolenia na pokolenie”[201]. Organizacja jest przedmiotem zainteresowania wielu nurtów naukowych i paradygmatów, w tym między innymi: prakseologii, nurtu systemowego, nurtu kulturowego oraz paradygmatu interpretatywnego[202].

Tadeusz Kotarbiński traktował organizację jako byt rzeczywisty w czasie i przestrzeni. Sformułował on koncepcję organizacji rozumianej jako: „pewien rodzaj całości ze względu na stosunek do niej jej własnych elementów, mianowicie taką całość, której wszystkie składniki współprzyczyniają się do powodzenia całości”[203]. Można również opisywać organizację w kategoriach atrybutowych, czyli traktować ją jako cechy rzeczy czy całości. Zwolennikiem takiego podejścia był Jan Zieleniewski. Twierdził on, że szczegółowo opisując organizację, ustanawiamy jej strukturę organizacyjną[204]. Nurt prakseologiczny[205], oprócz definicji rzeczowych i atrybutowych,

[199] M. Bielski, *Organizacje: istota, struktury, procesy*, Wyd. III, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2001, s. 8.

[200] C. Perrow, *A Society of Organizations*, „Theory and Society” 1991, vol. 20, nr 6, 1991.

[201] M. Kostera, B. Glinka, *Wstęp*, [w:] *Nowe kierunki w organizacji i zarządzaniu* (red.) M. Kostera, B. Glinka Wyd. II, Wolters Kluwer, Warszawa 2016, s. 21.

[202] Ł. Sułkowski, *Organizacja jako przedmiot badań nauk o zarządzaniu*, „Przedsiębiorczość i Zarządzanie” 2012, tom XIII, zeszyt 2, Wydawnictwo SAN, Łódź 2012, s. 10.

[203] T. Kotarbiński, *Traktat o dobrej robocie*, Zakład Narodowy im. Ossolińskich, Wrocław-Warszawa 1958, s. 75.

[204] M. Bielski, op. cit., s. 74.

[205] „Nauka o sprawności działań, którą Kotarbiński zaczął tworzyć przed I wojną światową (*Szkice praktyczne* 1919, *Czyn* 1934), a dojrzały jej system przedstawił w *Traktacie o dobrej robocie* (1955, wydanie 8, 2000) oraz w wielu innych pracach, proponując podstawową terminologię, ustalając zakres i miejsce prakseologii w: metodologii (metodologia ogólna), etyce (część interesująca się sprawnością po ocenie godziwości), filozofii (teoria praktyki lub praktyczności). Kotarbiński zapoczątkował jeden

mówi o definicjach czynnościowych, które ujmują organizację jako czynność organizowania. Jej przykładem jest definicja amerykańskiego teoretyka organizacji i zarządzania Charlesa Barnarda, opisująca: „organizację jako system[206] świadomie skoordynowanych działań lub sił dwu lub więcej ludzi”[207].

Andrzej Koźmiński i Dominika Latusek-Jurczak[208] przedstawili typologię i chronologię rozwoju teorii organizacji, zastrzegając, że jest niepełna i subiektywna oraz że poszczególne kierunki charakteryzują się różnym stopniem teoretycznej dojrzałości (Tabela 2.1). Jako pierwsza zamieszczona jest wizja organizacji z daleko posuniętym podziałem pracy, wąską specjalizacją pracowników z próbą standaryzacji i formalizacji metod pracy. Ma to się przysłużyć unikaniu nieprzewidywalnych zachowań ludzi, czym organizacja upodabnia się do maszyny. Zestawienie kończy perspektywa organizacji jako sieci czasowych i zmiennych związków interpersonalnych, międzyorganizacyjnych tworzonych na potrzeby konkretnego działania, w przypadku którego istotne są posiadane przez tworzących sieć zasoby oraz wiedza i istotniejsze są więzi nieformalne niż formalne. Duże znaczenie w tej wizji organizacji mają: chęć dzielenia się wiedzą, zaufanie, lojalność, status i reputacja.

Tabela 2.1. Główne kierunki i nurty w teorii organizacji

Kierunek	Wyzwania i praktyki	Wizja organizacji
Naukowe zarządzanie (przełom XIX i XX w.)	niska wydajność pracy robotników, niskie płace (popyt), opanowanie technologii i wielkości zakładów przemysłowych	mechanistyczna, zdeterminowana przez technologię i umiejętności; poszukiwanie korzyści skali, specjalizacji, standaryzacji, centralizacji, koncentracji i synchronizacji
Administracja (początek XX w.)	nieefektywność struktur administracyjnych	mechanistyczna, zdeterminowana przez przepisy i formalizację
Stosunki międzyludzkie (lata 30. i 40. w USA, lata 50. w Europie XX w.)	niezadowolenie z pracy i niskie morale, niski poziom identyfikacji z pracodawcą	organizacja jako „mieszanka” struktury formalnej i nieformalnej opartej na stosunkach międzyludzkich
Podejście systemowe (lata 50. i 60. XX w.)	suboptymalizacja, trudności w zarządzaniu wielkimi, niejednorodnymi organizacjami	organizacje jako systemy społeczno-techniczne podlegające regulacji, sterowaniu i projektowaniu

z działów prakseologii — ogólną teorię walki; za prakseologię uważał teorię organizacji (po jej rozbudowaniu w naukę organizacji i zarządzania, do czego się w znacznej mierze przyczynił, umieszczał prakseologię wśród nauk organizacyjnych). Propozycja Kotarbińskiego była całkowicie oryginalna”, źródło: https://encyklopedia.pwn.pl/haslo/prakseologia;4009631.html, dostęp: 5.02.2024 r.

[206] System – „zestaw składników, między którymi zachodzą wzajemne stosunki i gdzie każdy składnik połączony jest z każdym innym bezpośrednio lub pośrednio”, źródło: R.L. Ackhoff, *O system pojęć systemowych*, Prakseologia 1973, nr 2, s. 145.

[207] Ch. Barnard, *Funkcje kierownicze*, AE w Krakowie, Czytelnik, Kraków 1997.

[208] A.K. Koźmiński, D. Latusek-Jurczak, op. cit., s. 20.

Gra organizacyjna (lata 80.)	wewnętrzne i międzyorganizacyjne antagonizmy, rozgrywki, konflikty	organizacje jako przestrzeń gry o zasoby, władzę, informacje
Równowaga organizacyjna	zakłócenia równowagi funkcjonalnej, społecznej i materialnej, zewnętrznej i wewnętrznej	organizacje jako systemy zmierzające do równowagi; zakłócenia równowagi jako czynniki dynamiki i zmiany
Sieć	trudności w zarządzaniu współpracą, informacją i wiedzą w układach wewnątrz- i międzyorganizacyjnych o różnym stopniu spójności	organizacja jako sieć powiązań o zmiennej konfiguracji

Źródło: A.K. Koźmiński, D. Latusek-Jurczak, Rozwój teorii organizacji. Od systemu do sieci, Poltex, Warszawa 2017, s. 20.

Do organizacji typu sieciowego można zaliczyć organizację wirtualną, o której, jak twierdzą William Davidow i Michael Malone, nie można jednoznacznie powiedzieć, czym jest[209]. Może tworzyć ją sieć organizacji, zespołów i osób zorganizowanych w luźno powiązane struktury, które mają wspólny cel, jakim jest wytwarzanie dóbr lub świadczenie usług. Organizacja wirtualna ma jasno określoną specjalizację i wykorzystuje rozwinięte technologie informacyjne oraz elektroniczne w zarządzaniu. Jej struktura jest macierzowa i zdecentralizowana, a ponadto mogą w niej zaniknąć takie cechy, jak lojalność wobec współpracowników, akceptacja wizji i misji organizacji[210].

Monika Kostera zauważa, że podobnie jak wiele zjawisk społecznych i ekonomicznych, organizacje można rozpatrywać na dwa zasadnicze sposoby: jako stan lub jako proces[211]. Jedną z najczęściej przytaczanych definicji organizacji jako stan jest ta wywodząca się z podejścia systemowego[212]. Zakłada ona, że organizacje są złożonymi systemami otwartymi, tj. pozostającymi w ciągłej interakcji z otoczeniem, składającymi się z elementów bezpośrednio i pośrednio ze sobą powiązanych. Podejście systemowe zostało zapoczątkowane przez Ludwiga von Bertalanffy'ego[213] – twórcę

[209] W.H. Davidow, M.S. Malone, *The Virtual Corporation: Structuring and Revitalizing the Corporation for the 21st Century*, Harper Collins, New York 1992.

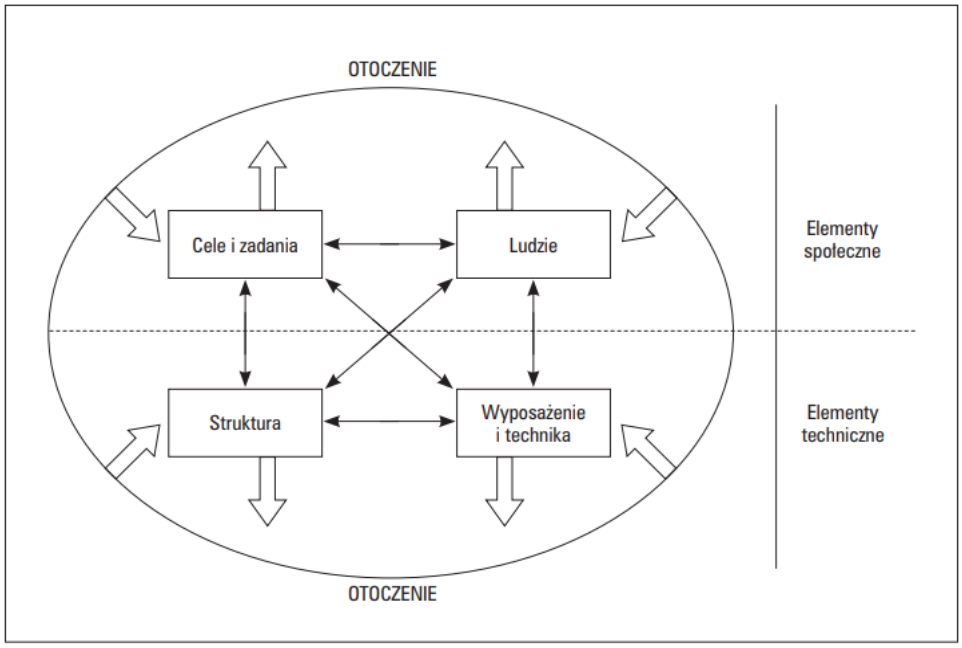
[210] M. Bednarek, *Kierunki rozwoju zarządzania we współczesnym przedsiębiorstwie*, [w:] *Kulturowa zmienność systemów zarządzania*, (red.) Ł. Sułkowski, M. Bednarek, A. Parkes, Difin, Warszawa 2016, s. 33.

[211] M. Kostera, B. Glinka, op. cit., s. 15.

[212] R.L. Ackoff, *O systemie pojęć systemowych*, Prakseologia 1973, nr 2; W. Piotrowski, *Organizacje i zarządzanie – kierunki, koncepcje, punkty widzenia*, [w:] *Zarządzanie: Teoria i praktyka*, (red.) A. Koźmiński, W. Piotrowski, Warszawa 2002, s. 693.

[213] L. von Bertalanffy, *General System Theory*, George Brazziler, New York 1968.

ogólnej teorii systemów[214] i Norberta Wienera[215] – twórcę cybernetyki. Elementami systemu organizacji są: cele i zadania, ludzie, wyposażenie oraz techniki i struktury formalne[216]. Zależności oraz umowny podział na elementy społeczne i techniczne przedstawili w swojej pracy Andrzej Koźmiński i Krzysztof Obłój (Rysunek 2.1).



Rysunek 2.1. Organizacja jako system społeczno-techniczny
Źródło: A.K. Koźmiński, K. Obłój, Zarys teorii równowagi organizacyjnej, PWE, Warszawa 1989, s. 21.

Organizacje są systemami społeczno-technicznymi, w których elementy społeczne, ludzie oraz cele i zadania, są systemami probabilistycznymi, tzn. ich zachowanie można przewidzieć tylko z pewnym prawdopodobieństwem, a elementy techniczne, struktura oraz wyposażenie i technika, są deterministyczne, tzn. ich zachowanie jest w pełni przewidywalne. Organizacja jako ogół jest probabilistyczna. Zgodnie z tym poglądem organizacja powinna być postrzegana jako całość (za Arystotelesem) – system jest czymś więcej niż sumą jego części[217]. Działania

[214] Ogólna teoria systemów została sformułowana w latach 30. XX w. przez niemieckiego biologa Ludwiga von Bertallanfy'ego. Jego zdaniem system można zdefiniować jako: „zbiór elementów pozostających we wzajemnych relacjach", L. von Bertallanfy, *Ogólna teoria systemów. Podstawy, rozwój, zastosowania*, PWE, Warszawa 1984. L. von Bertalanffy założył, że: „całość jest czymś więcej niż sumą części", co uniemożliwia wyjaśnienie zachowania się „całości" wyłącznie na podstawie charakterystyk elementów składowych.

[215] N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine (1948)*, MIT Press, Wyd. II, Massachusetts 1961.

[216] H.J. Leavitt, *Applied organizational change in industry: Structural and humanistic approaches*, Carnegie Institute of Technology, Graduate School of Industrial Administration, 1962.

[217] W. Piotrowski, *Organizacje i zarządzanie – kierunki, koncepcje, punkty widzenia*, [w:] *Zarządzanie: Teoria i praktyka*, (red.) A. Koźmiński, W. Piotrowski, Warszawa 2002, s. 694, 695.

podejmowane w jednym podsystemie mogą mieć wpływ na inne podsystemy. Co więcej, całość wywiera większy wpływ na części niż części na całość.

Badacz organizacji Karl Weick jest chyba najczęściej cytowanym przedstawicielem nurtu, myślenia o organizacji jako procesie[218]. Twierdzi on, że procesy występujące w organizacji polegają na łączeniu: „ciągłych niezależnych działań w sensowne sekwencje, czyli generowaniu mających sens wyników"[219]. Efektem organizowania są połączone ze sobą cykle, które przyjmują formę pętli. Pierwszym etapem jest inscenizacja (ang. *enactmen*t), która polega na wybraniu fragmentu otoczenia i urealnieniu go poprzez podjęcie działania. Drugim etapem jest selekcja (ang. *selection*), gdy osoby lub grupy tworzące organizację próbują zmniejszyć niepewność, obejmując działania swoimi schematami poznawczymi. Umożliwia im to nadanie działaniom sensu. Ostatnim etapem jest przechowywanie (ang. *retention*), w którym wyniki działań zapamiętywane są w schematach poznawczych. Na każdym etapie osoby lub grupy starają się mieć poczucie sensu dla całości działań. Według K. Weicka istnieje wiara w ciągłość i stabilność procesów i jest ona tak silna, że ludzie często traktują procesy organizacyjne jako coś stabilnego, trwałego.

Różnorodność organizacji skłoniła badaczy do podejmowania prób uporządkowania ich zbioru, co zaowocowało powstaniem wielu typologii. Jedną z systematyk zaproponowali Daniel Katz i Robert L. Kahn[220], gdzie wyznacznikiem jest funkcja pełniona w społeczeństwie. Badacze podzielili organizacje na:

- produkcyjne lub gospodarcze, które zajmują się dostarczaniem towarów i usług, np. zakłady przemysłowe;
- scalające, zajmujące się socjalizacją i szkoleniem ludzi do odgrywania ról w innych organizacjach i w całym społeczeństwie, np. szkoły, związki wyznaniowe;
- adaptacyjne, które mają na celu tworzenie wiedzy, innowacyjnych rozwiązań problemów, np. laboratorium badawcze, uniwersytety jako organizacje badawcze;

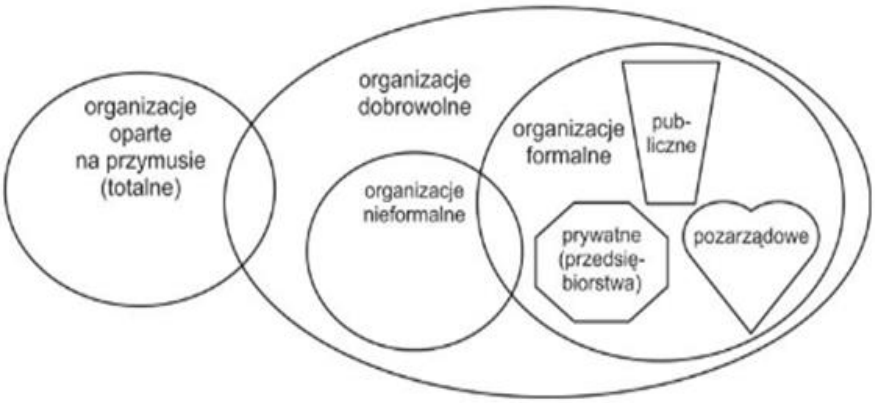
[218] M. Kostera, *Antropologia organizacji. Metodologia badań terenowych*, Wydawnictwo Naukowe PWN, Warszawa 2003, s. 68.

[219] K.E. Weick, *The Social Psychology of Organizing*, Random House 1979, s. 3; M. Kostera, *Studium przypadku a edukacja zarządzania,* [w:] *O zarządzaniu historie niezwykłe: studia przypadków z zarządzania humanistycznego*, (red.) M. Kostera, Difin, Warszawa 2014, s. 16.

[220] D. Katz, R.L. Kahn, *The social psychology of organizations*, Wyd. II, Wiley, New York 1978; polskie wydanie, tłumaczenie B. Czarniawska: D. Katz, R.L. Kahn, *Społeczna psychologia organizacji*, PWN, Warszawa 1979, s. 200–229.

– polityczne, mające związek z koordynacją i kontrolą ludzi oraz zasobów, a także negocjowaniem między konkurującymi ze sobą grupami, np. agencje rządowe, związki zawodowe.

W niniejszej pracy został przyjęty podział organizacji zaproponowany przez Monikę Kosterę, zaprezentowany poniżej (Rysunek 2.2). Wynika to z faktu, iż wojewódzkie sądy administracyjne są organizacjami dobrowolnymi, formalnymi i publicznymi.



Rysunek 2.2. Typy organizacji
Źródło: M. Kostera, Antropologia organizacji. Metodologia badań terenowych, Wydawnictwo Naukowe PWN, Warszawa 2003, s. 76.

Organizacje oparte na przymusie to szczególny typ organizacji, które mogą działać w dowolnym sektorze aktywności społeczno-gospodarczej i posiadać różne cele. Wspólną ich cechą jest odizolowanie członków organizacji od otoczenia. Są nimi na przykład: więzienia, obozy koncentracyjne, okręty wojenne, a także szkoły z internatem. Głównym dobrowolnych podziałem organizacji jest podział na organizacje nieformalne i formalne. Pierwsze powstają, ponieważ ludzie odczuwają potrzebę organizowania się z innych przyczyn, niż chęci realizacji formalnych celów. Organizacje te mogą dotyczyć również: więzi służbowych, więzi funkcjonalnych, sposobu działania, procesów pracy. Organizacje formalne, które tworzone są z myślą o osiągnięciu własnych celów, można podzielić według ich własności na organizacje sektora prywatnego, publicznego i pozarządowego. Pierwsze z nich to przede wszystkim podmioty założone przez osoby prywatne, działające na rynku, nastawione na zyski dla ich właścicieli. Sektor publiczny[221], m.in. wojewódzkie sądy

[221] Definicja sektora publicznego w Polsce: „Ogół podmiotów gospodarki narodowej grupujących własność państwową (Skarbu Państwa i państwowych osób prawnych), własność jednostek samorządu terytorialnego lub samorządowych osób prawnych oraz »własność mieszaną« z przewagą kapitału (mienia) podmiotów sektora publicznego.
Dodatkowe wyjaśnienia metodologiczne:

administracyjne, które są podmiotem badań podjętych w dysertacji, to różnego rodzaju urzędy i inne organizacje, które są własnością lub współwłasnością państwa. Organizacjami pozarządowymi[222] są prywatne podmioty, powstałe z inicjatywy ich założycieli, które nie działają w celu osiągnięcia zysku, a na rzecz wybranego interesu. Mogą one generować przychód, który jest przeznaczany na realizację formalnych celów organizacji. Podmioty te mogą być dotowane ze środków publicznych.

Jedną z metod wpływania na organizację jest zarządzanie. Sven-Erik Sjöstrand stwierdził, że zarządzanie jest szczególnym przypadkiem organizowania, w którym jednostki i zasoby są łączone w skoordynowany sposób, aby osiągnąć cel[223]. Za zarządzanie może być odpowiedzialna osoba lub grupa. Potrzeba zarządzania często pojawia się, gdy ludzie dostrzegają rosnącą niepewność. Jest ona często postrzegana jako poważne zagrożenie, z którym należy sobie poradzić, a ludzie chcą móc reagować na nią w kolektywny, zorganizowany sposób[224]. Procesy organizacyjne są wieloznaczne i złożone, poza formalnymi celami realizują również cele związane z zaspokojeniem różnych potrzeb rozmaitych grup interesariuszy.

W swojej pracy Jolanta Bieńkowska i Czesław Sikorski wymienili strukturę, strategię i kulturę organizacyjną jako instrumenty zarządzania, procedury działania zaś przypisali do struktury dynamicznej, która mieści się w ogólnym pojęciu struktury organizacyjnej[225]. Samo pojęcie zarządzania zdefiniowali jako proces: „kształtowania w przestrzeni organizacyjnej instrumentów i zależności między nimi, służących takiemu

---

W przypadku równego udziału kapitału publicznego (50% stanowi łączny udział własności: Skarbu Państwa, państwowych osób prawnych, jednostek samorządu terytorialnego) i prywatnego (50% stanowi łączny udział własności: krajowych osób fizycznych, pozostałych krajowych jednostek prywatnych, osób zagranicznych) podmiot gospodarki narodowej zaliczany jest do sektora prywatnego", źródło: GUS, https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/2961,pojecie.html, dostęp: 5.02.2024 r.

[222] „2. Organizacjami pozarządowymi są:

1) niebędące jednostkami sektora finansów publicznych w rozumieniu ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych lub przedsiębiorstwami, instytutami badawczymi, bankami i spółkami prawa handlowego będącymi państwowymi lub samorządowymi osobami prawnymi,

2) niedziałające w celu osiągnięcia zysku

– osoby prawne lub jednostki organizacyjne nieposiadające osobowości prawnej, którym odrębna ustawa przyznaje zdolność prawną, w tym fundacje i stowarzyszenia, z zastrzeżeniem ust. 4" (przy czym niektórych przepisów ustawy nie stosuje się do fundacji publicznych i fundacji partii politycznych), źródło: art. 3 ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (t.j. Dz. U. z 2023 r., poz. 571).

[223] S.E. Sjöstrand, *Företagsledning*, [w:] *Organisationsteori pa svenska*, (red.) B. Czarniawska, Liber, Malmö 1998 , s. 22–42.

[224] M. Kostera, *Antropologia organizacji: Metodologia badań terenowych*, PWN, Warszawa 2003, s. 73.

[225] J. Bieńkowska, C. Sikorski, *Ewolucja*…, op. cit., s. 9. Struktura organizacyjna: struktura organizacyjna w ujęciu statycznym: uprawnienia decyzyjne i podział pracy w organizacji; struktura organizacyjna w ujęciu dynamicznym: struktura procesów, czyli relacji między przebiegami informacji i zasileń w systemie organizacyjnym.

sposobowi wykorzystania posiadanych zasobów, który w danych warunkach otoczenia umożliwia właściwe realizowanie nadrzędnego celu organizacji, jakim jest misja"[226]. Misja w powyższej definicji rozumiana jest jako oceniany pozytywnie końcowy, a zarazem powtarzalny, efekt działalności organizacji.

2.2. Kultura organizacyjna instrumentem zarządzania

O kulturze organizacyjnej mówi się jako o trzecim instrumencie zarządzania, obok struktury i strategii organizacyjnej. Można spojrzeć na kulturę w kontekście przestrzeni organizacyjnej[227], rozumianej jako zależność między elementami, którymi są zewnętrzne uwarunkowania realizacji misji organizacji, tj. techniką i rynkiem, oraz wewnętrznymi instrumentami zarządzania, tj. strukturą, strategią i kulturą. W przestrzeni tej przebiega proces zarządzania organizacją, który polega na wykorzystywaniu zasobów w celu realizacji misji w określonych warunkach otoczenia[228]. Kultura rozumiana jest tu jako część organizacji, jako zmienna wewnętrzna wchodząca w relacje z innymi zmiennymi. Istniejące zależności pomiędzy elementami przestrzeni organizacyjnej mogą ulegać zmianie.

J. Bieńkowska i C. Sikorski wskazują trzy typy przestrzeni organizacyjnej[229]. Różnią się one tym, że w każdym z typów decydującą rolę odgrywa inny wewnętrzny instrument zarządzania. Za instrumenty wewnętrzne naukowcy uznają: strukturę, strategię i kulturę organizacyjną, które powinny być zaprojektowane w taki sposób, aby organizacja mogła pełnić swoją misję przy możliwościach i ograniczeniach, jakie stwarza otoczenie. Zauważają, że na zmiany w przestrzeni organizacyjnej decydujący wpływ mają zewnętrzne elementy i że wpływ pierwotny oraz rozstrzygający ma technika. Uwarunkowania techniczne w otoczeniu organizacji decydują o sposobie jej funkcjonowania, który następnie jest korygowany przez rynek, na którym funkcjonuje organizacja.

W okresie industrialnym, na przełomie XIX i XX w., zaczęła dominować struktura organizacyjna nad strategią i kulturą, a rynek w tym okresie był duży i chłonny. Otoczenie zewnętrzne charakteryzowało się: stabilnością zaopatrzenia i sprzedaży, nieskomplikowanymi technologiami produkcji, brakiem dostępu do

[226] Ibidem.

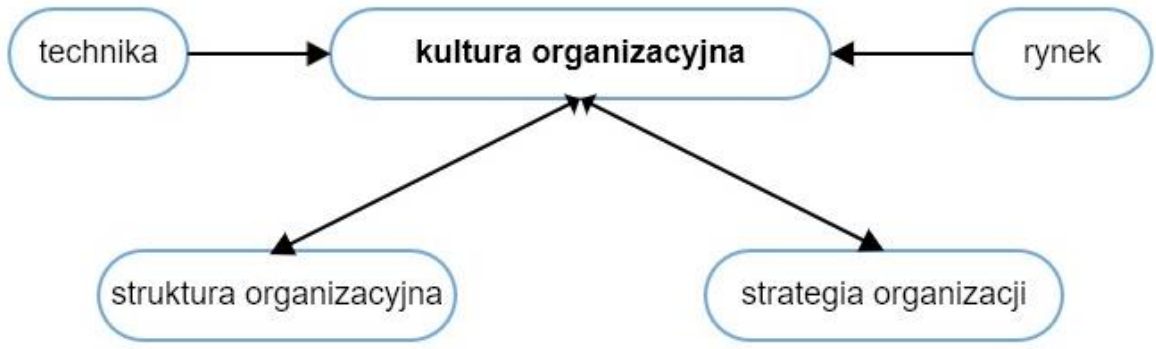
[227] J. Biernat, *Zarządzanie przestrzenią organizacji*, „Przegląd Organizacji" 2001, 24(2), s. 8–11.

[228] A.K. Koźmiński, D. Latusek-Jurczak, op. cit., s. 44; J. Bieńkowska, C. Sikorski, *Ewolucja*…, op. cit., s. 31; G. Aniszewska, I. Gielnicka, *Firma to ja, firma to my. Poradnik kultury organizacyjnej firmy*, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 1999, s. 44.

[229] J. Bieńkowska, C. Sikorski, *Ewolucja*…, op. cit., s. 31.

wykwalifikowanej kadry pracowniczej. Struktura organizacyjna decydowała o wydajności pracy, która była główną wartością organizacji w okresie industrialnym. Pracownicy wykonywali swoje czynności zgodnie z procesem zaprojektowanym przez kadrę zarządzającą. Uważano, że specjalizacja, prowadząca do zawężenia zakresu czynności, i standaryzacja procesów wykonywanych przez pracownika sprzyjały wydajności pracy. Strategia i kultura organizacyjna miały zapewniać stabilność funkcjonowania organizacji, która przez mało elastyczną strukturę nie mogłaby reagować na zmiany w otoczeniu. J. Bieńkowska i C. Sikorski przyjmują, że kultura organizacyjna w tym okresie była: „kulturą restrykcyjną charakteryzującą się identyfikacją kolektywną, orientacją na przyszłość oraz dużym dystansem władzy”[230].

W okresie modernistycznym (II poł. XX w.) przeważał typ przestrzeni, gdzie strategia organizacji była dominująca, a organizacje ukierunkowane były na szybkie przystosowanie się do wymagań rynku. Po II wojnie światowej nastąpił dynamiczny rozwój techniki i przyrost uczestników rynku, co zwiększyło konkurencję. Najważniejsza w tym okresie była strategia umożliwiająca wykorzystanie szans na rozwój organizacji, które się pojawiają w otoczeniu zewnętrznym. Konsekwencją braku właściwej strategii może być zakończenie działalności. Wymienione uwarunkowania zewnętrzne wymagały od organizacji większej elastyczności w tworzeniu struktury, gotowości do zatrudnienia „uniwersalnego” pracownika, który w krótkim czasie jest w stanie przystosować się do zmian. Kultura organizacyjna stała się bardziej liberalna, tolerancyjna, pozwala na wyrażanie swoich poglądów, wartości i celów.



Rysunek 2.3. Przestrzeń organizacyjna z dominacją kultury organizacyjnej
Źródło: J. Bieńkowska, C. Sikorski, Ewolucja zarządzania. Dyktat struktury, strategii i kultury, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2016, s. 31.

[230] J. Bieńkowska, C. Sikorski, *Ewolucja*…, op. cit., s. 48.

Rysunek 2.3 przedstawia typ przestrzeni organizacyjnej, który zaczął być widoczny w latach 90. XX w. i staje się dominujący w warunkach rynku elektronicznego, w tak zwanym okresie informacyjnym[231]. Sposób pełnienia misji jest uzależniony od wzorów myślenia i zachowania ludzi w organizacji. Kultura przestaje być w tym typie przestrzeni organizacyjnej elementem dostosowanym do strategii i struktury, a staje się czynnikiem wyznaczającym cechy tych dwóch elementów. Okres informacyjny charakteryzuje się hiperelastycznością[232] rynku oraz nastawieniem na projekty. Szczególne znaczenie przypisuje się komunikacji społecznej, dzięki której tworzone są sieci współpracy międzyludzkiej wewnątrz organizacji i współpracy międzyorganizacyjnej w celu realizacji krótkotrwałych projektów[233]. Dominuje w tym okresie kultura pragmatyczna, która promuje takie wartości, jak: zaufanie, otwartość, wiarygodność i odpowiedzialność[234]. Są one podstawą sprawnego funkcjonowania organizacji w różnorodnej pod względem kulturowym sieci powiązań[235].

2.3. Paradygmaty badania kultury organizacyjnej

Tematem tego podrozdziału jest analiza występujących w literaturze rozważań na temat kultury organizacyjnej, kształtowania się koncepcji jej wpływu na organizację i perspektyw zarządzania nią. Zagadnienie kultury organizacyjnej jest niezwykle istotne w kontekście zarządzania organizacjami. Poddając analizie rozwój koncepcji kulturowych w naukach o zarządzaniu, można zaobserwować wzrost złożoności teorii i metod badawczych przy jednoczesnym braku jednego, powszechnie akceptowanego

[231] A.S. Duff, *Castells versus Bell: A comparison of two grand theorists of the information age*, European Journal of Social Theory, 26(1), 2023, s. 90-108.

[232] „Termin hiperelastyczność jak dotąd nie został zdefiniowany w literaturze. Używa się go intuicyjnie. Skoro w drugiej połowie XX wieku organizacje działające na konkurencyjnych rynkach musiały wykształcić zdolność do elastycznego działania, czyli zdolność do szybkiego wprowadzania zmian w działaniu, to rosnący stopień złożoności, nieprzewidywalności i nieciągłości zdarzeń w otoczeniu organizacji wymaga użycia przyrostka hiper- w celu podkreślenia wyższego stopnia tych zdolności", J. Bieńkowska, C. Sikorski, *Hyperflexibility. A feature of e-commerce organisations*, Management, Vol. 20, 2016, s. 210–223.

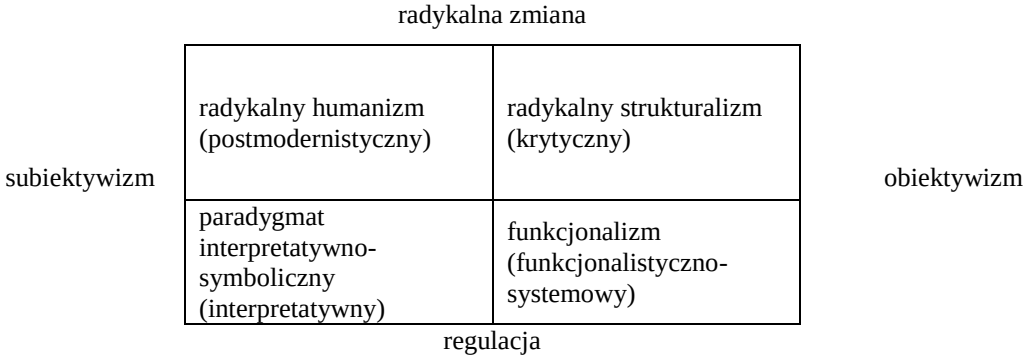
„Hiperelastyczność jest cechą organizacji, które działają na rynku e-commerce i których domeną jest:
– podejmowanie przedsięwzięć biznesowych, motywowanych współpracą w sieci współpracy,
– zdolność do wdrażania różnych rozwiązań organizacyjnych (strategicznych, strukturalnych), które będą najbardziej korzystne z punktu widzenia bieżącej sytuacji, i zdolność do płynnych zmian, a także potrzeby wynikające ze zmieniającej się sytuacji,
– pragmatyczna kultura organizacyjna, promująca zaufanie jako wartość nadrzędną, która jest podstawą sprawnego funkcjonowania organizacji w przestrzeni wirtualnej, i jako normę behawioralną – skupienie na teraźniejszości i indywidualizm w ramach kolektywu; organizacja, która jest w stanie utrzymać wewnętrzną spójność, pozostając otwartą na odmienne zachowania swoich współpracowników", Ibidem.

[233] J. Bieńkowska, C. Sikorski, *Ewolucja*…, op. cit., s. 94.

[234] J. Bieńkowska, C. Sikorski, *Hyperflexibility*…, op. cit., s. 210–223.

[235] A.K. Koźmiński, D. Jemielniak, D. Latusek D., *Współczesne spojrzenie na organizację*, „E-mentor" 2009, nr 3; J. Bieńkowska, C. Sikorski, *Ewolucja*…, op. cit., s. 94.

stanowiska na temat tego, jak rozumieć i badać kulturę. Są badacze, którzy koncentrują się na możliwości jej kształtowania, tak aby wspierała osiąganie celów przez organizację. Inni zaś stają na stanowisku, że kulturę można jedynie obserwować, jej rozwój jest spontaniczny i efekt podejmowanych prób jej zmiany nie jest możliwy do przewidzenia[236].



Rysunek 2.4. Cztery paradygmaty w naukach społecznych
Źródło: na podstawie: G. Burrel, G. Morgan, Sociological Paradigms and Organisational Analysis, Heinemann, London 1979, s. 22; Ł. Sułkowski, Funkcjonalistyczna wizja kultury organizacyjnej w zarządzaniu – dominujący paradygmat i jego krytyka, Wydział Zarządzania UW, Problemy Zarządzania, vol. 11, nr 4 (44), s. 21.

Te różnice w podejściu do badań związane są z przyjmowaniem różnych paradygmatów w rozwijaniu wiedzy w opisywanej dziedzinie. W związku z tym, że badania nad kulturą organizacyjną prowadzone są na pograniczu nauk o organizacji i zarządzaniu, antropologii kulturowej i socjologii, badacze czerpią z osiągnięć wszystkich tych dyscyplin. Stosując koncepcję uporządkowania paradygmatów w naukach społecznych (Rysunek 2.4), którą zaproponowali Gibson Burrella i Gareth Morgan[237], można przyjąć, że badania nad kulturą organizacyjną mogą być prowadzone w czterech paradygmatach w zależności od orientacji społecznej (regulacja kontra radykalna zmiana) i założeń co do roli nauki (subiektywizm kontra obiektywizm). Zestawienie różnic nurtów w badaniu kultury organizacyjnej i informację o ich przedstawicielach ujęto poniżej (Tabela 2.2).

[236] Ł. Sułkowski, *Zmiana kultury organizacyjnej – paradygmaty, modele i metody zarządzania*, [w:] *Metody zarządzania kulturą organizacyjną*, (red.) Ł. Sułkowski, Cz. Sikorski, Wydawnictwo Difin, Warszawa 2014, s. 11; A. Kołodziej-Durnaś, *Kultura organizacji – idea i instrumentalizacja. Socjologiczne studium krytyczne*, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2012, s. 12.

[237] G. Burrel, G. Morgan, *Sociological Paradigms and Organisational Analysis*, Heinemann, London 1979, s. 22. W 2014 r. Gibson Burrell i Gareth Morgan otrzymali nagrodę Joanne Martin Trailblazer American Academy of Management za współautorstwo: „klasycznego już tekstu *Sociological Paradigms and Organisational Analysis*, który popchnął badaczy do konfrontacji z ukrytymi założeniami dominujących paradygmatów w tej dziedzinie i ujawnił, w jaki sposób paradygmaty te wpływają na sposób, w jaki interpretujemy działania organizacyjne i rozwijamy teorię", źródło: https://omt.aom.org/awards/trailblazer-award, dostęp: 5.02.2024 r.

Tabela 2.2. Paradygmaty badania kultury organizacyjnej

Kryterium	**Paradygmat funkcjonalistyczno-systemowy**	**Paradygmat interpretatywny**	**Paradygmat krytyczny**	**Paradygmat postmodernistyczny**
Znaczenie kultury organizacyjnej	Integralność, holizm, spójność kultury	Sieci znaczeń, otwartość interpretacji, podziały i subkultury	Opresyjność, dominacja, indoktrynacja, ukryte nici władzy	Względność interpretacji, subiektywizm
Preferowane rodzaje, metody badań kultury	Obiektywizujące, ilościowe, dominują ankietowe	Subiektywistyczne, jakościowe, dominuje antropologia organizacji i metody tekstualne	Zaangażowane, jakościowe, dominuje action research	Brak metod badawczych *sensu stricto*, glossy, metafory, tekstualizm
Metody zmiany kulturowej	Projektowanie i wdrażanie rozwojowych i optymalizujących zmian kultury	Tworzenie i rozwijanie nowych znaczeń kultury (np. management of meaning, sensemaking)	Wdrażanie emancypacyjnych zmian, np. empowerment, denaturalizacja	Brak metod zmiany *sensu stricto*, pogłębiona refleksja, brak kontroli nad zmianą
Ujęcie procesów kulturowych	1. Kultura organizacyjna rozumiana jako zmienna wewnętrzna wpływająca na efektywność, którą menadżerowie mogą manipulować za pomocą technik organizatorskich. 2. Problemy: modeli, typologii, klasyfikacji, zmiany, efektywności kultury organizacyjnej.	1. Kultura interpretowana jako metafora rdzenna, tzn. organizacja jest kulturą, jest w dużej mierze nieuświadomiona i trudna do kształtowania. 2. Kluczowe problemy zarządzania dotyczą: interakcji, komunikacji, subkultur i kontrkultur, języka, gier organizacyjnych, spontanicznego przekształcania się kultury, tożsamości organizacyjnej, kulturowych barier racjonalności.	1. Kultura jako narzędzie sprawowania władzy i utrzymywania niesprawiedliwej struktury społecznej przez indoktrynację i przemoc symboliczną. 2. Problemy demaskacji i denaturalizacji oraz humanizacji kultury organizacyjnej za pomocą metod emancypacyjnych.	1. Kultura rozumiana wyłącznie metaforycznie i wieloznacznie jako gra, tekst, dyskurs. 2. Ważniejsze problemy dotyczyły: krytyki funkcjonalizmu i imperializmu nauki, dekonstrukcji kultury organizacyjnej, glossowania i studiów kulturowych opartych na relatywizmie poznawczym.
Kluczowe metafory	Maszyna, organizm	Tekst, język, gra językowa	Więzienie, panopticon, kolonizacja umysłów	Happening, kłącze, metanarracja
Przedstawiciele	E. Schein, Ch. Handy, T. Deal, A. Kennedy, P. Bate, A. Pettigrev, G. Hofstede,	G. Morgan, L. Smircich, M.J. Hatch, K.E. Weick, N. Brunsson, J. Vann Maanen, M. Pacanowsky	H. Willmott, M. Alvesson, D. Knights, J. Brewis, J. Gavin, A. Prasad	S. Clegg, G. Burrell, R. Cooper, B. Czarniawska, M. Kostera, P. Boje

Kryterium	Paradygmat funkcjonalistyczno-systemowy	Paradygmat interpretatywny	Paradygmat krytyczny	Paradygmat postmodernistyczny
	C. Sikorski, L. Zbiegień-Maciąg, A. Czerska			

Źródło: opracowanie własne na podstawie: Ł. Sułkowski, Zmiana kultury organizacyjnej – paradygmaty, modele i metody zarządzania, [w:] Metody zarządzania kulturą organizacyjną, (red.) Ł. Sułkowski, C. Sikorski, s. 11–26, Wydawnictwo Difin, Warszawa 2014, s. 14; Ł. Sułkowski, Kultura organizacyjna od podstaw, Społeczna Akademia Nauk, Łódź 2020, s. 24–25.

W podejściu funkcjonalistycznym kulturę organizacyjną traktuje się jako podsystem, który podlega kontroli. Zarządza się nim, tak jak strategią czy strukturą organizacyjną, dążąc do uzyskania równowagi systemowej, a co za tym idzie – do zwiększenia skuteczności i efektywności zarządzania. Zgodnie z podejściem obiektywistycznym w badaniach stosowane są metody ilościowe. Zakłada się możliwość kształtowania kultury przez jej doskonalenie i optymalizację. W nurcie funkcjonalistycznym powstały różne modele[238] i typologie kultur pochodzące z badań etnologicznych. Wśród najbardziej rozpowszechnionych koncepcji[239] są: poziomy kultury zwane „górą lodową" Edgarda Scheina[240], teoria wymiarów kulturowych Geerta Hofstedego[241] oraz „model wartości konkurujących" Kima Camerona i Roberta Quinna[242].

W paradygmacie interpretatywnym opisuje się kulturę: „jako lokalne sensy i wspólnoty znaczeń tworzone przez i dla członków organizacji"[243]. Ujęcie symboliczne traktuje organizację i kulturę jako systemy wspólnych symboli i znaczeń[244]. Zakłada się, że nie można obiektywnie zbadać kultury, gdyż nie jest ona jednolita dla całej

[238] Model – „Teoria skonstruowana w taki sposób, aby można było operatywnie manipulować zmiennymi wchodzącymi w jej skład. Służy nie tylko orientacji w rzeczywistym otoczeniu, ale i zastąpieniu realnego eksperymentu rozumowaniem, polegającym na zmienianiu wartości poszczególnych zmiennych i na sprawdzaniu, jakie konsekwencje wywołuje to w odniesieniu do pozostałych zmiennych", J. Zieleniewski, *Organizacja i zarządzanie*, PWE, Warszawa 1979, s. 44–45.

„Hipotetyczna konstrukcja myślowa, będąca uproszczonym obrazem badanego fragmentu rzeczywistości, stanowi sformalizowane ujęcie pewnej teorii lub sytuacji przyczynowej, w której zakłada się, że generuje on badane dane" J. Apanowicza, *Metodologiczne uwarunkowania pracy naukowej. Prace doktorskie. Prace habilitacyjne*, Difin, Warszawa 2005, s. 113.

[239] Ł. Sułkowski, *Zmiana*…, op. cit., s. 17.

[240] E.H. Schein, *Organizational culture and leadership*, Edycja 3, Jossey-Bass, 2004, s. 26.

[241] G. Hofstede, *Culture's Consequences: International differences in work-related values*, Sage Publications, Beverly Hills 1980.

[242] K.S. Cameron, R.E. Quinn, *Kultura organizacyjna – diagnoza i zmiana. Model wartości konkurujących*, Oficyna Ekonomiczna, Kraków 2003.

[243] Ł. Sułkowski, *Zmiana*…, op. cit., s. 14.

[244] M. Kostera, *Postmodernizm w zarządzaniu*, Polskie Wydawnictwo Ekonomiczne, Warszawa 1996, s. 64.

organizacji (występują subkultury[245]) oraz podlega ciągłym niekontrolowanym zmianom. Kultura interpretowana jest jak metafora rdzenna, co oznacza, że każda organizacja jest kulturą oraz jest formą ludzkiej ekspresji[246]. Ważne jest poznanie zbiorowej tożsamości organizacji, na którą wpływ mają przede wszystkim ludzie ją tworzący, ich przekonania, postawy, wartości oraz postrzeganie siebie w organizacji[247]. Koncentracja na aspektach społecznych wymaga wykorzystywania w badaniach metod i technik jakościowych, takich jak obserwacja, analiza dokumentów czy wywiad. Uważa się, że zmiany kultury można dokonać przede wszystkim w sferach postrzegania, rozumienia i odczytania samej organizacji oraz jej członków, poprzez nadawanie zmianom sensów i znaczeń oraz rozpowszechnianie ich w komunikacji społecznej. Przykładami metod zarządzania kulturą organizacyjną w podejściu interpretatywnym są sensemaking i management of meaning[248].

Przedstawiciele nurtu krytycznego (radykalnego strukturalizmu), badając organizacje, wskazują na opresyjność kultury organizacyjnej, która podporządkowana jest zwiększaniu efektywności i wydajności, zauważają mechanizmy menedżerskiej propagandy, manipulacji oraz ideologii służącej utrzymaniu dominacji[249]. Porównują te działania do uwięzienia lub kolonizacji umysłów osób w organizacji. Krytykują również ujęcia i typologie powstałe w podejściu funkcjonalistyczno-systemowym za zbytnie uproszczenia, które nie opisują złożoności zjawisk w organizacji. Preferują metody badań jakościowych, w szczególności badanie w działaniu (ang. *action research*). Oprócz zdemaskowania instrumentalnych i manipulatorskich praktyk organizacyjnych badacz, zdaniem przedstawicieli radykalnego strukturalizmu, powinien szukać sposobów uwolnienia się spod dominacji grup uprzywilejowanych. Przedstawiciele tego nurtu są zwolennikami wdrażania emancypacyjnych zmian.

---

[245] A. Sitko-Lutek, *Aspekty złożoności kultury organizacyjnej*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2018, s. 77; M.J. Hatch, *Teoria organizacji*, Wydawnictwo Naukowe PWN, Warszawa 2002, s. 230.

[246] L. Smircich, *Concepts of Culture and Organizational Analysis*, Administrative Science Quarterly, Vol. 28(3), 1983, s. 339–358, s. 347; D. Chmielewska-Muciek, *Dyskusja nad pojęciem kultury organizacyjnej*, „Annales Universitatis Mariae Curie-Skłodowska. Sectio H, Oeconomia" 2009, 43, s. 317–331.

[247] M. Armstrong, *Zarządzanie zasobami ludzkimi*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 1996, s. 86.

[248] Ł. Sułkowski, *Interpretatywne koncepcje zarządzania – sensemaking, enactment oraz management of meaning*, Przegląd Organizacji, Nr 12 (875), 2012, s. 4–6.

[249] M. Alvesson, S. Deetz, *Doing Critical Management Research*, Sage Publications, London–Thousand Oaks–New Dehli 2000; H. Willmott, *Strength is ignorance; slavery is freedom: Managing culture in modern organizations*, „Journal of Management Studies" 1993, Nr 30/4, s. 515–552.

Podobnie jak paradygmat interpretatywny, postmodernizm (radykalny humanizm) oparty jest na przekonaniu o względności interpretacji i subiektywizmie oceny. Organizacja jest tworzona przez ludzi, ale dzieje się to ich kosztem, ponieważ są „uwięzieni" w nierealnej, ale uznawanej za konieczną, rzeczywistości. „Dlatego badacz, zdaniem radykalnych humanistów, powinien dążyć do demaskowania fałszywych pułapek zbiorowej świadomości, do których tworzenia przyczyniają się sami »uwięzieni«"[250]. Przedstawiciele nurtu uważają, że postmodernizm jest jedyną odpowiedzią na ponowoczesny świat organizacji, który jest: chaotyczny, zmienny, pełen siatek powiązań. Radykalni humaniści, zajmując się kulturą organizacyjną, nie określają metod badawczych, posługują się metaforami (np. happening, kłącze) i glossami[251]. Nie proponują metod zmian kultury organizacyjnej, demaskują tylko nieprawidłowości, a osoba, dowiadując się o tym, może sama zmienić swoje postępowanie.

2.4. Próby zdefiniowania kultury organizacyjnej

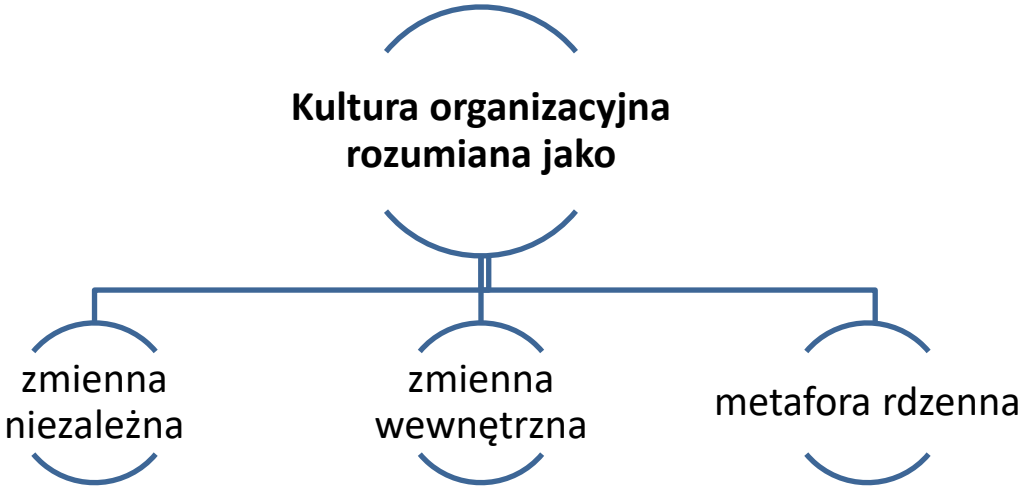
Pierwsze definicje kultury były tworzone przez antropologów. Wśród badaczy zauważane są obecnie problemy związane ze zdefiniowaniem tego pojęcia[252]. Osąd Adama Kupera: „Istnieją fundamentalne problemy epistemologiczne i nie rozwiąże się ich, chodząc na paluszkach wokół pojęcia kultury lub udoskonalając definicje"[253], jest zgodny z obecnym trendem w antropologii, która odchodzi od prób zdefiniowania kultury na rzecz scharakteryzowania rozmaitych jej rozumień. Według Pawła Krzyworzeki badacze teorii organizacji i zarządzania wydają się nie dostrzegać tego trendu i w swoich pracach nadal próbują dokonywać przeglądu definicji, pokazując różnice, lub wskazywać listy elementów wspólnych[254]. Barbara Czarniawska[255] uważa, że wpływ antropologii na teorię organizacji został ograniczony przez wpływy teorii systemów na teorię organizacji, czym tłumaczy rozbieżności w podejściu do definiowania kultury pomiędzy antropologami a badaczami teorii organizacji.

[250] M. Kostera, *Postmodernizm*…, op. cit., s. 34.
[251] Ł. Sułkowski, *Zmiana*…, op. cit., s. 15.
[252] S. Wright, *The politization of „culture"*, Anthropology Today, Vol. 14(1), 1998, s. 7–15.
[253] A. Kuper, I. Kołbon, *Kultura : Model Antropologiczny*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2005, s. VIII.
[254] P. Krzyworzeka, *Kultura organizacyjna – ślepa uliczka teorii organizacji*, „Master of Business Administration" 2012, 01, s. 72–81.
[255] B. Czarniawska, *Antropologia i teoria organizacji: wczoraj i dziś*, „Problemy Zarządzania: Antropologia Organizacji" 2011, 9/2 (32), s. 11–29.

Różnicami w definiowaniu zajmowała się Linda Smircich[256], która zauważyła, że w pracach z zakresu teorii organizacji kultura rozumiana jest jako (Rysunek 2.5):

- **Zmienna niezależna –** utożsamiana z kulturą kraju, w którym organizacja funkcjonuje. W tym nurcie uważa się, że kultura powstaje poza organizacją, że do organizacji jest tylko wnoszona. Badania w tym nurcie prowadzone są w temacie wpływu cech narodowych na jej funkcjonowanie, np. badania międzykulturowe Geerta Hofstede'a firmy IBM.
- **Zmienna wewnętrzna –** którą można zarządzać, zmieniać. Dostrzega się, że organizacja działa w szerszym kontekście kulturowym, ale skupia się na procesach społeczno-kulturowych wewnątrz organizacji. W tym rozumieniu kultury jest ona jedną z cech, jednym z elementów organizacji, tak więc można badać wzajemne relacje między instrumentami zarządzania. Przykładem takiego podejścia jest model E. Scheina.
- **Metafora rdzenna –** kultura jest pojmowana jako wspólne nadawanie sensu rozmaitym zjawiskom i sytuacjom. Kulturą są rezultaty ludzkich działań, natomiast idee wartości wynikają z życia społecznego. Rezygnuje się z wizji, że kultura jest czymś, co organizacja posiada, na rzecz założenia, że organizacja jest kulturą. Jeżeli organizacja jest kulturą, to można jej przypisać cechy charakterystyczne do nowego rozumienia kultury, zgodnego z podejściem antropologów. To znaczy, że kultura jest aktywnym procesem tworzenia znaczeń, a idee nigdy nie tworzą zamkniętych ani spójnych całości. Przedstawicielem tego podejścia jest np. Gareth Morgan.

[256] L. Smircich, *Concepts*…, op. cit., s. 339–358.



Rysunek 2.5. Nurty rozumienia kultury organizacyjnej
Źródło: opracowanie własne na podstawie P. Krzyworzeka, Kultura i organizacje,[w:] Perspektywa antropologiczna. Nowe kierunki w organizacji i zarządzaniu, (red.) B. Glinka, M. Kostera, Wolters Kluwer 2016 (według analizy L. Smircich, Concepts of Culture and Organizational Analysis. Administrative Science Quarterly, nr 28/3, 1983, s. 339–358).

Pomimo zauważonej w literaturze krytyki definiowania kultury organizacyjnej przedstawione zostały poniżej definicje (Tabela 2.3), które są przytaczane w wielu pracach dotyczących teorii organizacji[257].

Tabela 2.3. Wybrane definicje kultury organizacyjnej

Autorzy	**Definicje**
E. Jacques	Zwyczajowy lub tradycyjny sposób myślenia i działania, który jest w pewnym stopniu podzielany przez członków organizacji i który nowi pracownicy muszą przynajmniej częściowo zaakceptować[258].
G. Hofstede	„Zaprogramowanie umysłów" członków organizacji, a więc zespół skutecznie wpajanych przez grupę wartości, norm i reguł organizacyjnych[259].
R. Likert, J. Likert	Dominujący wzorzec: wartości, mitów, wierzeń, założeń, norm, ich uosobienia w: języku, symbolach, artefaktach, jak również technologii, celach i praktykach zarządzania, uczuciach, postawach, działaniach oraz interakcjach[260].

[257] M. Śliwa, M. Kostera, *Zarządzanie w XXI wieku. Jakość, twórczość, kultura*, Wolters Kluwer, Warszawa 2012; A. Kołodziej-Durnaś, op. cit.
[258] E. Jacques, *The Changing Culture of a Factory*, Dryden Press, New York 1952, s. 251.
[259] G. Hofstede, G.J. Hofstede, *Kultury i organizacje. Zaprogramowanie umysłu*, Wydanie II zmienione, PWE, Warszawa 2007, s. 16–17.
[260] R. Likert, J. Likert, *New Ways of Managing Conflict*, McGraw–Hill, New York 1976.

Autorzy	Definicje
E.H. Schein	Wzór podzielanych, fundamentalnych założeń, które dana grupa stworzyła, rozwiązując problemy adaptacji do otoczenia i integracji wewnętrznej. Wzór można uznać za obowiązujący. Jest on wpajany nowym członkom organizacji jako prawidłowy sposób rozwiązywania problemów[261].
R. Deshapande, R. Parasurman	Kultura organizacyjna polega na niepisanych, przestrzeganych często podświadomie zasadach, które wypełniają lukę między tym, co formalnie obowiązujące, a tym, co się faktycznie dzieje[262].
L. Smircich	Sieci znaczeń utkane przez ludzi w procesie organizowania[263].
G. Morgan	Kultura organizacyjna zazwyczaj odnosi się do wzorca rozwoju odzwierciedlonego przez: społeczne systemy wiedzy, ideologię, wartości, prawa i codzienne rytuały[264].

Źródło: opracowanie własne.

Widoczne w zestawieniu różnice w definiowaniu kultury organizacyjnej potwierdzają pogląd Mary Jo Hatch[265], że jest to prawdopodobnie najtrudniejsze pojęcie do zdefiniowania w teorii organizacji. Poznanie różnych definicji rozmaitych autorów reprezentujących odmienne paradygmaty pozwala zauważyć najważniejsze składniki i procesy związane z kulturą organizacyjną. Żadna z wymienionych definicji nie uwzględnia ich wszystkich jednocześnie. Ł. Sułkowski, poszukując rdzenia występujących w literaturze definicji, zauważył wspólne: „elementy konstytuujące kulturę organizacyjną[266]:

1. Jest ona fenomenem społecznym i grupowym.
2. Stanowi produkt grupy społecznej, którą jest organizacja.
3. Stanowi medium przekazywania znaczeń i wartości pomiędzy ludźmi.
4. Tworzy się częściowo spontanicznie, a częściowo podlega kontroli zarządzających".

[261] E.H. Schein, *Organizational Culture and Leadership*, Jossey-Bass Publisher, San Francisco–Washington–London 1985, s. 6.

[262] R. Deshapande, R. Parasurman, *Linking corporate to strategic planning*, „Organizacja i Kierowanie" 1987, nr 6.

[263] L. Smircich, *Studing Organisations as Cultures*, [w:] G. Morgan, *Beyond Method: Strategies for Social Research*, Beverly Hills London ñ New Delhi 1983; C. Geertz, *The Interpretation of Culture*, Basic Book, London 1973, s. 25.

[264] G. Morgan, *Images of Organization*, Thousand Oaks 1997.

[265] M.J. Hatch, op. cit.

[266] Ł. Sułkowski, *Wieloznaczność kultury organizacyjnej*, „Przedsiębiorczość i Zarządzanie" 2012, Wydawnictwo SAN, TOM XIII, Zeszyt 12, s. 11–25, s. 15.

2.5. Funkcje, modele, typologie kultury

Kultura spełnia funkcje integracyjne, percepcyjne i adaptacyjne[267]. Funkcja integracyjna przejawia się akceptacją przez członków organizacji wspólnych celów, wartości, norm i poglądów. Funkcja percepcyjna polega na występowaniu podobnego postrzegania rzeczywistości przez pryzmat charakterystycznych dla organizacji filtrów poznawczych i stereotypów. Funkcja adaptacyjna ma na celu stabilizowanie rzeczywistości przez wypracowanie schematów działania w określonych sytuacjach. Dodatkowo kultura może pełnić funkcję nadawania tożsamości organizacji[268]. Związane jest to z tworzeniem wspólnego, spójnego wizerunku organizacji, zrozumiałego tak dla pracowników, jak i otoczenia. Budowanie tożsamości[269] jest dla organizacji tym, czym dla człowieka kształtowanie osobowości.

Kultura odgrywa również istotną rolę w zmniejszaniu niepewności poprzez ułatwienie porozumiewania się ludzi. W okresie industrialnym trzema filarami redukującymi niepewność była relacja przełożony – podwładny, formalizacja i kolektywizm. W okresie informacyjnym[270] członek organizacji pozbawiony jest oparcia w postaci silnego przywódcy, jednolitych standardów realizacji zadań i wyraźnie określonej stałej grupy społecznej, z którą się identyfikuje. Coraz częściej skazany jest na samodzielne radzenie sobie z niepewnością w pracy. Współczesna kultura organizacyjna nie redukuje niepewności, może jedynie pomagać w radzeniu sobie z nią[271].

Literatura przedmiotu prezentuje wiele modeli[272], które przyczyniły się do powstania różnych typologii dotyczących kultury organizacyjnej. Jeden z nich, do którego odwołuje się wielu badaczy i który jest obecnie uważany za najbardziej rozpowszechnioną koncepcją kultury organizacyjnej[273], to model E. Scheina (Rysunek

[267] C. Sikorski, *Nauka o zarządzaniu*, Wydawnictwo AHE, Łódź 2009, s. 177; B. Mazur, *Kultura organizacyjna w zróżnicowanym wyznaniowo otoczeniu,* Oficyna Wydawnicza Politechniki Białostockiej, Białystok 2012; Ł. Sułkowski, *Kulturowa zmienność organizacji*, PWE, Warszawa 2002, s. 60.

[268] Ł. Sułkowski, *Kulturowa zmienność organizacji*…, op. cit., s. 62.

[269] Ibidem.

[270] Okres informacyjny – nazwa okresu przyjęta na wstępie pracy: J. Bieńkowska, C. Sikorski, *Ewolucja*…, op. cit., określająca okres epoki cywilizacji informacyjnej II połowa lat 90. XX w.

[271] C. Sikorski, *From Reducing Uncertainty to Dealing with Uncertainty. Change of Function of Organizational Culture*, Edukacja Ekonomistów i Menedżerów, Tom 46, Nr 4, 2017, s. 9–21.

[272] Między innymi modele: E. Scheina, C. Sikorskiego, G. Hofstede.

[273] J. Czekaj, B. Ziębicki, *Pozytywna nauka o organizacji na tle ewolucji teorii i koncepcji zarządzani*a, „Organizacja i Kierowanie" 2013, nr 3(156), s. 45–56; Ł. Sułkowski, *Functionalistic models of organizational culture*, „Przedsiębiorczość i Zarządzanie" 2014, Wydawnictwo SAN, tom XV, zeszyt 10, część II, s. 155–163; D. Plecka, L. Młodzik, *Kulturowe uwarunkowania zarządzania wiedzą w organizacjach publicznych*, „Studia Iuridica" 2022, vol. 92, s. 290.

2.6). Jest on złożony z trzech elementów nazwanych poziomami kultury. To, co najbardziej widoczne w organizacji, to artefakty. Poniżej nich znajdują się wartości i normy zachowań. Najniższy poziom to główne, podstawowe założenia filozoficzne i światopoglądowe, które wpływają na funkcjonowanie danej społeczności.

Rysunek 2.6. Poziomy kultury według E. Scheina
Źródło: E.H. Schein, Organizational culture and leadership, Edycja 3. Jossey-Bass, 2004, s. 26.

Artefakty obejmują widoczne wytwory organizacji, takie jak: architektura, język, symbole, technika i produkty, sposób ubierania się, sposób zwracania się do siebie, mity i historie opowiadane o organizacji; występujące rytuały i ceremonie. Normy i wartości dzieli się na deklarowane przez członków organizacji oraz na przestrzegane, które można poznać dzięki nieformalnym rozmowom i zachowaniom. Podstawę kultury organizacyjnej stanowią założenia, które są wzorcami odbioru rzeczywistości, koncepcjami filozoficznymi i światopoglądowymi. Jeśli nieznany jest wzór podstawowych założeń w organizacji, nie będzie można prawidłowo interpretować artefaktów oraz artykułowanych wartości.

Czesław Sikorski, który w swojej pracy podzielał funkcjonalistyczną koncepcję kultury[274], uznał, że kultura organizacyjna to system nieformalnie utrwalonych w środowisku społecznym organizacji wzorów myślenia i działania, mających znaczenie dla realizacji celów formalnych. Według niego system ten składa się z takich elementów, jak wzory myślenia, wzory zachowań oraz symbole.

1. Wzory myślenia:
   a) Założenia kulturowe (wierzenia)

      Przekonanie ludzi na temat istoty: czasu i przestrzeni, rzeczywistości oraz prawdy, natury ludzkiej, ludzkiej działalności i stosunków międzyludzkich. Na te przekonania wpływ mają doświadczenia z dzieciństwa, wrodzone skłonności, rodzice i inne autorytety.

[274] C. Sikorski, *Nauka*…, op. cit. s. 157.

b) Zbiór wartości

   W kulturze organizacyjnej wartości: są zbiorowymi preferencjami, definiują sukces, formują poczucie tożsamości, związanie z organizacją, koleżeńskość.

c) Normy

   Niepisane reguły (moralne, obyczajowe, prakseologiczne), na których oparte jest życie społeczne w organizacji – do czego dążyć, czego unikać i w jaki sposób należy to czynić.

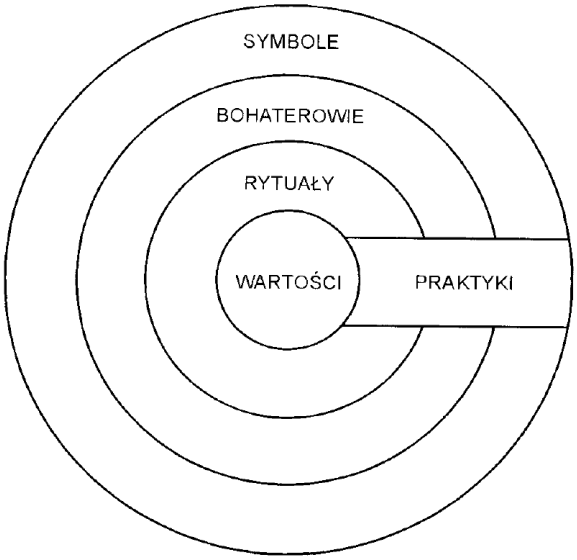
2. Wzory zachowań kształtują się na skutek upowszechnienia postaw[275], będących wynikiem określonych wzorów myślenia. Postawy są następstwem zastosowania norm i wartości kulturowych do przedmiotów oraz sytuacji występujących w danej organizacji.
3. Symbole są instrumentami kulturowej socjalizacji. Dzięki symbolom kultura organizacyjna upowszechnia się i utrwala w danym środowisku. Symbole mogą być: fizyczne (elementy ubioru, insygnia), językowe (mowa korporacyjna, język ciała, gesty przekazujące informację, mity), behawioralne (rytuały, ceremonie, okresowe narady – sposób rozmieszczenia osób, kolejność i forma wypowiedzi).

Geert Hofstede jest autorem modelu kultury organizacyjnej (Rysunek 2.7), w którym przedstawia w uporządkowany sposób jej przejawy w organizacji[276]. Model nazwany przez autora „diagramem cebuli" w swojej najgłębszej warstwie zawiera wartości – oddają one to, co jest ważne dla danej organizacji. Definiowane są jako skłonności do dokonywania określonego wyboru. Rytuały oraz bohaterowie tworzą warstwy środkowe. Rytuały stanowią powtarzające się czynności, wyrażające podstawowe wartości organizacji. Można je obserwować w gestach, sposobach powitań, protokołach oficjalnych spotkań czy obchodach uroczystości. Bohaterowie to postacie współczesne lub historyczne, które utożsamiają najbardziej cenione cechy w danej kulturze, stają się wzorami do naśladowania. Zewnętrzną, najbardziej widoczną warstwą są symbole. Są nimi: język, gesty, przedmioty, znaki graficzne, rozpoznawalne przez członków danej kultury. Symbole, bohaterowie i rytuały składają się na praktyki,

[275] „Postawa jest zawsze czyjaś i zawsze skierowana na jakiś obiekt, albo grupę lub rodzaj obiektów. Postawa człowieka wobec jakiegoś obiektu (osoby, przedmiotu, zdarzenia, idei) to względnie trwała tendencja do pozytywnego lub negatywnego wartościowania tego obiektu przez tego człowieka", źródło: B. Wojciszke, *Człowiek wśród ludzi: zarys psychologii społecznej*, Wydawnictwo Naukowe Scholar, Warszawa 2004, s. 180.

[276] G. Hofstede, *Kultury i organizacje. Zaprogramowanie umysłu*, PWE, Warszawa 2000, s. 43.

które są widoczne na zewnątrz, ale w pełni czytelne jedynie dla członków danej kultury – w praktykach, a nie wartościach G. Hofstede dostrzegł trzon kultury organizacyjnej – jego zdaniem wartości członków organizacji zależą przede wszystkim od czynników zewnętrznych, takich jak narodowość czy wieku, a nie od przynależności do organizacji.



Rysunek 2.7. „Diagram cebuli" przejawy kultury na różnych poziomach głębokości
Źródło: G. Hofstede, Kultury i organizacje. Zaprogramowanie umysłu, PWE, Warszawa 2000, s. 43.

W związku z tym, że obserwuje się różnorodność kultur, brak jednorodności nawet w jednej organizacji, aby ułatwić ich scharakteryzowanie lub porównanie, opracowane zostały różnorodne podejścia do klasyfikacji kultury. Klasyfikacje te okazują się bardzo cennymi narzędziami w zrozumieniu problemów związanych z kulturą organizacyjną. Twórcy typologii kultur organizacyjnych bazowali na różnych kryteriach tworząc m.in. typologie dychotomiczne, czterodzielne.

Według Czesława Sikorskiego[277] najbardziej popularnymi systemami wymiarów kultury są odniesienia: Florence Kluckhohna i Freda L. Strodtbecka[278], Geerta Hofstede[279] oraz Charlese Hampden-Turnera i Alfonsa Trompenaarsa[280]. Zgodnie z koncepcją zaproponowaną przez F. Kluckhohna i F.L. Strodtbecka kultury wykazują różnice w swoim podejściu do niżej wymienionych aspektów:

[277] C. Sikorski, *Kształtowanie kultury organizacyjnej. Filozofia, strategie, metody*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2009, s. 14.
[278] F. Kluckhohn, F.L. Strodtbeck, *Variations in Value Orientations*, Peterson, Evanston 1961.
[279] G. Hofstede, *Culture's Consequences. International Differences in Work-Related Values*, Sage, Beverly Hills–London–New Delhi 1984.
[280] Ch. Hampden-Turner, A. Trompenaars, *Siedem kultur kapitalizmu*, Dom Wydawniczy ABC, Warszawa 1998.

1. **Natura –** z jednej strony istnieje skłonność do podporządkowania się naturze i do dostosowywania się do jej praw, podczas gdy z drugiej strony istnieje dążenie do dominacji nad naturą i do podporządkowania jej ludzkim potrzebom.
2. **Orientacja czasowa –** można koncentrować się na przeszłości, wspominając dawne czasy i trzymając się tradycji, albo skupić się na przyszłości, tworzeniu długoterminowych planów.
3. **Natura ludzka –** osoby mogą być postrzegane jako z natury dobre lub z natury złe.
4. **Działania –** z jednej strony istnieje przekonanie, że zwiększona aktywność i zachowanie zorientowane na osiągnięcie celu prowadzą do osiągnięcia sukcesu, z drugiej strony istnieje niechęć do nadmiernego wysiłku, dążenie do zapewnienia sobie spokoju i sprawiania sobie przyjemności.
5. **Lokalizacja odpowiedzialności –** z jednego punktu widzenia osobie przypisuje się całkowitą odpowiedzialność za to, co się jej przytrafiło, podczas gdy z drugiego punktu widzenia odpowiedzialność ta spoczywa na grupie społecznej, do której dana osoba należy.
6. **Przestrzeń społeczna –** z jednej strony propagowana jest publiczna otwartość w zachowaniu ludzi, z drugiej strony zwraca się uwagę na istotność ochrony prywatności naszych zachowań.

G. Hofstede, opierając się na badaniach porównawczych kultur organizacyjnych w koncernie IBM, przeprowadzonych w 50 krajach w latach 1968–1972, zaproponował cztery wymiary kulturowe. Pierwszym z nich jest **dystans władzy.** Wymiar ten rozróżnia kultury na podstawie tego, czy osoby są skłonne przywiązywać większą lub mniejszą wagę do swojej pozycji w hierarchii władzy. Mały dystans władzy oznacza, że ludzie uważają, że wszyscy powinni mieć równe prawa, a władza powinna być sprawowana etycznie i stale kontrolowana. W kulturze dużego dystansu władzy hierarchia jest zupełnie naturalna, a władza jest źródłem prestiżu, wyznaczającym miejsce osób w strukturze społecznej. Drugi wymiar **indywidualizm – kolektywizm** podkreśla różnice między kulturami pod względem roli przypisanej jednostce w organizacji, co za tym idzie – również pod względem dominacji orientacji na cele jednostki czy grupowe. Trzecim wymiarem jest **męskość – kobiecość.** Ten wymiar odzwierciedla wsparcie albo dla kultury męskiej, charakteryzującej się opartym na rywalizacji podejściem do życia społecznego, albo dla kultury kobiecej, cechującej się

większą troską i zrozumieniem w relacjach społecznych. Stopień **unikania niepewności** jest czwartym wymiarem, gdzie organizacje o kulturze wysokiej tolerancji niepewności są pozytywnie nastawione do podejmowania ryzyka i są otwarte na zmiany, podczas gdy organizacje o niskiej tolerancji preferują poczucie pewności oraz bezpieczeństwa. W latach późniejszych zbiór był rozszerzony do sześciu wymiarów. Wyodrębnienie piątego wymiary było związane z badaniami na Dalekim Wschodzie, prowadzonymi m.in. przez Michaela Bonda. Dotyczył orientacji czasowej i przeciwstawiał zorientowanie na przyszłość zorientowaniu na teraźniejszość i przeszłość[281]. **Orientacja długoterminowa** wiąże się z: zapobiegliwością, oszczędnym gospodarowaniem zasobami, wytrwałością i cierpliwością. Inwestuje się w trwałe i wieloletnie sieci powiązań – a o tym, co jest dobre, a co złe, decydują okoliczności. Orientacja długoterminowa charakteryzuje się hołdowaniu uczciwości, zdolności adaptacji i samodyscyplinie. Natomiast **orientacja krótkoterminowa** wiąże się z presją na szybkie zyski, dążeniem do natychmiastowych nagród za osiągnięcia. Wzajemna lojalność uzależniona jest od tymczasowo występujących korzyści. Hołduje się takim wartościom, jak wolność, prawa jednostki, uniwersalnym zasadom określającym dobro i zło. Do drugiego rozszerzenia modelu wymiarów Hofstede'a przyczynili się badacze Ronald Inglehart oraz Michael Minkova. Szóstym wymiarem jest **przyzwolenie – restrykcyjność.** Kultura przyzwolenia charakteryzuje się zgodą na zaspokojenie pragnień danej osoby, przywiązywanie wagi do wolności słowa. Wiąże się z wyższym poziomem optymizmu i lepszym zdrowiem. Restrykcyjność charakteryzuje się przywiązaniem dużej wagi do zachowania porządku w społecznościach, przekonaniem, że przyjemności powinny być ściśle regulowane.

Charles Hampden-Turner i Fons Trompenaars w swojej pracy[282], której celem było obalenie mitu istnienia najlepszego sposobu zarządzania i organizacji, przedstawili siedem wymiarów kultury, które dały możliwość lepszego zrozumienia danej kultury oraz różnic kulturowych pomiędzy organizacjami. Pierwszy z nich to **uniwersalizm – partykularyzm.** W podejściu uniwersalistycznym przywiązuje się wagę do uniwersalnych, znormalizowanych zasad, zaś w partykularystycznym akceptuje się zindywidualizowane podejście i wyjątki wynikające z relacji międzyludzkich i szczególnych okoliczności. Wymiar **indywidualizm – kolektywizm**, podobnie jak

[281] G. Hofstede, G.J. Hofstede, M. Minkov, *Kultury i organizacje. Zaprogramowanie umysłu*, Wydanie III zmienione, PWE, Warszawa 2011, s. 16–17.

[282] Ch. Hampden-Turner, F. Trompenaars, *Siedem wymiarów kultury*, Oficyna Ekonomiczna, Kraków 2002, s. 22–24.

w perspektywie G. Hofstede'a, bada, czy ważniejsze jest koncentrowanie się na pojedynczych osobach, na ich rozwoju dla dobra organizacji, czy też istotniejszy jest interes kolektywu, wspólny dla wielu jej członków. Trzeci wymiar, **powściągliwość – emocjonalność,** pozwala określić, czy w danej kulturze preferuje się kontrolowanie emocji i zachowanie obiektywizmu, bezstronności, czy też dopuszczalne jest ich okazywanie. Wymiar **wycinkowość – całościowość** bada, w jakim stopniu osoby angażują się w wykonywanie działań, czy stawiają granice pomiędzy sferą życia prywatną a publiczną. W kulturach wycinkowych działania są od siebie odseparowane, związane są z miejscem, celem aktywności. W kulturach całościowych barier jest mniej, a życie prywatne członków organizacji przenika się z działalnością publiczną. Piąty wymiar, **osiągnięcie statusu – otrzymanie statusu,** pokazuje, czy wyżej cenione są osiągnięcia osobiste, doświadczenie, czy też status społeczny, pochodzenie, wiek. Podobnie jak u G. Hofstede'a, badacze zauważyli, że wpływ na zarządzanie ma **stosunek do czasu.** Są organizacje, których członkowie skupiają się na chwili obecnej i na przyszłości, traktują czas liniowo jako ciąg następujących po sobie zdarzeń. Są również takie, w których, jak w ruchu po okręgu, przeszłość i teraźniejszość współistnieją z przyszłymi możliwościami. Ostatnim wymiarem jest **stosunek do otoczenia,** rozumianego jako odniesienie do przyrody, jak i do drugiego człowieka. Badacze powiązali ten aspekt z opozycją: wewnątrzsterowność – zewnątrzsterowność, która bada, czy osoby polegają na swoich wewnętrznych osądach i obowiązkach, czy też nadają priorytet zewnętrznym sygnałom i wymaganiom.

Zaprezentowane powyżej zestawienie koncepcji metod różnicowania kultur organizacyjnych dostarcza informacje na temat wymiarów kulturowych, które wpływają na ludzkie zachowanie i procesy organizacyjne. W literaturze przedmiotu można znaleźć opisy różnych wielowymiarowych klasyfikacji kultur[283]. W kolejnym rozdziale zostanie omówiona szczegółowo dwuwymiarowa typologia K. Camerona i R. Quinna[284] – w związku z wykorzystaniem w pracy narzędzia badawczego opartego na jej założeniach.

[283] Ch. Hampden-Turner, F. Trompenaars, *Siedem wymiarów kultury*, Oficyna Ekonomiczna, Kraków 2002, s. 190; T.E. Deal, A.A. Kennedy, *Corporate cultures: the rites and rituals of corporate life*, Penguin, Harmondsworth 1982, s. 107–127; C.B. Handy, *Understanding organizations*, Penguin, London 1999; R. Harrison, *Understanding your organization's character*, „Harvard Business Review, 1972, s. 119–128; T.J. Peters, *Business Policy in Action*, „Management decision" 1993, Vol. 31 No. 6.; G. Hofstede, *Kultury i organizacje. Zaprogramowanie umysłu*, PWE, Warszawa 2000, s. 217; Cz. Sikorski, *Kultura organizacyjna*, Wydawnictwo C.H. Beck, Warszawa 2002, s. 30.

[284] K.S. Cameron, R.E. Quinn, *Kultura*…, op. cit., s. 40–49.

Przedstawione powyżej modele i typologie kultury organizacyjnej są charakterystyczne dla paradygmatu funkcjonalistyczno-systemowego. Krytycy tego podejścia w badaniu kultury organizacyjnej zwracają uwagę, że jest ono oparte na teorii poznania nauk przyrodniczych, wywodzącej się z paradygmatu mechanicyzmu, który w fizyce został zastąpiony przez paradygmat teorii względności czy mechaniki kwantowej[285]. Koncepcja funkcjonalistyczno-systemowa jest bliska takim subdyscyplinom nauk o zarządzaniu, jak rachunkowość zarządcza, zarządzanie logistyką czy zarządzanie informacją. Holistyczna wizja ładu organizacyjnego, charakterystyczna dla tego podejścia, może przesłonić elementy tworzenia znaczenia, występujące na poziomie zachowań i interakcji. Interpretacje procesów: ustanawiania i sprawowania władzy, komunikacji jednostek i grup, kształtowania elementów kultury czy nadawania sensu rzeczywistości organizacyjnej, mogą zostać utracone[286]. Odpowiedzią na krytykę może być podejście interpretatywne, które pozwala na prezentację złożoności i dynamiki kultury danej organizacji. O mechanizmach składających się na procesy tworzenia kultury organizacyjnej pisała przedstawicielka nurtu interpretatywnego – Mary Jo Hatch. W stworzonym przez nią modelu dynamiki kulturowej (Rysunek 2.8) na pierwszy plan wysuwają się procesy, łączące poszczególne elementy kultury: założenia, wartości, artefakty i symbole. Procesy te, według autorki, są dwukierunkowe[287]:

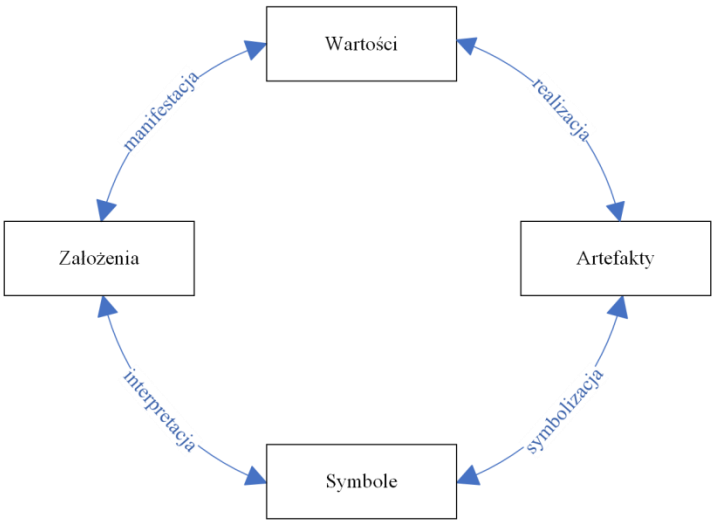
- „manifestacja założeń kultury w postaci wartości,
- realizacja wartości w postaci artefaktów,
- symbolizacja artefaktów, czyli nadanie niektórym artefaktom statusu symboli,
- interpretacja symboli wspierająca założenia".

Choć powyższe procesy związane z kulturą zachodzą w organizacji nieustannie, cyrkularny charakter modelu sprawia, że to, co dynamiczne, stwarza wrażenie statycznego systemu.

[285] M.J. Wheatley, *Leadership and the New Science. Discovering Order in a Chaotic World*, Berret-Koehler Publishers, San Francisco 1999, s. 10–11.

[286] Ł. Sułkowski, *Paradygmaty*…, op. cit., s. 17–26.

[287] M. Kostera, P. Krzyworzeka, M. Połeć, op. cit., s. 42.



Rysunek 2.8. Dynamika kultury organizacji
Źródło: M. Jo Hatch, The dynamics of organizational culture, Academy of Management Review, 1993, 18/4, s. 660.

Prace badawcze w naukach społecznych z reguły prowadzone są w jednym paradygmacie[288]. Pojawiają się jednak stanowiska proponujące badania łączące różne paradygmaty, wykorzystując najlepsze cechy każdego z nich[289]. Barbara Mazur[290], uważając za zasadne przyjęcie w aspekcie kultury organizacyjnej założeń pluralizmu epistemologicznego i metodologicznego, przedstawiła koncepcję połączenia dwóch podejść w badaniu kultury, nazywając ją paradygmatem funkcjonalistyczno-interpretatywnym. Ł. Sułkowski dopuszcza łączenie paradygmatów, zwracając uwagę na odpowiednie uzasadnienie wyboru oraz określenie relacji między nimi[291]. W literaturze przedmiotu pojawia się termin badań metodami mieszanymi (ang. *mixed methods research*)[292], w których łączy się metody charakterystyczne dla poszczególnych paradygmatów. Są one definiowane jako: „rodzaj badań, w których badacz lub zespół badaczy łączy elementy jakościowych i ilościowych metod badawczych (np. wykorzystanie jakościowych i ilościowych perspektyw, gromadzenia danych, analiz, technik wnioskowania) w celu uzyskania szerokiego i dogłębnego

[288] M. Kostera, B. Glinka, op. cit., s. 15.
[289] D. Miller, *Paradigm prison, or in praise of aheoretic research*, „Strategic Organizations" 2007, nr 5, s. 177–184.
[290] B. Mazur, *Kultura organizacyjna w perspektywie poznawczej. Próba operacjonalizacji*, [w:] *Metody zarządzania kulturą organizacyjną*, (red.) Ł. Sułkowski, C. Sikorski, Wydawnictwo Difin, Warszawa 2014, s. 58–74..
[291] Ł. Sułkowski, *Paradygmaty*…, op. cit., s. 24.
[292] Ł. Sułkowski, R. Lenart-Gansiniec, *Metody badań mieszanych w naukach o zarządzaniu*, (red.) Ł. Sułkowski, R. Lenart-Gansiniec, Wydawnictwo Naukowe Akademii WSB, Dąbrowa Górnicza 2023, s. 8.

zrozumienia i weryfikacji”[293]. Zwolennicy tego rodzaju badań twierdzą, że ich wykorzystanie w dyscyplinie nauki o zarządzaniu może odegrać ważną rolę w jej rozwoju, bowiem wyniki uzyskane z zastosowania różnych metod mogą wzbogacić co zapewniają lepsze zrozumienie problemów zarządczych[294].

2.6. Wybrane metody badań kultury organizacyjnej w paradygmatach funkcjonalistyczno-systemowym i interpretatywnym

W literaturze dotyczącej kultury organizacyjnej podejmowane są tematy związane z możliwością poznania kultury organizacyjnej, jak również opisywane są metody zmiany kultury[295]. Jak zauważają badacze[296], zmiana kultury organizacyjnej nie jest procesem łatwym, wymaga dużo czasu, a efekt jest trudny do przewidzenia. W badaniu przeprowadzonym przez brytyjskich badaczy[297] zidentyfikowano 70 narzędzi do badania kultury organizacyjnej, zbiór ten tworzą zarówno narzędzia metod ilościowych (np. kwestionariusz ankiety), jak i jakościowych (np. dziennik obserwacji, dyspozycje do wywiadu). Zauważono, że większość z nich znajduje się na wstępnym etapie rozwoju. Autorzy wnioskują, że nie ma idealnego narzędzia do badania kultury organizacyjnej, a decyzja o jego wyborze powinna być uzależniona od celu badania.

2.6.1. Metoda badań kultury organizacyjnej w paradygmacie funkcjonalistyczno-systemowym

W podejściu funkcjonalistyczno-systemowym do zidentyfikowania cech kultury występującej w organizacji, jak i kultury pożądanej przez osoby w niej pracujące, wykorzystywane są metody ilościowe. Jednym z narzędzi do pomiaru kultury organizacyjnej jest model wartości konkurujących (ang. *Competing Values*

[293] R.B. Johnson, A.J. Onwuegbuzie, L.A. Turner, *Toward a Definition of Mixed Methods Research*, „Journal of Mixed Methods Research” 2007, 1(2), s. 123.

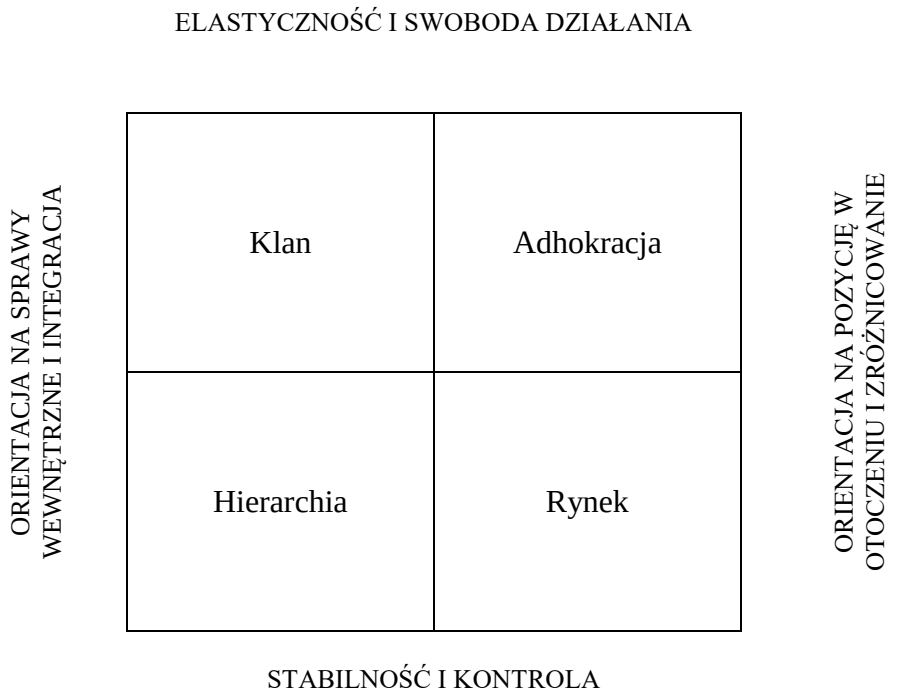
[294] J.F. Molina-Azorín, M.D. López-Gamero, *Mixed methods studies in environmental management research: Prevalence, purposes and designs*, „Business Strategy and the Environment” 2016, 25(2), s. 134–148; J.W. Creswell, A. Tashakkori, *Differing perspectives on mixed methods research*, „Journal of Mixed Methods Research” 2007, 1(4), s. 303–308; Ł. Sułkowski, R. Lenart-Gansiniec, *Metody*…, op. cit., s. 13.

[295] M. Czerska, *Proces kształtowania kultury organizacji*, „Prace Naukowe Akademii Ekonomicznej We Wrocławiu. Zmiana warunkiem sukcesu: Integracja, globalizacja, regionalizacja – wyzwania dla przedsiębiorstw” 2002, 32/33 (963), s. 77–93.

[296] Ł. Sułkowski, *Zmiana*…, op. cit., s. 18; A.K. Koźmiński, D. Jemielniak, D. Latusek-Jurczak, *Zasady zarządzania*, Wolters Kluwer SA, Warszawa 2014, s. 228.

[297] T. Jung, T. Scott, H. Davies, P.Bower, D. Whalley, R.Mcnally, R. Mannion, *Instruments for Exploring Organizational Culture: A Review of the Literature*, „Public Administration Review” 2009, 69, s. 1087–1096.

Framework)[298]. Model ten powstał w wyniku badań nad wskaźnikami efektywności organizacji. Zbiór zidentyfikowanych wskaźników został podzielony na cztery grupy: klan, adhokracja, hierarchia i rynek, według dwóch wymiarów. Jeden wymiar zestawia kryteria efektywności związane z „elastycznością i swobodą działania" ze „stabilnością i kontrolą". Drugi wymiar przeciwstawia „orientację na sprawy wewnętrzne i integrację „orientacji na pozycję w otoczeniu i zróżnicowanie" (Rysunek 2.9).



Rysunek 2.9. Model wartości konkurujących
Źródło: K.S. Cameron, R.E. Quinn, Kultura organizacyjna – diagnoza i zmiana. Model wartości konkurujących, Oficyna Ekonomiczna, Kraków 2003, s. 40.

Przedstawione cztery grupy (Rysunek 2.9) wskaźników efektywności (klan, adhokracja, rynek, hierarchia) określają, jakie wartości są najbardziej cenione w organizacji. Stanowią one wartości przeciwstawne, konkurujące ze sobą. W organizacjach typu klanowego ważna jest praca zespołowa, zaangażowanie pracowników, lojalność i tradycja. Dynamika działania, kreatywność, podejmowanie ryzyka i elastyczność są cechami organizacji typu adhokratycznego. Członkowie organizacji typu hierarchicznego przede wszystkim zwracają uwagę na wartości, takie jak: wydajność, rzetelność, przewidywalność i stabilizacja. Organizacje typu rynkowego są zorientowane na osiąganie celów i są nastawione na rywalizację.

[298] R. E. Quinn, K. S. Cameron, *Organizational life cycles and shifting criteria of effectiveness*, „Management Science" 1983, 29, s. 33–51.

Uniwersalność modelu wartości konkurujących skłoniła autorów do zastosowania go do badania kultury organizacyjnej[299]. Powstało narzędzie do pomiaru kultury organizacyjnej (ang. *Organizational Culture Assessment Instrument*, skrót: OCAI). Zakładając, że nie można się skupić jednocześnie na wszystkich aspektach funkcjonowania organizacji, autorzy OCAI określili wymiary kultury, które będą podlegały badaniu. Dzielą je na dwa rodzaje: wymiary treści kultury i wymiary wzorca. Wymiary treści opierają się na teorii archetypów[300], a wzorce to profile kultury (tj.:klan, adhokracja, rynek, hierarchia), które otrzymuje się jako podsumowanie wyników uzyskanych dzięki kwestionariuszowi do oceny kultury. Kwestionariusz OCAI bazuje na sześciu wymiarach treści:

1) ogólna charakterystyka organizacji;
2) styl przywództwa w organizacji (ogólne podejście do zarządzania);
3) styl zarządzania pracownikami;
4) cechy zapewniające spójność organizacji (mechanizmy jednoczące);
5) sprawy, na które kładzie się największy nacisk (czynniki kształtujące strategię organizacji);
6) kryteria sukcesu (co jest definiowane jako zwycięstwo).

Kultura klanowa łączy w sobie orientacje na sprawy wewnętrzne z dużą elastycznością i swobodą działania. Charakteryzuje się przyjaznym środowiskiem pracy, w którym pracownicy są otwarci na współpracę i wykazują osobiste zaangażowanie, co sprzyja wysokiej efektywności. Organizacja działa w taki sposób, aby jednostki mogły się rozwijać i korzystać z dużej niezależności. Przywództwo budowane jest na mentoringu, a decyzje w tego typu organizacji często oparte są na konsensusie. Jedność organizacji opiera się na lojalności i tradycji. Miarą sukcesu jest rozwój własnych zasobów ludzkich i spełnienie potrzeb interesariuszy.

W kulturze adhokracji, która łączy orientację na pozycję w otoczeniu i zróżnicowanie z dużym stopniem elastyczności i swobody działania, wysoko cenione są innowacje i przełomowe pomysły pracowników. Kierownictwo organizacji, w której

[299] K.S. Cameron, R.E. Quinn, *Kultura*…, op. cit; J. Strengers, L. Mutsaers, L. van Rossum, E. Graamans, *The organizational culture of scale-ups and performance*, Journal of Organizational Change Management, Vol. 35, No. 8, 2022, s. 115–130; M. Dębski, M. Cieciora, P. Pietrzak, W. Bołkunow, *Organizational Culture in Public and Non-public Higher Education Institutions in Poland: A Study Based on Cameron and Quinn's Model*, „Human Systems Management" 2020, 39, s. 345–355; J. Kacała, A. Michaluk, *Rozwój kadr a kultura organizacyjna w dobie profesjonalizacji sił zbrojnych RP*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Nauki o Zarządzaniu, 4. Zarządzanie w teorii" 2010, nr 137, s. 265–273.

[300] I. I. Mitroff, *Stakeholders of organizational mind*, Jossey-Bass, San Francisco 1983.

ten typ kultury dominuje, nie wykazuje cech autorytarnej władzy, koncentruje się na wspieraniu przedsiębiorczości i kreatywności, nawet jeśli takie podejście wiąże się ze znacznym ryzykiem. Praca często jest wykonywana przez zespoły, które są rozwiązywane po wykonaniu zadania. Takie podejście sprawia, że organizacja jest w stanie szybko dostosować się do nowych okoliczności. Sukcesem jest możliwość zaoferowania przez organizację innowacyjnych rozwiązań.

Kultura rynkowa łączy silną orientację na wzrost pozycji w otoczeniu zewnętrznym z potrzebą stabilności i kontroli. Charakteryzuje się naciskiem na efektywność i konkurencyjność. Zarządzanie w tego typu organizacji opiera się na jasno zdefiniowanych i monitorowanych zadaniach. Kierownictwo jest bezwzględne i wymagające. Spójność organizacji zapewniają ekspansywność i wola zwycięstwa. Miarą sukcesu jest wzrost pozycji w otoczeniu.

Kultura hierarchii łączy orientację na sprawy wewnętrzne i integrację ze stabilnością i kontrolą. Organizację z przewagą tego typu kultury można opisać jako miejsce pracy z jasno zdefiniowanymi procedurami i strukturami, gdzie sposób realizacji zadań charakteryzuje się zespołową odpowiedzialnością. Zadaniem kierownictwa jest przede wszystkim koordynowanie, organizowanie i kontrolowanie działań. Najważniejsze jest sprawne, stabilne funkcjonowanie organizacji. Miarą sukcesu jest osiągnięcie celów działania przy jak najniższych kosztach.

Wynikiem badań przeprowadzonych za pomocą narzędzia OCAI jest profil obecny i profil pożądany kultury organizacyjnej, w których – zgodnie z ramami wartości konkurencyjnych – obecne są mieszanki wszystkich czterech typów kultury. Zastosowany kwestionariusz pozwala zidentyfikować dominujący, obecny typ kultury i jego siłę, a ponadto dostrzec rozbieżność między kulturą obecną a pożądaną oraz określić stopień zbieżności kulturowej danej organizacji z innymi badaniami[301].

Rzetelność metody/narzędzia została udowodniona przez wielu badaczy[302]. G. Wudarzewski[303] przeprowadził w swojej pracy badanie walidacyjne, które

[301] K.S. Cameron, R.E. Quinn, *Kultura*…, op. cit., s. 70.

[302] R. Quinn, G. Spreitzer, *The Psychometric of the Competing Values Culture Instrument and an Analysis of the Impact of Organizational Culture on Quality of Life*, [w:] *Research in Organizational Change and Development*, (red.) W.R. Woodman, W.A. Pasmore, Vol. 5 1991, JAI Press, Greenwich, s. 115–142; M. Karlsson, F. Karlsson, J. Åström, T. Denk, *The effect of perceived organizational culture on employees' information security compliance*, „Information & Computer Security" 2022, Vol. 30 (3); J. Strengers, L. Mutsaers, L. van Rossum, E. Graamans, op. cit., s. 115–130; M. Dębski, M. Cieciora, P. Pietrzak, W. Bołkunow, op. cit., s. 345–355; H. Jarosiewicz, *Świadomość organizacji. O znaczeniu klimatu dla rozwoju osoby i sukcesu przedsiębiorstwa*, Uniwersytet Wrocławski, Instytut Psychologii, Wrocław 2022, s. 96; J. Sompór-Świderska, *Diagnoza kultury organizacyjnej uniwersytetu: elastyczne podejście do kierunków zmian i nowych wyzwań*, „Prace Naukowe Uniwersytetu Ekonomicznego we

potwierdziło poprawność koncepcyjną metody wartości konkurencyjnych K. Camerona i R. Quinna. Stwierdził on, że kwestionariusz posiada odpowiednie właściwości psychometryczne w zakresie trafności, rzetelności i mocy dyskryminacyjnej, a rozkłady wyników skal OCAI nie odbiegają znacząco od charakteru rozkładu normalnego.

Wybór narzędzia OCAI do badań kultury organizacyjnej w wojewódzkich sądach administracyjnych uzasadnia również przegląd systematyczny literatury dokonany przez Victora Cancino i Mario Aliaga[304], w którym to zidentyfikowano w bazach danych w okresie od 2006 do 2020 r. 131 artykułów opisujących wykorzystanie OCAI. Z powyższego przeglądu literatury oraz innych prac[305] wynika, że narzędzie zastosowane zostało w badaniach różnych organizacji zarówno z sektora publicznego, jak i w organizacjach prywatnych, np.: firmy logistyczne[306], samorządy lokalne[307], urzędy skarbowe[308], opieka zdrowotna[309]. Zauważono, że w organizacjach krajów europejskich najczęściej identyfikowana jest kultura hierarchiczna, a pożądana jest kultura klanowa. Polska badaczka Jagoda Stampór-Świderska[310], badając kulturę

Wrocławiu" 2012, nr 249, s. 390–402; A. Sitko-Lutek, op. cit., s. 83; B. Heritage, C. Pollock, L. Roberts, *Validation of the Organizational Culture Assessment Instrument,* „PLoS ONE" 2014, 9(3), e92879.

[303] G. Wudarzewski, *Validation of Cameron and Quinn's Organizational Culture Assessment Instrument (OCAI) in Polish conditions,* „Central and Eastern European Journal of Management and Economics" 2018, Vol. 6, No. 1, s. 79–105.

[304] V. Cancino, M. Aliaga, *Instrumento de evaluación de la cultura organizacional: revisión sistemática de su aplicación*, „Revista Venezolana de Gerencia" 2022, Vol. 27, No. 97, s. 107–126.

[305] M. Cieciora, P. Pietrzak, M. Dębski, K. Kandefer, W. Bołkunow, *Differences in the Perception of Organizational Culture in Non-Public Universities in Poland by Academic and Administrative Staff – A Study Based on Cameron and Quinn's Model*, „Foundations of Management" 2021, 13, s. 131–144; M. Balková, T. Jambal, *Evaluation of organizational culture in enterprises in the Czech Republic using OCAI*, „Frontiers in Psychology" 2023, 14:1297041; P. Fernandes, R. Pereira, G. Wiedenhöft, *The Effect of Organizational Cultures on Relationships between IT Governance and Individual Behavior*, „Emerging Science Journal Open Access" 2023, Vol. 7, I. 5, s 1602–1635.

[306] L. Ližbetinová, S. Lorincová, Z. Caha, *The Application of the Organizational Culture Assessment Instrument (OCAI) to Logistics Enterprises*, „NAŠE MORE: znanstveni časopis za more i pomorstvo" 2016, 63(3), (Special Issue), s. 170–176; M. Čuček, S. Mlaker Kač, *Organizational culture in logistics sector and its relation to employee satisfaction*, „Journal of Contemporary Management Issues" 2020, Vol. 25, No. 2.

[307] A. Marek, *Model wartości konkurujących w badaniu kultury organizacji samorządowych (The model of competing values in the study of the culture of local government organizations),* „Roczniki Ekonomii i Zarządzania" 2014, 6(42), s. 289–299.

[308] A. Patapas, G. Labenskyte, *Research of organisational culture and values of state tax inspectorate of N county*, „Public Policy and Administration" 2011,Vol. 10, Issue 4, s. 589–603.

[309] A. Frączkiewicz-Wronka, *Diagnozowanie kultury organizacyjnej w podmiocie leczniczym – studium szpitala publicznego*, [w:] *Instrumentarium zarządzania publicznego*, (red.) B. Kożuchowska, Ł. Sułkowski, Difin, Warszawa 2015, s. 177–198; V.H. Nguyen, T.H.T. Nguyen et al., *The validation of organisational culture assessment instrument in healthcare setting: results from a cross-sectional study in Vietnam*, „BMC Public Health" 2020, Vol. 20, 316; R.G. Bing-You, K. Varaklis, *Organizing Graduate Medical Education Programs into Communities of Practice,* „Medical Education Online" 2016, nr 2; R. Frey, M. Boyd, S. Foster, J. Robinson, M. Gott, *What's the Diagnosis? Organisational Culture and Palliative Care Delivery in Residential Aged Care in New Zealand,* „Health & Social Care in Community, 2016", 24, s. 450-462.

[310] J. Sompór-Świderska, op. cit., s. 390–402.

organizacyjną narzędziem OCAI w Instytucie Psychologii na Uniwersytecie Wrocławskim, uzyskała wyniki wskazujące na to, iż dominuje tam kultura hierarchii i rynku, zarówno w odczuciu wykładowców, jak i studentów. W obu grupach pożądanymi profilami kultury były kultura klanu i adhokracji. Podobne wyniki otrzymali Maciej Dębski, Małgorzata Cieciora, Piotr Pietrzak, Wiktor Bołkunow w badaniach[311] przeprowadzonych w ośmiu polskich uczelniach. Zauważyli oni następującą prawidłowość: w uczelniach publicznych dominowała kultura hierarchiczna, podczas gdy w uczelniach niepublicznych dominowała kultura rynkowa. Metodę OCAI zastosowano również w badaniu kultury organizacyjnej w uczelniach na całym świecie[312]. Wyniki pokazują, że kultury występujące na uczelniach wyższych różnią się w zależności od kraju i organizacji[313]. Na przykład kultura klanowa była kulturą identyfikowaną i pożądaną na Uniwersytecie Stanowym Ohio oraz na wielu chrześcijańskich uczelniach w Stanach Zjednoczonych[314]. Z kolei uniwersytety w Słowenii charakteryzowały się wysoko rozwiniętą kulturą rynkową[315], podczas gdy w szkołach wyższych z Rosji[316], Portugali i Hiszpanii[317] dominowała kultura hierarchiczna.

2.6.2. Metoda badań kultury organizacyjnej w paradygmacie interpretatywnym

Badania jakościowe powiązane z paradygmatem interpretatywnym[318] pozwalają na całościowe ujęcie zjawisk w ich naturalnym kontekście. Opierają się na rozumowaniu indukcyjnym, z danych empirycznych buduje się stopniowo

[311] M. Dębski, M. Cieciora, P. Pietrzak, W. Bołkunow, op. cit., s. 345–355, https://doi.org/10.3233/HSM-190831.

[312] M. Sousa, M.J. Raposo, J. Mendonça, B. Corchuelo, *Exploring organisational culture in higher educational institutions: a comparative study*, „International Journal of Management in Education" 2022, Volume 16, Issue 1, s. 62–82; A. Caliskan, Ch. Zhu, *Organizational Culture Type in Turkish Universities using OCAI: Perceptions of Students*, „Journal of Education Culture and Society" 2019, No. 2.

[313] N. Gaus, *Organisational culture in higher education: mapping the way to understanding cultural research*, „Journal of Further and Higher Education" 2017, No. 43, s. 848.

[314] A. A. Berrio, *An Organizational Culture Assessment Using the Competing Values Framework: A Profile of Ohio State University Extension*, „Journal of Extension" 2003, 41(2); A.M. Obenchain, W.C. Johnson, P.A. Dion, *Institutional Types, Organizational Cultures, and Innovation in Christian Colleges and Universities*, „Christian Higher Education" 2004, 3:1, s. 15–39.

[315] D. Omerzel, R. Biloslavo, A. Trnavcevic, *Knowledge management and organisational culture in higher education institutions*, „Journal for East European Management Studies" 2011, 16, s. 111–139.

[316] B. Vasyakin, M. Ivleva, Y.L. Pozharskaya, O.I. Shcherbakova, A s*tudy of the Organizational Culture at a Higher Education Institution (Case Study: Plekhanov Russian University of Economics)*, „International Journal of Environmental and Science Education" 2016, 11, s. 11515–11528.

[317] M. Sousa, M.J. Raposo, J. Mendonça, B. Corchuelo, op. cit., s. 62–82.

[318] Ł. Sułkowski, R. Lenart-Gansiniec, *Metody*…, op. cit.

uogólnienia[319]. Obserwacje, wywiady i analizy tekstów, metody charakterystyczne dla badań jakościowych[320], mogą być wykorzystywane do poznania kultury danej organizacji[321]. Ten typ badań terenowych określany jest jako etnografia organizacji. Metody stosowane przez etnografów zakładają: zazwyczaj długi okres trwania badań; bezpośredni kontakt badacza z „terenem", czyli z badaną organizacją; stosowanie tzw. gęstego opisu[322] oraz triangulację metod i źródeł danych[323].

2.7. Kultura organizacyjna w sektorze publicznym

Organizacje sektora publicznego wyróżnia nałożony na nie obowiązek prawny świadczenia powszechnie dostępnych usług publicznych[324]. Podobnie jak organizacje z sektora prywatnego, stosują one w swoim działaniu określone praktyki, procedury, cele oraz kształtują własną kulturę organizacyjną[325]. Zarządzanie nimi jest ściśle i nierozerwalnie powiązane z polityką i prawem, przy uwzględnianiu efektywności społecznej i politycznej oraz efektywności ekonomicznej wyborów dokonywanych w sektorze publicznym[326]. Kultura organizacyjna i jej wpływ na efektywność działania w organizacjach publicznych są uznawane przez badaczy za równie ważne i są analizowane podobnie jak w organizacjach sektora prywatnego[327]. Badań tego rodzaju jest przeprowadzanych mniej, często podejmowane są w nich problemy różnic występujących pomiędzy organizacjami publicznymi a prywatnymi[328]. Zauważalne są

[319] M. Kostera, P. Krzyworzeka, M. Połeć, op. cit., s. 25–28.

[320] Ibidem, s. 116–194; T. Jung, T. Scott, H. Davies, P. Bower, D. Whalley, R. Mcnally, R. Mannion, op. cit., s. 1087–1096.

[321] A. Kołodziej-Durnaś, op. cit., s. 47; Ł. Sułkowski, *Kultura organizacyjna od podstaw*, Społeczna Akademia Nauk, Łódź 2020, s. 43.

[322] C. Geertz, *Interpretation of cultures. Selected essays*, Basic Books, New York 1973, s. 3–30.

[323] Zbieranie danych przy wykorzystaniu dwóch lub większej liczby metod oraz konfrontowanie różnych ich źródeł, np. poprzez prowadzenie wywiadów z uczestnikami organizacji, posiadającymi odmienne spojrzenie na analizowane zagadnienia.

[324] B. Kożuch, K. Sienkiewicz-Małyjurek, Ł. Sułkowski, *Zarzadzanie publiczne oparte na wartościach*, Wydawnictwo Społecznej Akademii Nauk, Łódź 2021, s. 14.

[325] B. Kożuch, *Zarządzanie publiczne w teorii i praktyce polskich organizacji*, Wydawnictwo Placet, Warszawa 2004, s. 87.

[326] A. Kożuch, B. Kożuch, Ł. Sułkowski, E. Bogacz-Wojtanowska, M. Lewandowski, K. Sienkiewicz-Małyjurek, A. Szczudlińska-Kanoś, S. Jung-Konstanty, *Obszary zarządzania publicznego,* Instytut Spraw Publicznych UJ (Monografie i Studia Instytutu Spraw Publicznych Uniwersytetu Jagiellońskiego), Kraków 2016, s. 8–9.

[327] A. Frączkiewicz-Wronka, *Poszukiwanie istoty zarządzania publicznego,* [w:] *Zarządzanie publiczne – elementy teorii i praktyki*, Akademia Ekonomiczna w Katowicach, Katowice 2009, s. 36; A. Kołodziej-Durnaś, op. cit., s. 325.

[328] Ł. Sułkowski, *Kultura organizacji publicznej* [w:] *Instrumentarium zarządzania publicznego*, (red.) B. Kożuchowska, Ł. Sułkowski, Difin, Warszawa 2015, s. 92; G. Hofstede, *Culture and organizations*, „International Studies of Management & Organization" 1980, nr 10(4), s. 15–41; E.H. Schein, *Culture: The missing concept in organization studies*, „Administrative Science Quarterly" 1996, nr 41(2), s. 229–240.

w literaturze zmiany w kierunku upodabniania się sektorów prywatnego i publicznego, z jednej strony występuje społeczna odpowiedzialność korporacji[329], z drugiej organizacje publiczne stosują narzędzie, takie jak budżet zadaniowy[330].

Jak zauważył Ł. Sułkowski[331], w literaturze światowej, ale również polskiej, w przedmiocie kultury organizacyjnej w sektorze publicznym występują przede wszystkim studia przypadków poszczególnych organizacji, albo badania ograniczające się do pewnego wycinka organizacji w konkretnym kraju. Pomimo prób stworzenia uogólnionego modelu zarządzania publicznego, nieuwzględniającego zmiennych kulturowych (m.in. w nurcie nowego zarządzania publicznego – ang. *New Public Management*[332]), Ł. Sułkowski stwierdził, iż w wielu opracowaniach opisujących kulturę danej organizacji lub porównujących obiekty badań uwzględniany jest kontekst kulturowy jako zmienna mająca znaczący wpływ na zarządzanie[333]. Podobnie uważa Agnieszka Kołodziej-Durnaś[334], mówiąc o popularności idei przeprowadzania zmian w sferze norm i wartości w celu budowania kultury proefektywnościowej. W badaniach dotyczących kultury organizacyjnej sektora publicznego obiektami badań są organizacje bardzo odmienne kulturowo, np.: szpitale publiczne[335], szkoły wyższe[336], jednostki samorządu terytorialnego[337], administracja państwowa[338], armia[339] czy policja[340].

[329] A.B. Carroll, *Corporate social responsibility: Evolution of a definitional construct*, „Business and Society" 1999, vol. 38, no. 3; E. Jaworska, *Społeczna odpowiedzialności przedsiębiorstw jako źródło szans i przewagi konkurencyjnej*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Instrumenty zarządzania kosztami i dokonaniami" 2012, nr 252, , s. 180–192.

[330] A. Kołodziej-Durnaś, op. cit., s. 338.

„Budżetowanie zadaniowe wpisuje się w ogólnoświatowy trend transformacji administracji publicznej i wprowadzenia na dużą skalę podejścia definiowanego jako New Public Management. Metoda ta jest próbą zastosowania modeli i zasad zarządzania, wypróbowanych z wielkim powodzeniem w sektorze prywatnym". Pełni rolę „(…) planu finansowego w układzie budżetowym; który jest wdrażany w systemie finansów publicznych", źródło: J. Toborek-Mazur, *Budżet zadaniowy jako nowy plan finansowy systemu finansów publicznych*, Studia Ekonomiczne, nr 252, 2015, s. 159–174.

[331] Ł. Sułkowski, *Kultura organizacji publicznej*…, op. cit., 92–115.

[332] C. Hood, *A Public Management for All Seasons?* Public Administration, 69(1), 1991, s. 3–19.

[333] J.E. Lane, *New public management: an introduction*, Routledge 2002.

[334] A. Kołodziej-Durnaś, op. cit., s. 325.

[335] B. Buchelt, J. Jonczyk, *Powiązania kultury organizacyjnej i zarządzania zasobami ludzkimi w szpitalach publicznych,* „Zarządzanie Publiczne" 2017, 40, s. 50–64; A. Szeptuch, *Pomiar kultury organizacyjnej w organizacjach ochrony zdrowia,* e-Mentor, [s. l.], vol. 65, 3, 2016, s. 60–67; A. Frączkiewicz-Wronka, *Diagnozowanie*…, op. cit., s. 177–198.

[336] M. Dębski, M. Cieciora, P. Pietrzak, W. Bołkunow, op. cit., s. 345–355.

[337] K. Krukowski, *Cechy kultury organizacyjnej na różnych poziomach dojrzałości procesowej wybranych urzędów miast,* „Optimum. Economic Studies" 2018, nr 1(91), s. 114–125; M. Siemiński, K. Krukowski, P. Szamrowski, op. cit.

A. Pawluczuk, U. Ryciuk, *Variables Shaping the Culture in Organizational Learning in Municipalities,* „International Journal of Contemporary Management" 2015, Vol. 14, No. 2, s. 51–62; A. Podgórniak-Krzykacz, *The relationship between the professional, social, and political experience and leadership style of mayors and organisational culture in local government. Empirical evidence from Poland,* „PLoS ONE" 2021, 16(12), s. 1–23.

Wspólne dla tych organizacji są następujące elementy: publiczne źródła finansowania ich działalności, szczególna rola wartości i odpowiedzialności publicznej, prawny wymóg równego traktowania interesariuszy, problemy z jasnym zrozumieniem skuteczności i efektywności oraz wysokie upolitycznienie podejmowania decyzji[341]. W związku z różnorodnością wewnętrzną sektora publicznego, prowadząc analizę kultur tego zbioru organizacji, należy mieć świadomość, że poszukiwane są jedynie dominujące wzorce. Ł. Sułkowski zaproponował w swoim opracowaniu wybór dychotomicznych typologii kultur organizacji publicznych, biorąc pod uwagę powszechność ich stosowania w badaniach (Tabela 2.4).

Tabela 2.4. . Dychotomiczne typologie kultur organizacyjnych

kultura pragmatyczna	versus	kultura biurokratyczna
kultura konserwatywna		kultura innowacyjna
kultura hierarchiczna		kultura równościowa
kultura indywidualistyczna		kultura kolektywistyczna
kultura słaba		kultura silna
kultura pozytywna		kultura negatywna

Źródło: opracowanie własne na podstawie: *Ł. Sułkowski, Kultura organizacji publicznej, [w:], Instrumentarium zarządzania publicznego, (red.) B. Kożuchowska, Ł. Sułkowski, Difin, Warszawa 2015, s. 100.*

Z analizy literatury wynika, że w organizacjach publicznych dominującymi cechami kulturowymi są: biurokratyzacja, konserwatyzm, hierarchiczność i kolektywizm[342]. Kultura biurokratyczna jest wysoko sformalizowana z dominacją komunikacji pisemnej. Ważniejsze od skuteczności i szybkości działania są porządek, stabilność i jedność[343]. Konserwatyzm wyraża się szacunkiem do tradycji i do osób

[338] L. Młodzik, *Kultura organizacyjna w instytucji publicznej*, Wydawnictwo Stowarzyszenia Maximus Primus, Zielona Góra 2014.

[339] J. Kacała, A. Michaluk, op. cit., s. 265–273; K.B. Fosher, R. Lane, E. Tarzi, K. Post, E.M. Gauldin, B. Tashev, J. Edwards, J.D. McLean, *Translational Research in a Military Organization: The Marine Corps Organizational Culture Research Project*, „Annals of Anthropological Practice" 2020, 44(1), s. 14–32.

[340] D. Gutschmidt, A. Vera, *Organizational culture, stress, and coping strategies in the police: An empirical investigation*, „Police Practice & Research" 2022, 23(5), s. 507–522; K. Amrozy, *O czym mówimy, kiedy mówimy o kulturze policyjnej?* „Athenaeum. Polskie Studia Politologiczne" 2018, nr 57.

[341] A. Frączkiewicz-Wronka, *Zarządzanie publiczne – elementy teorii i praktyki*, Wydawnictwo Akademii Ekonomicznej w Katowicach, Katowice 2009; B. Kożuch, K. Sienkiewicz-Małyjurek, Ł. Sułkowski, op. cit., s. 88–89.

[342] Ł. Sułkowski, *Kultura organizacji publicznej*, [w:] B. Kożuchowska, Ł. Sułkowski, (red.) *Instrumentarium zarządzania publicznego*, Difin, Warszawa 2015, s. 111; A. Frączkiewicz-Wronka, *Diagnozowanie*…, op. cit., s. 197; K. Krukowski, *Cechy*…, op. cit., s. 114–125.

[343] M. Weber, *The Theory of Social and Economic Organization*, The Free Press, New York 1965;

doświadczonych w organizacji oraz niższym poziomem akceptacji ryzyka. W organizacjach hierarchicznych preferowanymi wartościami są dyscyplina i porządek. które to są narzucane przez przełożonych. Władza jest scentralizowana, występuje wiele szczebli kierowniczych oraz zróżnicowanie w uprawnieniach grup pracowniczych. W organizacjach publicznych występuje wysoki stopień kolektywizmu, cele grupowe są ważniejsze od indywidualnych.

Kultury organizacji publicznych częściej bliższe są kulturom słabym, ponieważ model interesariuszy prowadzi do powstawania subkultur, a nawet kontrkultur wewnątrz organizacji, zauważalny jest niski stopień lojalności pracowników wobec całej organizacji. Przykładem mogą być badania kulturowe przeprowadzane w szpitalach, w których silne subkultury tworzą np. lekarze i pielęgniarki[344]. W sektorze publicznym przeważają cechy kultury negatywnej, które są konsekwencją m.in. biurokratyzmu i konserwatyzmu. Negatywna kultura[345] charakteryzuje się: niską aktywnością i elastycznością pracowników, postawą oczekiwania na wytyczne przełożonych w celu rozwiązywania problemów, koncentracją na własnych obowiązkach.

Poszukując istoty kultury organizacji publicznych, warto zauważyć, że jej odmienność wynika przede wszystkim z tego, że osoby zarządzające tymi organizacjami muszą łączyć efektywność z realizacją celów prospołecznych, które z reguły nie są efektywne ekonomicznie[346].

J.W. Whorton, J.A. Whorton, *A perspective on the challenge of public management: Environmental paradox and organizational culture*, Academy of Management Review, nr 6.3, 1981, s. 357–361.

[344] D. Simonet, *The new public management theory and the reform of European health care systems: An international comparative perspective*, „International Journal of Public Administration" 2011, 34(12), s. 815–826; P. Bate, *Changing the culture of a hospital: from hierarchy to networked community*, „Public Administration" 2000, 78(3), s. 485–512.

[345] L. Zbiegień-Maciąg, *Kultura w organizacji: Identyfikacja kultur znanych firm*, PWN, Warszawa 1999, s. 52–63.

[346] M. Siemiński, K. Krukowski, P. Szamrowski, op. cit., s. 42.

3. Metodyka badań

3.1. Identyfikacja luki badawczej

3.1.1. Przegląd i analiza literatury

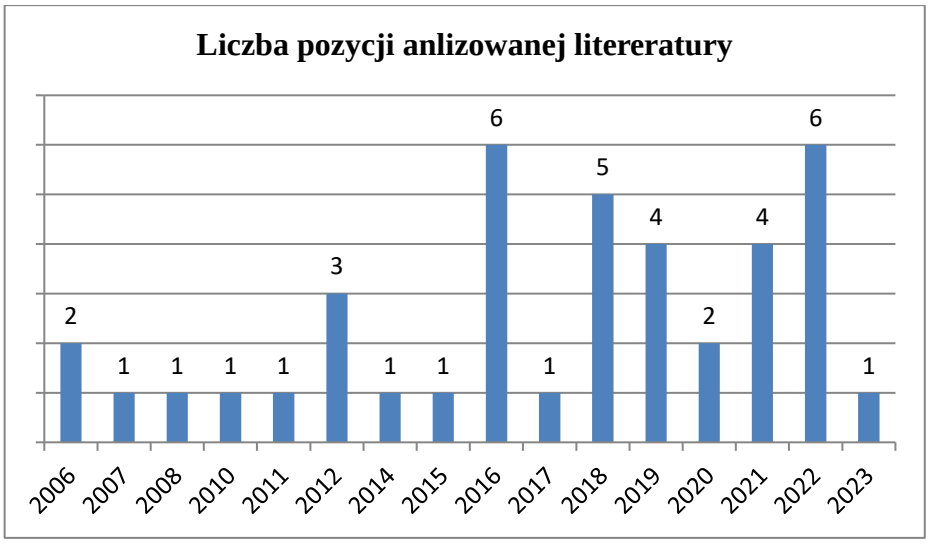
Celem przeprowadzonego systematycznego przeglądu literatury[347] było sprawdzenie stanu wiedzy w obszarze badań identyfikujących relacje pomiędzy kulturą organizacyjną a dojrzałością systemów zarządzania bezpieczeństwem informacji oraz zidentyfikowanie luki badawczej[348]. Przegląd ten był elementem pierwszego etapu postępowania badawczego (Rysunek 0.1). W styczniu 2023 r. dokonano analizy publikacji dostępnych poprzez multiwyszukiwarki EBSCO oraz w rozpowszechnionych wśród badaczy bazach bibliometryczno-abstraktowych: Web of Science oraz Scopus[349], w obszarach Zarządzania (ang. *Management*) i Informatyki (ang. *Computer Science*), bez ograniczeń czasowych. Pierwsze badanie było badaniem pilotażowym. Narzędzie EBSCO Discovery Service umożliwia jednoczesne przeszukiwanie wielu baz[350], m.in.: ScienceDirect, Scopus, SpringerLink, Willey. Decyzja o braku przyjętego ograniczenia czasowego została podjęta w związku z małą liczbą publikacji w badanym obszarze oraz informacjami na temat dat publikacji. Wszystkie wyszukane publikacje powstały w XXI w. (Rysunek 3.1). Kryteriami wyboru baz oraz narzędzi użytych do wyszukiwania były: dostępność artykułów związanych z badaną tematyką, zaawansowane mechanizmy wyszukiwania, dostępność artykułów w języku polskim i angielskim.

[347] R. Lenart-Gansiniec, *Systematyczny przegląd literatury w naukach społecznych : przewodnik dla studentów, doktorantów i nie tylko*, Wydawnictwo Naukowe Scholar, Warszawa 2021; J. Davis, K. Mengersen, S. Bennett, L. Mazerolle, *Viewing systematic reviews and meta-analysis in social research through different lenses*, „Springer Plus" 2014, 3, 511; H. Snyder H., *Literature review as a research methodology: An overview and guidelines*, „Journal of Business Research" 2019, Vol. 104, s. 333–339.

[348] W. Czekon, *Podstawy metodologii badań w naukach o zarządzaniu*, Wolters Kluwer, Warszawa 2015, s. 119–139.

[349] A.A. Chadegani, M. Hadi Salehi, M. Md Yunus, H. Farhadi, M. Fooladi, M. Farhadi, and N. Ale Ebrahim, *A Comparison between Two Main Academic Literature Collections*, „Asian Social Sciences" 2013, Vol. 9, No. 5; S.P. Paul, A. Shruti, *A Systematic Analysis of Research Trends on Network Control System in Wireless Sensor Network*, 2022, 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Advanced Computing and Communication Systems (ICACCS), 2022 8th International Conference on 1 (March), s. 1758–1763.

[350] Bazy, do których licencje posiada Biblioteka Uniwersytetu Łódzkiego w roku 2023; A. Kołodziej-Durnaś, *Kultura organizacji – idea i instrumentalizacja. Socjologiczne studium krytyczne*, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2012, s. 123.



Rysunek 3.1. Liczba pozycji analizowanej literatury
Źródło: opracowanie własne.

Przeszukując bazy, wykorzystano następujące zwroty w językach angielskim i polskim:

„information security management" AND „system" AND „maturity" AND „organizational culture"

"zarządzanie bezpieczeństwa informacji" AND „system" AND „dojrzałość" AND „kultura organizacyjna"

Odnotowano brak w rezultatach przeszukiwań baz literaturowych artykułów w języku polskim. Tabela 3.1 przedstawia wyniki dotyczące anglojęzycznych prac i proces ich weryfikacji.

Tabela 3.1. Kryteria i wyniki przeszukiwań baz literaturowych

Kryteria	**EBSCO**	**Web of Science**	**Scopus** Computer Science, Social Science Busines, Management and Accounting
„information security management" AND "system" AND "maturity" AND „organizational culture" Zrecenzowane naukowo, w języku angielskim	8	2	(22 – bez ograniczeń na obszar badań) 22
Dostępny pełen tekst publikacji	7		2

Kryteria	EBSCO	Web of Science	**Scopus** Computer Science, Social Science Busines, Management and Accounting
Artykuły zamieszczone w czasopismach naukowych	6	2	2
Po wyeliminowaniu duplikatów	5	2	2
Po weryfikacji abstraktów, tytułów	2	1	1
Różne artykuły – łącznie	2		

Źródło: opracowanie własne.

Poniżej przedstawiono dane dotyczące dwóch publikacji, które są rezultatem przeprowadzonych przeszukiwań baz literaturowych:

1. Mohamed N., Kaur A.P Gian Singh J., *A Conceptual Framework for Information Technology Governance Effectiveness in Private Organizations*, „Information Management & Computer Security" 2012, Vol. 20, nr 2, s. 88–106.
2. Pollini A., Tiziana C.C., Tedeschi A., Ruscio D., Save L., Chiarugi F., Guerri D., *Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach*, Cognition, „Technology & Work" 2022, 24, nr 2, s. 371–390.

Rozszerzono badania literaturowe do poszukiwań publikacji dotyczących nie tylko relacji pomiędzy kulturą organizacyjną a dojrzałością systemów zarządzania bezpieczeństwem informacji, ale również pomiędzy kulturą organizacyjną a zarządzaniem bezpieczeństwem informacji.

Do przeszukiwań baz zostały wykorzystane następujące zwroty w językach angielskim i polskim:

„information security management" AND „organizational culture"

"zarządzanie bezpieczeństwa informacji" AND "kultura organizacyjna"

Ponownie w rezultatach badania nie pojawiły się artykuły w języku polskim. Tabela 3.2 przedstawia wyniki przeszukiwania baz literaturowych i proces ich weryfikacji.

Tabela 3.2. Kryteria i wyniki rozszerzonych przeszukiwań baz literaturowych

Kryteria	**EBSCO**	**Web of science**	**Scopus** Computer Science, Social Science Busines, Management and Accounting
„information security management" AND „organizational culture" Zrecenzowane naukowo, w języku angielskim	137	159	(332 – bez ograniczeń na obszar badań) 246
Dostępny pełen tekst publikacji	115	42	42
Artykuły zamieszczone w czasopismach naukowych	77	31	30
Po wyeliminowaniu duplikatów	49		
Po weryfikacji abstraktów, tytułów	25	16 (10 artykułów różnych niż ebsko)	13 (4 artykuły różne niż przeszukiwania wcześniejsze)
Różne artykuły – łącznie	39		

Źródło: opracowanie własne.

Poniżej przedstawiono wykaz publikacji poddanych analizie szczegółowej. Pozycja numer 40 to artykuł, który znalazł się w wynikach pierwszej podjętej próby przeszukiwania baz literaturowych, a nie ujęto go w wynikach drugiej próby:

(1) Hassandoust F., Subasinghage M., Johnston A.C., *A Neo-Institutional Perspective on the Establishment of Information Security Knowledge Sharing Practices*, „Information & Management" 2022, Vol. 59 (1).

(2) Da Veiga A., *An Approach to Information Security Culture Change Combining ADKAR and the ISCA Questionnaire to Aid Transition to the Desired Culture*, „Information & Computer Security" 2018, Vol. 26 (5), s. 584–612.

(3) Tolah A., Furnell S.M., Papadaki M., *An Empirical Analysis of the Information Security Culture Key Factors Framework*, „Computers & Security" 2021, Vol. 108.

(4) Thomson K., Niekerk J. van, *Combating Information Security Apathy by Encouraging Prosocial Organisational Behaviour*, „Information Management & Computer Security" 2012, 20 (1), s. 39–46.

(5) Hogail A.A., *Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study*, „IJSIA" 2015, Vol. 9 (7), s. 163–178.

(6) Lin, C. Wittmer J.L.S., Luo X.R., *Cultivating Proactive Information Security Behavior and Individual Creativity: The Role of Human Relations Culture and IT*

Use Governance, „Information & Management" 2022, Vol. 59 (6).

(7) Da Veiga A., Martins N., *Defining and Identifying Dominant Information Security Cultures and Subcultures,* „Computers & Security" 2017, 70, s. 72–94.

(8) Da Veiga A., Astakhova L.V., Botha A., Herselman M, *Defining Organisational Information Security Culture—Perspectives from Academia and Industry,* „Computers & Security" 2020, Vol. 92.

(9) Uchendu B., Nurse J.R.C., Bada M., Furnell S., *Developing a Cyber Security Culture: Current Practices and Future Needs,* „Computers & Security" 2021, Vol. 109.

(10) Amankwa E., Loock M., Kritzinger E., *Establishing Information Security Policy Compliance Culture in Organizations,* „Information & Computer Security" 2018, Vol. 26(4), s. 420–436.

(11) Ernest Chang S., Lin C., *Exploring Organizational Culture for Information Security Management,* „Industrial Management & Data Systems" 2007, 107 (3), s. 438–458.

(12) Humaidi N., Balakrishnan V., *Indirect Effect of Management Support on Users' Compliance Behaviour towards Information Security Policies*, „Health Information Management Journal" 2018, Vol. 47 (1), s. 17–27.

(13) Ali R.F., Dominic P.D.D., Ali S.E.A., Rehman M., Sohail A, *Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance,* „Applied Sciences" 2021, Vol. 11 (8).

(14) Kessler S.R., Pindek S., Kleinman G., Andel S.A., Spector P.E., *Information Security Climate and the Assessment of Information Security Risk among Healthcare Employees*, „Health Information Management Journal" 2020, Vol. 26 (1), s. 461–473.

(15) Niekerk J.F. van, Solms R. von, *Information Security Culture: A Management Perspective*, „Computers & Security" 2010, Vol. 29 (4), s. 476–486.

(16) Flores W.R., Antonsen E., Ekstedt M., *Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture*, „Computers & Security" 2014, 43, s. 90–110.

(17) Soomro Z.A., Shah M.H., Ahmed J., *Information Security Management Needs More Holistic Approach: A Literature Review*, „International Journal of Information Management" 2016, 36 (2), s. 215–225.

(18) Singh A.N., Gupta M.P., *Information Security Management Practices: Case Studies from India,* „Global Business Review" 2019, Vol. 20 (1), s. 253–271.

(19) Ashenden D., *Information Security Management: A Human Challenge?* Information Security Technical Report 2008, 13 (4), s. 195–201.

(20) Knapp K.J., Marshall T.E., Kelly R.R., Nelson F.F., *Information Security: Management's Effect on Culture and Policy,* „Information Management & Computer Security" 2006, Vol. 14 (1), s. 24–36.

(21) Dhillon G., Syed R., Pedron C., *Interpreting Information Security Culture: An Organizational Transformation Case Stud*y, „Computers & Security" 2016, Vol. 56, s. 63–69.

(22) Pollini A., Tiziana C.C., Tedeschi A., Ruscio D., Save L., Chiarugi F., Guerri D., *Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach,* „Cognition, Technology & Work" 2022, 24, nr 2 s. 371–390.

(23) Hu Q., Dinev T., Hart P., Cooke D., *Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture: Managing Employee Compliance with Information Security Policies,* „Decision Sciences" 2012, Vol. 43 (4), s. 615–660.

(24) Sharma S., Aparicio E., *Organizational and Team Culture as Antecedents of Protection Motivation among IT Employees,* „Computers & Security" 2022, 120.

(25) Pérez-González D., Preciado S.T., Solana-Gonzalez P., *Organizational Practices as Antecedents of the Information Security Management Performance: An Empirical Investigation,* „Information Technology & People" 2019, Vol. 32 (5), s. 1262–1275.

(26) Hassandoust F., Johnston A.C., *Peering through the Lens of High-reliability Theory: A Competencies Driven Security Culture Model of High-reliability Organisations,* „Information Systems Journal" 2023, Vol. 33(5).

(27) Karlsson M., Denk T., Åström, J. *Perceptions of Organizational Culture and Value Conflicts in Information Security Management,* „Information & Computer Security" 2018, Vol. 26 (2), s. 213–229.

(28) Akter S., Uddin M.R., Sajib S., Lee W.J.T., Michael K., Hossain M.A., *Reconceptualizing Cybersecurity Awareness Capability in the Data-Driven Digital Economy,* „Annals of Operations Research" 2022.

(29) Flores R.W., Ekstedt M., *Shaping Intention to Resist Social Engineering through Transformational Leadership, Information Security Culture and Awareness*,

„Computers & Security” 2016, Vol. 59, s. 26–44.

(30) Harnesk D., Lindström J., *Shaping Security Behaviour through Discipline and Agility: Implications for Information Security Management,* „Information Management & Computer Security” 2011, Vol. 19 (4), s. 262–276.

(31) Arsenijevic O., Trivan D., Milosevic M., *Storytelling as a Modern Tool of Construction of Information Security Corporate Culture*, „Industrial Organization” 2016, Vol. 62 (4), s. 105–114.

(32) Kam H.-J., Mattson T., Kim D.J., *The "Right" Recipes for Security Culture: A Competing Values Model Perspective*, „Information Technology & People” 2021, Vol. 34 (5), s. 1490–1512.

(33) Karlsson M., Karlsson F., Åström J., Denk T., *The Effect of Perceived Organizational Culture on Employees' Information Security Compliance*, „Information & Computer Security” 2022, Vol. 30 (3), s. 382–401.

(34) Chmura J., *The impact of positive organisational culture values on information security management in the company*, „Journal of Positive Management” 2016, Vol. 7 (1), 87–98.

(35) Tang M., Li M., Zhang T., *The Impacts of Organizational Culture on Information Security Culture: A Case Study*, „Information Technology & Management” 2016, Vol. 17 (2), s. 179–186.

(36) Burdon M., Coles-Kemp L., *The Significance of Securing as a Critical Component of Information Security: An Australian Narrative*, „Computers & Security” 2019, Vol. 87.

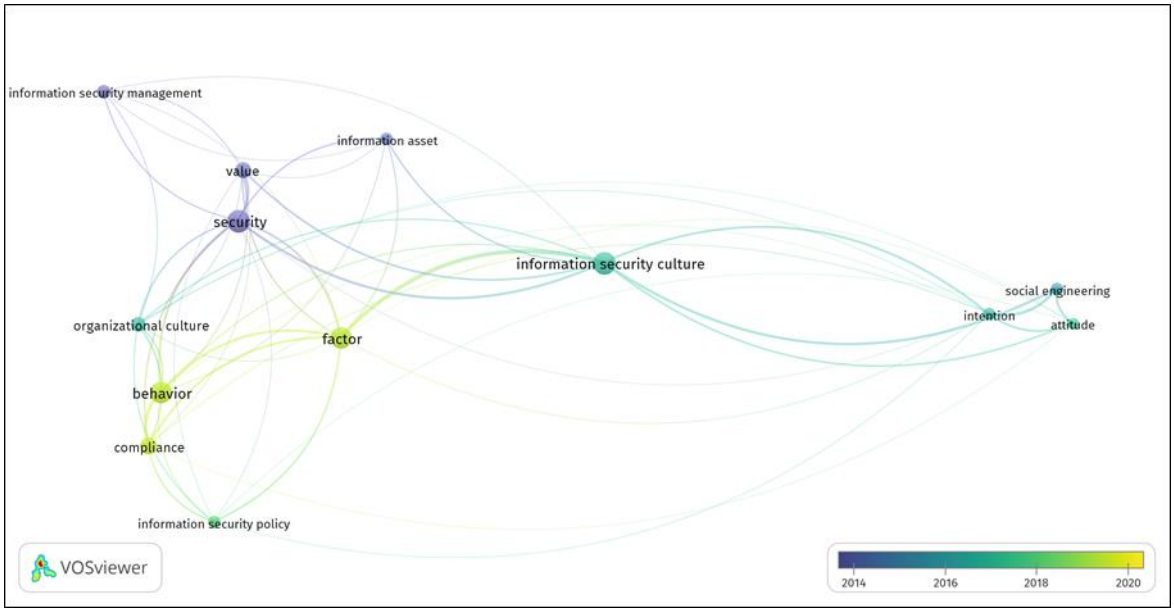
(37) Dhillon G., Torkzadeh G., *Value-Focused Assessment of Information System Security in Organizations*, „Information Systems Journal” 2006, Vol. 16 (3),s. 293–314.

(38) Khan H.U., AlShare K.A., *Violators versus Non-Violators of Information Security Measures in Organizations—A Study of Distinguishing Factors*, „Journal of Organizational Computing and Electronic Commerce” 2019, Vol. 29 (1), s. 4–23.

(39) Sommestad T., *Work-Related Groups and Information Security Policy Compliance*, „Information & Computer Security” 2018, Vol. 26 (5), s. 533–550.

(40) Mohamed N, Kaur A/P Gian Singh J., *A Conceptual Framework for Information Technology Governance Effectiveness in Private Organizations*, „Information Management & Computer Security” 2012, Vol. 20, nr 2, s. 88–106.

Następnie przeprowadzono analizę z wykorzystaniem narzędzia przeznaczonego do oceny danych jakościowych, opierającego się na technikach uczenia maszynowego (ang. *computer-assisted qualitative data analysis*), co pozwoliło na szczegółową analizę tematyczną oraz relacyjną wybranych pozycji literatury. Graficzną prezentację wyodrębnionych tematów zaprezentowano poniżej (Rysunek 3.2).



Rysunek 3.2. Mapa tematów i koncepcji wyodrębniona w analizowanej literaturze
Źródło: opracowanie własne wykonane przy użyciu oprogramowania VOSviewer.

Tematy zostały pogrupowane w trzy klastry ze względu na wzajemne powiązania w badaniach. Można zauważyć, że wyodrębnienie klastrów było związane z czasem powstania artykułów. Tabela 3.3 zawiera tłumaczenie angielskich nazw tematów.

Tabela 3.3. Zestawienie tłumaczenia na język polski nazwy tematów i koncepcji wyodrębnionych przez oprogramowanie VOSviewer wraz z przyporządkowaniem do klastra

Lp.	Nazwa w języku angielskim	Tłumaczenie na język polski	Numer klastra
1	factor	czynnik	1
2	information asset	zasób informacyjny	1
3	information security culture	kultura bezpieczeństwa informacji	1
4	information security management	zarządzanie bezpieczeństwem informacji	1
5	management	kierownictwo	1
6	organisation	organizacja	1
7	security	bezpieczeństwo	1
8	value	wartość	1
9	behavior	zachowanie	2
10	compliance	zgodność	2
11	information security policy	polityka bezpieczeństwa informacji	2
12	organizational culture	kultura organizacyjna	2

Lp.	Nazwa w języku angielskim	Tłumaczenie na język polski	Numer klastra
13	user	użytkownik	2
14	attitude	postawa	3
15	intention	zamiar	3
16	social engineering	inżynieria społeczna	3

Źródło: opracowanie własne.

Większość badań, bo aż 90%, ma charakter badań empirycznych, terenowych. W nawiasach kwadratowych zostały podane numery porządkowe z zamieszczonego powyżej wykazu publikacji poddanej szczegółowej analizie. Część badań przeprowadzono metodą mieszaną z wykorzystaniem technik zarówno badań jakościowych, jak i ilościowych [5, 16, 20, 21, 22, 26, 29, 34]. W analizowanej literaturze pojawiało się wcześniej niezdefiniowane w dysertacji pojęcie *kultura bezpieczeństwa informacji,* które zostanie omówione w następnym podrozdziale.

Badacze podkreślają znaczenie ustanawiania odpowiednich praktyk[351] i potrzeby pielęgnowania kultury przestrzegania zasad [1, 10, 22, 23, 25, 26, 35] dla zapewniania zgodności (ang. *compliance*) zachowania (ang. *behavior*) pracowników z politykami bezpieczeństwa informacji (ang. *information security policies*). Osoby odpowiedzialne w organizacji za bezpieczeństwo (ang. *security*) informacji w organizacji powinny skupić się na działaniach zmierzających do przekonania najwyższego kierownictwa (ang. *management*) do ważności działań na rzecz bezpieczeństwa informacji oraz zwiększenia jego zaangażowania w wymuszanie zmian i prowadzenie nadzoru ich wykonania [1, 10, 12, 17, 18, 19, 20, 22, 23, 26, 34].

Z badań wynika, iż organizacje stają w obliczu zagrożeń bezpieczeństwa w odniesieniu do swoich zasobów informacyjnych (ang. *information assets*). Zagrożenia te wynikają głównie z reprezentowanych wartości (ang. *value*), postaw (ang. *attitudes*) i zachowań ich własnych pracowników [2, 3, 4, 5, 6, 7, 8, 10, 13, 14, 15, 19, 22, 30, 34]. Eliminację nieodpowiednich zachowań można uzyskać przez zmianę kultury bezpieczeństwa informacji (ang. *information security culture*), która jest podsystemem[352] kultury organizacyjnej (ang. *organizational culture*). Część artykułów (57%) opisuje kulturę bezpieczeństwa informacji tak jak kulturę organizacyjną, jako zmienną wewnętrzną, którą można modyfikować, kształtować, udoskonalać.

[351] F. Hassandoust, M. Subasinghage, A.C. Johnston, *A Neo-Institutional Perspective on the Establishment of Information Security Knowledge Sharing Practices*, „Information & Management" 2022, Vol. 59 (1).

[352] A. da Veiga, L.V. Astakhova, A. Botha, M. Herselman, *Defining Organisational Information Security Culture—Perspectives from Academia and Industry*, „Computers & Security" 2020, Vol. 92.

W badaniach poszukiwane są czynniki (ang. *factors*), które wpływają na kulturę bezpieczeństwa informacji [3, 8, 9, 21, 26, 29, 30, 37, 38, 39]. Wyodrębniane są z nich te, które pozwalają doskonalić, czyli zwiększać pozioma dojrzałości zarządzania bezpieczeństwem informacji (ang. *information security management*) [3, 11, 34, 40]. Naukowcy podejmują badania, mające na celu określenie wpływu cech kultury organizacyjnej na skuteczność wdrażania zarządzania bezpieczeństwem informacji [10, 11, 13] lub badają, jak kultura organizacyjna wpływa na zamiar (ang. *intention*) przestrzegania polityki bezpieczeństwa informacji istniejącej w organizacji [15, 23, 24, 27]. Podczas gdy cechy kultury organizacyjnej zorientowanej na kontrolę, skuteczność i spójność mają pozytywny wpływ na zasady zarządzania bezpieczeństwem informacji, to cechy kultury organizacyjnej zorientowanej na elastyczność, kooperatywność i innowacyjność, nie są w znaczący sposób powiązane z tymi zasadami. Zauważono jeden wyjątek: współpraca jest negatywnie powiązana z poufnością [11]. Badania pokazują, że biurokratyczna forma kultury organizacyjnej najskuteczniej sprzyja przestrzeganiu polityki bezpieczeństwa informacji przez pracowników [32, 33]. Zauważono, podobnie jak dla kultury organizacyjnej, wpływ kultury narodowej na kulturę bezpieczeństwa informacji, jest to czynnik zewnętrzny [8, 9, 16].

Badacze widzą też potrzebę zrozumienia podłoża konfliktów wartości pomiędzy bezpieczeństwem informacji a innymi wartościami organizacyjnymi. Zaobserwowano, że konflikty wartości [13, 22, 27] dotyczące bezpieczeństwa informacji regularnie występują wśród pracowników zarówno w sektorze prywatnym, jak i publicznym. Występowanie konfliktów wartości jest powiązane, według badanych, z sytuacją w pracy, wrażliwością informacyjną i postrzeganiem kultury organizacyjnej. Osoby, które postrzegają swoje organizacje jako posiadające elastyczną kulturę zorientowaną na zewnątrz, częściej doświadczają konfliktów wartości [27]. Rozwiązaniem konfliktów mogą być poszukiwania konsensusu i zaangażowania w wartości, które umożliwiają osiągnięcie bezpieczeństwa. Zauważono, że kluczową kwestią jest zdolność osób do „właściwego zrozumienia komunikatu dotyczącego bezpieczeństwa". Komunikat służy do stworzenia uzgodnionego konsensusu w zakresie wartości w środowiskach ogarniętych konfliktem [36].

Podkreślane są skuteczność inicjatyw szkoleniowych w poprawie postrzegania i akceptacji przeprowadzanych zmian na rzecz poprawy bezpieczeństwa informacji [2, 4, 13, 15, 17, 22, 25, 26, 28, 30] oraz praktyka dzielenia się wiedzą ze współpracownikami w zakresie bezpieczeństwa informacji [1, 16, 25, 31]. Motywacje

pracowników, ich wewnętrzne przekonania są również ważne dla kształtowania kultury bezpieczeństwa informacji [4, 13, 21, 22, 24].

Badacze zajmowali się także identyfikacją w organizacji subkultur bezpieczeństwa informacji [7, 14]. Zauważyli, że stosując interwencje w zakresie bezpieczeństwa informacji, organizacje mogą obrać za cel swoje subkultury wysokiego ryzyka i monitować wprowadzane zmiany, minimalizując w ten sposób ryzyko utraty bezpieczeństwa informacji w związku z niewłaściwym zachowaniem swoich członków [7, 24].

W omawianej literaturze postawiono pytanie, jak kultura organizacyjna lub jej elementy (np.: zachowanie, przywództwo, postawy, wartości) wpływają na efektywność systemu zarządzania bezpieczeństwem informacji [34]. Połączenie kultury organizacyjnej i „organizowania" bezpieczeństwa informacji składa się na pojęcie kultury bezpieczeństwa informacji. Z analizy wyników badań można wywnioskować, że kulturę bezpieczeństwa informacji, w związku z jej naturą, należy kultywować, a nie sztywno projektować[353] [9, 34].

Zauważalnym trendem jest zmiana podejścia w analizowanych pracach badawczych w temacie relacji kultury organizacyjnej i zarządzania bezpieczeństwem informacji (Rysunek 3.2). Początkowo badania skupiały się na bezpieczeństwie zasobów informacyjnych, na aspektach technicznych. Badacze zajmowali się modelami zarządzania bezpieczeństwem informacji. Późniejsze badania traktują przede wszystkim o wpływie czynników związanych z kulturą organizacyjną na efektywność i skuteczność wdrożonych polityk bezpieczeństwa informacji.

3.1.2. Kultura bezpieczeństwa informacji

W centralnej części mapy wygenerowanej przez oprogramowanie VOSviewer pojawiło się pojęcie kultury bezpieczeństwa informacji. Wiąże się ono ze wszystkimi pozostałymi wyodrębnionymi w badaniu tematami (Rysunek 3.2). Fredrik Karlsson w swojej przeglądowej pracy[354] przedstawił sięgającą początku obecnego stulecia historię[355] zainteresowania badaczy tym pojęciem oraz próbował odpowiedzieć na

[353] B. Uchendu, J.R.C. Nurse, M. Bada, S. Furnell, *Developing a Cyber Security Culture: Current Practices and Future Needs*, „Computers & Security" 2021, Vol. 109.

[354] F. Karlsson, *Information security culture – state-of-the-art review between 2000 and 2013*, „Information & Computer Security" 2015, Vol. 23, No. 3, s. 246–285.

[355] C. Vroom, R. von Solms, *Towards information security behavioural compliance*, „Computers and Security" 2004, Vol. 23, No. 3, s. 191–198; A. Da Veiga, N. Martins, *Defining and Identifying Dominant Information Security Cultures and Subcultures*, „Computers & Security" 2017, 70, s. 72–94; S.

pytanie, jakie tematy związane z kulturą bezpieczeństwa informacji podlegały badaniu. Jego praca wykazała cztery metapytania, które powtarzały się najczęściej w badanych pracach:

1) Czym jest kultura bezpieczeństwa informacji?
2) Jakie są korzenie kultury bezpieczeństwa informacji?
3) Jakie są rezultaty różnych kultur bezpieczeństwa informacji?
4) Jak kultywować kulturę bezpieczeństwa informacji?

Zauważył, że najmniej badań dotyczy rezultatów różnych kultur bezpieczeństwa informacji. Należy stwierdzić, że w pracach późniejszych, również w tych, które znalazły się w wynikach przeprowadzonego systematycznego przeglądu literatury, znajdują się badania dotyczące rezultatów danej kultury bezpieczeństwa informacji [10, 34]. W tym rozdziale dysertacji podjęta będzie próba przedstawienia, na podstawie wykonanego przeglądu literatury, odpowiedzi tylko na pierwsze pytanie. Według F. Karlssona istnieje powszechne zrozumienie, że kultura bezpieczeństwa informacji w danej organizacji składa się ze wspólnego wzorca wartości, modeli mentalnych i działań, które z czasem są przedmiotem wymiany między członkami organizacji, wpływając na bezpieczeństwo informacji[356]. Z jego badań wynika, że kilka teorii związanych z kulturą bezpieczeństwa informacji jest związanych z modelami lub typologiami kultur organizacyjnych, np. z modelami Scheina[357] z 1985 r. lub G. Hofstede[358] z 1997 r.

Według da Veigi [2] kultura bezpieczeństwa informacji to: „postawy, założenia, przekonania, wartości i wiedza, których pracownicy/interesariusze używają do interakcji z systemami i procedurami organizacji w dowolnym momencie. Interakcja skutkuje akceptowalnym lub niedopuszczalnym zachowaniem, widocznym w artefaktach i kreacjach, które stają się częścią sposobu, w jaki wykonywane są działania w organizacji w celu ochrony jej zasobów informacyjnych”[359]. Areej Alhogail [5] definiuje pojęcie jako: „Zbiór postrzegań, postaw, wartości, założeń i wiedzy, które kierują interakcją człowieka z zasobami informacyjnymi w organizacji w celu wywarcia

Ernest Chang, C. Lin, *Exploring Organizational Culture for Information Security Management*, „Industrial Management & Data Systems” 2007, 107 (3), s. 438–458.

[356] F. Karlsson, *Information*…, op. cit., s. 246–285.

[357] E.H. Schein, *Organizational Culture and Leadership*, Jossey-Bass Publisher, San Francisco–Washington–London 1985.

[358] G. Hofstede, G.J. Hofstede, M. Minkov, *Kultury i organizacje. Zaprogramowanie umysłu*, Wydanie III zmienione, PWE, Warszawa 2011.

[359] A. Da Veiga, J.H.P. Eloff, *A framework and assessment instrument for information security culture*, Computers & Security, Vol. 29, No. 2010, s. 196–207.

wpływu na zachowania pracowników związane z bezpieczeństwem w celu zachowania bezpieczeństwa informacji"[360]. J.F. Van Niekerk, R. von Solms uważają, że kulturę bezpieczeństwa informacji można opisać za pomocą czterech poziomów związanych z bezpieczeństwem informacji, a mianowicie: artefaktów, wyznawanych wartości, wspólnych milczących założeń i wiedzy [15]. Przytoczone próby zdefiniowania pojęcia kultury bezpieczeństwa informacji świadczą o bliskości z pojęciem kultury organizacyjnej.

Przeprowadzony przegląd literatury miał pewne ograniczenia, wynikające z metody[361]. Były to m.in. ograniczenia w dostępie w bazach literaturowych do pełnych tekstów artykułów oraz możliwość niewłaściwego doboru słów kluczowych. Rezultatami przeprowadzonego przeglądu literatury są przedstawienie stanu wiedzy w badanym obszarze, zaprezentowanie kierunków prowadzonych badań oraz zidentyfikowanie luki badawczej. Przegląd wykazał, że w literaturze polskiej został w sposób niedostateczny przeanalizowany problem związku pomiędzy cechami kultury organizacyjnej a dojrzałością systemów zarządzania bezpieczeństwem informacji. O tej luce badawczej świadczy brak wśród wyszukanych pozycji artykułów w języku polskim oraz to, że wśród nich znalazł się tylko jeden artykuł badający wpływ kultury organizacyjnej na zarządzanie bezpieczeństwem informacji w polskiej organizacji [34]. W literaturze światowej podnoszony był aspekt wpływu kultury narodowej na kulturę organizacyjną, a wśród badaczy i praktyków istnieje opinia, że czynniki kulturowe, behawioralne, a nie tylko techniczne, mają wpływ na zarządzanie bezpieczeństwem informacji w organizacji [8, 9, 16]. W analizowanej literaturze nie występują badania w organizacjach typu sądy, w których to znajdują się różne subkultury [7, 14], m.in. subkultura grupy zawodowej sędziów i asesorów[362]. Sędziowie i asesorowie mają specyficzne uprawnienia i odgrywają szczególną rolę w organizacji, jaką jest sąd, co wynika z krajowych przepisów prawnych. W sprawowaniu swojego urzędu są niezawiśli i podlegają tylko Konstytucji RP oraz ustawom. Na swoje stanowiska są

[360] A. Alhogail, A. Mirza, *Information security culture: a definition and a literature review*, [w:] Proceedings of IEEE World Congress On Computer Applications and Information Systems, 2014, s. 1–7.

[361] W. Czekon, op. cit., s. 137.

[362] S. Shetreet, *Creating A Culture of Judicial Independence: The Practical Challenge and the Conceptual and Constitutional Infrastructure*, [w:] *The culture of judicial independence: Conceptual foundations and practical challenges*, S. Shetreet, C. Forsyth (red.), Martinus Nijhoff, Boston 2011, s. 15–68.

T. Halliday, *Judges under stress: Legal complexes and a sociology of hope*, 2023, http://dx.doi.org/10.2139/ssrn.4482114.

powoływani lub mianowani przez Prezydenta Polski i chroni ich immunitet[363]. W literaturze przedmiotu brak jest usystematyzowanych informacji na temat dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych w kontekście kultury organizacyjnej.

3.2. Cele i przedmiot badań

W etapie drugim przeprowadzonej pracy badawczej została zidentyfikowana luka badawcza:

1) niedostatecznie zbadany problem zależności pomiędzy cechami kultury organizacyjnej a dojrzałością systemów zarządzania bezpieczeństwem informacji w polskich organizacjach sektora publicznego,
2) brak usystematyzowanej wiedzy na temat dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych w kontekście kultury organizacyjnej

oraz określone zostały cele i przedmiot badań.

Przedmiotem badań uczyniono kulturę organizacyjną i systemy zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych. Głównym celem dysertacji było zdiagnozowanie dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych z uwzględnieniem kontekstu kultury organizacyjnej.

Celami poznawczymi przeprowadzonych badań były:

1. Identyfikacja dominujących cech kultury organizacyjnej w wojewódzkich sądach administracyjnych.
2. Rozpoznanie i analiza istniejącego stanu systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych.

Celami praktycznymi przeprowadzonych badań były:

3. Ocena dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych.
4. Wyodrębnienie cech kultury organizacyjnej mających potencjalny związek z dojrzałością systemów zarządzania bezpieczeństwem informacji.

Aby zrealizować postawione cele, sformułowano następujące szczegółowe pytania badawcze:

[363] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.); ustawa z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (t.j. Dz. U. z 2024 r., poz. 334 z późn. zm.).

(Cel badań nr 1)

P1. Jakie są w ocenie pracowników dominujące profile kultury organizacyjnej wojewódzkich sądów administracyjnych?

P2. Jakie cechy kultury organizacyjnej są identyfikowane w wojewódzkich sądach administracyjnych?

(Cel badań nr 2)

P3. Jakie działania zarządcze podejmowane są przez kierownictwo sądów w celu zapewnienia bezpieczeństwa informacji?

P4. Jakie standardy i dobre praktyki zostały wdrożone w poszczególnych sądach administracyjnych?

(Cel badań nr 3)

P5. Jaki poziom dojrzałości systemów zarządzania bezpieczeństwem informacji osiągają poszczególne wojewódzkie sądy administracyjne?

(Cel badań nr 4)

P6. Czy, a jeśli tak, to jakie cechy kultury organizacyjnej mają związek z dojrzałością systemów zarządzania bezpieczeństwem informacji?

W oparciu o przeprowadzony przegląd literatury[364] sformułowano hipotezę badawczą[365].

H: Istnieją różnice w zakresie identyfikowanej kultury organizacyjnej w sądach w zależności od grupy zawodowej.

3.3. Sądy administracyjne – zarys zasad funkcjonowania

3.3.1. Historia sądownictwa administracyjnego w Polsce oraz podstawy prawne ich działania

Zadaniem sądownictwa administracyjnego jest kontrola zgodności działań administracji publicznej z prawem. Początki historii sądownictwa administracyjnego na ziemiach polskich przypadają na koniec XVIII i początek XIX w. W roku 1807 po raz pierwszy utworzono oddzielny, nawiązujący do francuskiej koncepcji, sąd administracyjny – Radę Stanu Księstwa Warszawskiego. W latach 1815–1831 funkcjonowała Pierwsza Rada Stanu Królestwa Polskiego, natomiast w latach 1832–1841 Druga Rada Stanu Królestwa Polskiego.

[364] Kessler S. R.; Pindek S.; Kleinman, G.; Andel S. A.; Spector P. E., *Information Security Climate and the Assessment of Information Security Risk among Healthcare Employees*, „Health Informatics J" 2020, Vol. 26 (1), s. 461–473.

Da Veiga A., Martins N., *Defining and Identifying Dominant Information Security Cultures and Subcultures*, „Computers & Security" 2017, *70*, s. 72–94.

[365] A. Jeszka, *Problemy badawcze i hipotezy w naukach o zarządzaniu*, Organization and Management, Nr 5, 2013, s. 27-46.

Po odzyskaniu niepodległości w roku 1918 w ustawie z dnia 17 marca 1921 r. – Konstytucja Rzeczypospolitej Polskiej[366] znalazły się m.in. następujące zapisy: „Państwo będzie sprawowało nadzór nad działalnością samorządu przez wydziały samorządu wyższego stopnia; nadzór ten mogą jednak ustawy przekazać częściowo sądownictwu administracyjnemu (…)" (art. 70) oraz: „Do orzekania o legalności aktów administracyjnych w zakresie administracji tak rządowej, jak i samorządowej powoła osobna ustawa sądownictwo administracyjne, oparte w swej organizacji na współdziałaniu czynnika obywatelskiego i sędziowskiego z Najwyższym Trybunałem Administracyjnym" (art. 73).

Najwyższy Trybunał Administracyjny[367] został powołany do życia ustawą z dnia 3 sierpnia 1922 r. Był on pierwszym po odzyskaniu przez Polskę niepodległości, powołanym przez ustawodawcę, sądem administracyjnym o ogólnokrajowym zasięgu działania. Najwyższy Trybunał Administracyjny funkcjonował zaledwie 17 lat (1922–1939), odegrał jednak istotną rolę w kształtowaniu pozycji ustrojowej sądownictwa administracyjnego w II połowie XX w.

Po II wojnie światowej odtworzenie sądownictwa administracyjnego nastąpiło dopiero 31 stycznia 1980 r. W tym dniu Sejm uchwalił ustawę o Naczelnym Sądzie Administracyjnym i o zmianie ustawy – Kodeks postępowania administracyjnego. Nie w pełni samodzielny, bo podlegający nadzorowi judykacyjnemu Sądu Najwyższego, Naczelny Sąd Administracyjny (dalej NSA) został utworzony w dniu 1 września 1980 r. Od tego czasu model prawny sądownictwa administracyjnego ulegał kilkukrotnie zmianom. Poszerzał się obszar działań administracji publicznej poddany kontroli sądowej oraz zwiększały się i wzmacniały uprawnienia skarżącego w postępowaniu sądowoadministracyjnym. Przejście z klauzuli enumeratywnego określenia właściwości Naczelnego Sądu Administracyjnego na klauzulę generalną, nieograniczającą kontrolowanej działalności, odbyło się w roku 1990. Dwuinstancyjny model postępowania sądowoadministracyjnego został zapisany w Konstytucji z 1997 r.

Wypełnienie tego zapisu nastąpiło dopiero w 2004 r., kiedy to mocą uchwalonych, na podstawie art. 184 w zw. z art. 175 ust. 1 i art. 178 Konstytucji Rzeczypospolitej Polskiej[368], ustaw[369] zreformowano sądownictwo administracyjne,

[366] Dz. U. Nr 44, poz. 267.
[367] Dz. U. Nr 67, poz. 600.
[368] Ustawa z dnia 2 kwietnia 1997 r. Konstytucja Rzeczypospolitej Polskiej (Dz. U. Nr 78, poz. 483 ze zm., dalej: Konstytucja RP).

powołując wojewódzkie sądy administracyjne jako sądy pierwszej instancji oraz Naczelny Sąd Administracyjny, jako sąd odwoławczy, sprawujący nadzór judykacyjny i organizacyjny nad sądami pierwszej instancji.

Zgodnie z art. 184 Konstytucji: „Naczelny Sąd Administracyjny oraz inne sądy administracyjne sprawują, w zakresie określonym w ustawie, kontrolę działalności administracji publicznej. Kontrola ta obejmuje również orzekanie o zgodności z ustawami uchwał organów samorządu terytorialnego i aktów normatywnych terenowych organów administracji rządowej". Sąd administracyjny w wyniku kontroli zaskarżonego działania lub bezczynności organu wykonującego administrację publiczną stosuje środki przewidziane ustawą. Poza nielicznymi wyjątkami istotą tych środków jest zniesienie działania lub bezczynności niezgodnej z prawem, a nie merytoryczne rozstrzygnięcia. Sąd administracyjny nie przejmuje roli administracji publicznej, może zastosować sankcję nieważności lub sankcję wzruszalności, a w zakresie bezczynności nakazać podjęcie działania, bez określenia treści tego działania[370].

Zgodnie z art. 14 § 1 i 2 ustawy z dnia 25 lipca 2002 r. Prawo o ustroju sądów administracyjnych (dalej: p.u.s.a.) w projekcie dochodów i wydatków NSA zawarte są również dochody i wydatki wojewódzkich sądów administracyjnych. Minister właściwy do spraw finansów publicznych włącza projekt Prezesa Naczelnego Sądu Administracyjnego do projektu budżetu państwa. Prezes NSA posiada uprawnienia ministra właściwego do spraw finansów publicznych w zakresie wykonywania budżetu sądów administracyjnych.

Artykuł 15 § 1 p.u.s.a. zobowiązuje Prezesa NSA do informowania Prezydenta Rzeczypospolitej Polskiej i Krajowej Rady Sądownictwa o działalności sądów administracyjnych. Należy zauważyć, iż nie jest to sprawozdanie, a tylko informacja – wynika to z zasady niezawisłości władzy sądowniczej. Z kolei § 2 nakłada obowiązek informowania Prezesa Rady Ministrów o problemach funkcjonowania administracji publicznej wynikających ze spraw rozpatrywanych przez sądy administracyjne.

[369] Ustawa z dnia 25 lipca 2002 r. – Prawo o ustroju sądów administracyjnych (t.j. Dz. U. z 2022 r. poz. 2492 z późn. zm.); ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz. U. z 2023 r. poz. 1634 z późn. zm.); ustawa z dnia 30 sierpnia 2002 r. – Przepisy wprowadzające ustawę – Prawo o ustroju sądów administracyjnych i ustawę – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. Nr 153, poz. 1271 ze zm.).

[370] B. Adamiak, J. Borkowski, *Charakter kompetencji judykacyjnej sądów administracyjnych*, [w:] B. Adamiak, J. Borkowski, *Metodyka pracy sędziego w sprawach administracyjnych*, Wolters Kluwer 2020, s. 343.

Dla obszaru każdego z szesnastu województw ustalono siedziby wojewódzkich sądów administracyjnych[371]. Utworzono również Wydział Zamiejscowy w Radomiu WSA w Warszawie dla powiatów: białobrzeskiego, grójeckiego, kozienickiego, lipskiego, przysuskiego, radomskiego, szydłowieckiego, zwoleńskiego oraz miasta Radomia.

W myśl art. 15 § 1 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (dalej: p.p.s.a.) Naczelny Sąd Administracyjny: rozpoznaje środki odwoławcze od orzeczeń wojewódzkich sądów administracyjnych, tj. skargi kasacyjne i zażalenia od wyroków i postanowień; podejmuje uchwały mające na celu wyjaśnienie przepisów prawnych, których stosowanie wywołało rozbieżności w orzecznictwie sądów administracyjnych; podejmuje uchwały zawierające rozstrzygnięcie zagadnień prawnych budzących poważne wątpliwości w konkretnej sprawie sądowoadministracyjnej; rozstrzyga spory o właściwość między organami jednostek samorządu terytorialnego i między samorządowymi kolegiami odwoławczymi oraz spory kompetencyjne między organami tych jednostek a organami administracji rządowej; rozpoznaje inne sprawy należące do właściwości NSA na mocy odrębnych ustaw.

3.3.2. Struktura organizacyjna i kierownictwo wojewódzkich sądów administracyjnych

Strukturę organizacyjną WSA określają głównie dwa akty prawne: wspomniana już ustawa p.u.s.a. oraz rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 5 sierpnia 2015 r. Regulamin wewnętrznego urzędowania wojewódzkich sądów administracyjnych (t.j. Dz. U. z 2024 r. poz. 779).

Wojewódzki sąd administracyjny dzieli się na wydziały, które tworzy i znosi Prezes NSA. Wydziałem w WSA kieruje prezes lub wiceprezes sądu albo wyznaczony sędzia.

Osoby pracujące w strukturach WSA można podzielić na dwie podstawowe grupy. Pierwszą z nich jest skład orzeczniczy WSA, do którego wchodzą: prezes sądu, wiceprezesi sądu, sędziowie i asesorzy sądowi. Liczbę sędziów, wiceprezesów sądu

[371] Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 25 kwietnia 2003 r. w sprawie utworzenia wojewódzkich sądów administracyjnych oraz ustalenia ich siedzib i obszarów właściwości (Dz. U. Nr 72, poz. 652 z późn. zm.), Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 16 grudnia 2005 r. w sprawie utworzenia Wydziału Zamiejscowego w Radomiu Wojewódzkiego Sądu Administracyjnego w Warszawie (Dz. U. Nr 256, poz. 2144 z późn. zm.).

i asesorów sądowych określa Prezes NSA, a powołuje na stanowisko Prezydent Rzeczypospolitej Polskiej, na wniosek Krajowej Rady Sądownictwa. Należy podkreślić, iż: „Sędziowie sądów administracyjnych i asesorzy sądowi w sprawowaniu swojego urzędu są niezawiśli i podlegają tylko Konstytucji oraz ustawom" (art. 4 p.u.s.a). Sprawy dyscyplinarnych sędziów sądów administracyjnych i asesorów sądowych rozstrzygane są przed sądem dyscyplinarnym, którym jest NSA (art. 41 p.u.s.a.).

Drugą grupę osób pracujących w WSA stanowią: starsi referendarze sądowi, referendarze sądowi, starsi asystenci sędziów, asystenci sędziów oraz urzędnicy i inni pracownicy sądowi. W stosunku do tej grupy Prezes WSA wykonuje czynności z zakresu prawa pracy, a wymagane kwalifikacje dla poszczególnych stanowisk opisane są w rozporządzeniu Prezydenta Rzeczypospolitej Polskiej z dnia 22 marca 2011 r. w sprawie stanowisk i wymaganych kwalifikacji urzędników sądowych i innych pracowników oraz szczegółowych zasad wynagradzania referendarzy sądowych, starszych referendarzy sądowych, asystentów sędziów, starszych asystentów sędziów, urzędników oraz innych pracowników wojewódzkich sądów administracyjnych (t.j. Dz. U. z 2024 r. poz. 822).

Organami wojewódzkiego sądu administracyjnego są: prezes sądu, zgromadzenie ogólne sędziów wojewódzkiego sądu administracyjnego, zwane dalej „zgromadzeniem ogólnym" oraz kolegium wojewódzkiego sądu administracyjnego, zwane dalej „kolegium sądu" (art. 19 p.u.s.a)

Prezes WSA kieruje sądem i reprezentuje go na zewnątrz, pełni czynności administracji sądowej i inne czynności przewidziane w ustawie, jest organem podległym Prezesowi NSA, przez którego jest powoływany na 5-letnią kadencję, może być również przez niego odwołany.

Zwierzchni nadzór nad działalnością administracyjną sądów administracyjnych sprawuje Prezes Naczelnego Sądu Administracyjnego, który też ustala zasady biurowości w tychże sądach.

Wojewódzki sąd administracyjny dzieli się na[372]:

- Wydziały orzecznicze

  Przewodniczący wydziałów orzeczniczych kierują wydziałami, mogą pełnić funkcję wiceprezesów WSA. Wydziały orzecznicze odpowiedzialne są za realizację głównego celu WSA, jakim jest sprawowanie kontroli zgodności

[372] Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 5 sierpnia 2015 r. Regulamin wewnętrznego urzędowania wojewódzkich sądów administracyjnych (t.j. Dz. U. z 2024 r. poz. 779).

działań z prawem administracji publicznej. Liczba wydziałów orzeczniczych zależy od wpływu określonego rodzaju spraw oraz liczby sędziów. W strukturach wydziałów istnieją sekretariaty, na czele których stoją kierownicy.

- Wydział informacji sądowej (dalej WIS)
- Przewodniczący WIS jest rzecznikiem prasowym sądu. W ramach wydziału utworzony jest sekretariat informacji o sprawach, który udziela informacji o stanie spraw załatwianych w sądzie i udostępnia do wglądu akt spraw. Do zadań WIS należy również udostępnianie informacji publicznej o działalności sądu, prowadzenie sprawozdawczości statystycznej sądu oraz biblioteki sądowej. W jego strukturach wykonuje swoje zadania administrator systemu informatycznego.
- Oddział spraw ogólnych i osobowych (dalej OSOiO)
- Oddział ten zajmuje się m.in.: sprawami kadrowymi; osobowymi i socjalnymi sędziów i innych pracowników sądu; szkoleniami; sprawami organizacyjnymi; prowadzeniem biura podawczego i archiwum zakładowego; prowadzeniem sekretariatów prezesa i wiceprezesa sądu.
- Oddział administracyjno-gospodarczy (dalej OAG)

  Do głównych zadań tego oddziału należy: zarządzanie budynkiem sądowym i innymi składnikami majątku sądowego, prowadzenie remontów i inwestycji, zakup urządzeń i materiałów biurowych. Powyższe czynności muszą być przeprowadzane zgodnie z przepisami obowiązującymi dla jednostek sektora finansów publicznych, w tym z ustawą z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2023 r. poz. 1605 z późn. zm.). Oddział realizuje również zadania w zakresie ochrony pracowników i pomieszczeń sądowych.
- Oddział finansowo-budżetowy (dalej OFB)
- Kierownik OFB jest głównym księgowym sądu. Podstawowymi zadaniami oddziału są: projektowanie dochodów i wydatków budżetowych sądu, wykonywanie dyspozycji środkami pieniężnymi oraz prowadzenie rachunkowości.

Zwierzchnikiem kierowników oddziałów sądu jest dyrektor WSA, którego powołuje Prezes NSA na wniosek prezesa WSA.

Na podstawie art. 20 ust. 1 p.u.s.a. oraz na podstawie art. 53 ust. 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2023 r. poz. 1270 z późn. zm.) dyrektor WSA może zostać upoważniony przez prezesa WSA do: załatwiania spraw finansowych i gospodarczych, wykonywania czynności kierownika zamawiającego w zakresie określonym w przepisach o zamówieniach publicznych, reprezentowania Sądu przed sądami, organami administracji publicznej i innymi podmiotami w sprawach wymienionych powyżej.

Bezpośrednio pod prezesa WSA podlegają: pełnomocnik do spraw ochrony informacji niejawnych[373]; audytor wewnętrzny, powoływany na zasadach określonych w przepisach o finansach publicznych[374]; inspektorzy ds. BHP[375] i obrony cywilnej oraz inspektor ochrony danych[376].

Rysunek 3.3 przedstawia strukturę organizacyjną Wojewódzkiego Sądu Administracyjnego w Łodzi. Podobne zależności występują w pozostałych sądach administracyjnych, różnice spowodowane są liczbą osób zatrudnionych do obsługi sędziów i asesorów orzekających w danej placówce. Jest to struktura stosunkowo płaska z dosyć szeroką rozpiętością zarządzania[377]. Prezesowi podlegają bezpośrednio przełożeni pięciu jednostek organizacyjnych i osoby pracujące na stanowiskach samodzielnych. Jak już nadmieniono, do części czynności związanych z zarządzaniem prezes WSA może upoważnić dyrektora sądu, zatem istnieje w praktyce podział odpowiedzialności za zapewnienie sprawnego i skutecznego osiągnięcia celów strategicznych. Prezes wraz z wiceprezesami oraz dyrektor sądu są kierownikami najwyższego szczebla. Istnieje jednakże podział na obszary zarządzania: dyrektor sądu odpowiada za sprawy finansowe i gospodarcze, prezes sądu – za orzeczniczą działalność sądu oraz politykę kadrową. Zależności organizacyjne, występujące w wojewódzkich sądach administracyjnych, można zaliczyć do struktur liniowo-sztabowych.

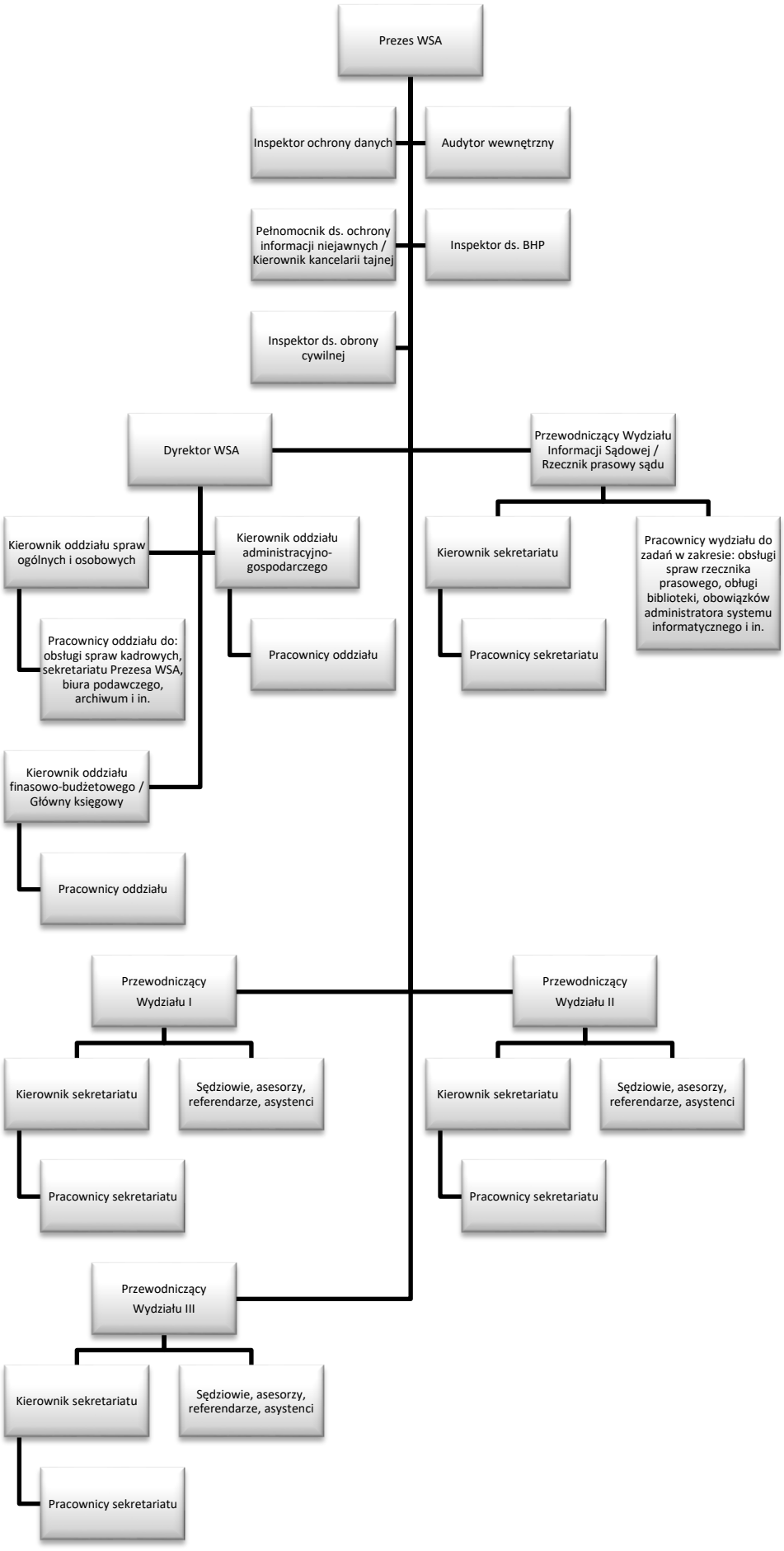
[373] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2024 r. poz. 632).

[374] Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2023 r. poz. 1270 z późn. zm.).

[375] Rozporządzenie Rady Ministrów z dnia 2 września 1997 r. w sprawie służby bezpieczeństwa i higieny pracy (Dz. U. Nr 109, poz. 704 z późn. zm.).

[376] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).

[377] R.W. Griffin, *Podstawy zarządzania organizacjami*, Wydawnictwo Naukowe PWN, Warszawa 2017.



Rysunek 3.3. Struktura organizacyjna Wojewódzkiego Sądu Administracyjnego w Łodzi
Źródło: opracowanie własne.

3.3.3. Regulacje dotyczące Systemów Zarządzania Bezpieczeństwem Informacji w Wojewódzkim Sądzie Administracyjnym

Sądy administracyjne należą do sektora finansów publicznych w myśl art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2023 r. poz. 1270 z późn. zm.), zwanym często sektorem publicznym. Do tego artykułu często odwołują się inne ustawy, określając podmioty, do których odnoszą się poszczególne przepisy.

Poniżej wymienione są przepisy dotyczące systemów zarządzania bezpieczeństwem informacji obowiązujące sądy administracyjne:

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 307), między innymi nakładająca obowiązek prowadzenie Biuletynu Informacji Publicznej (BIP) oraz udostępnienia elektronicznej skrzynki podawczej (ESP), spełniającej standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji.
2. Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2024 r., poz. 773). Między innymi w § 19 zawarty jest obowiązek opracowania systemu zarządzania bezpieczeństwem informacji na podstawie norm:
   - PN-ISO/IEC 27001 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania;
   - PN-ISO/IEC 27002 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczenie informacji;
   - PN-ISO/IEC 27005 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji[378].

[378] Norma PN-ISO/IEC 27005 występuje w Rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2024 r., poz. 773) pomimo, iż PN-ISO/IEC 27005:2014-01 została wycofana z dniem 12 października 2021 r. (https://sklep.pkn.pl/pn-iso-iec-27005-2014-01p.html). Według PKN zbiór norm wycofanych nie jest zbiorem norm, których stosowanie jest zakazane

Wymienione w rozporządzeniu normy dotyczące bezpieczeństwa informacji zostały opracowane przez podkomitet ISO/IEC JTC 1/SC 27 i wprowadzone do zbioru Polskich Normy (skrót: PN) przez Komitet Techniczny nr 182 ds. Ochrony Informacji w Systemach Teleinformatycznych. Komitet jest organem technicznym działającym przy Polskim Komitecie Normalizacyjnym (PKN), zajmującym się m.in. współpracą z ISO w zakresie prac prowadzonych w ISO/IEC JTC 1/SC 27. Opiniuje on opracowane międzynarodowe normy oraz nadzoruje proces tłumaczenia na język polski.

3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L. z 2016 r. Nr 119, s. 1 z późn. zm.) – dalej: RODO.

   Rozporządzenie to ma zastosowanie do przetwarzania danych osobowych przez sądy administracyjne, z tym zastrzeżeniem, iż w zakresie, w którym sądy te sprawują wymiar sprawiedliwości, niektóre regulacje RODO zostały wyłączone, zaś w ich miejsce obowiązują procedury wynikające z ustawy – Prawo o postępowaniu przed sądami administracyjnymi (ponieważ przetwarzanie to odbywa się celu realizacji obowiązków prawnych, dostęp do danych może mieć miejsce wyłącznie na zasadach określonych przywołaną ustawą, zaś usuwanie danych z akt jest niedopuszczalne; przepisy określają terminy przechowywania akt sądowych i urządzeń ewidencyjnych; dostęp do wymienionych powyżej systemów informatycznych mają zaś wyłącznie upoważnione osoby). W pozostałych obszarach działania sądów administracyjnych przepisy RODO obowiązują w pełnym zakresie. Przetwarzanie danych osobowych przez sądy administracyjne w ramach sprawowania przez nie wymiaru sprawiedliwości nie podlega nadzorowi sprawowanemu przez Urząd Ochrony Danych Osobowych (art. 55 ust. 3 RODO). Nadzór ten został powierzony na podstawie przepisów prawa krajowego wyznaczonym organom wymiaru sprawiedliwości, w przypadku wojewódzkich sądów administracyjnych organem nadzorczym jest Prezes

(https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-stosowania-pn-wycofanych).

Naczelnego Sądu Administracyjnego, natomiast dla Naczelnego Sądu Administracyjnego organem nadzorczym jest Krajowa Rada Sądownictwa[379].

4. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).
5. Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M. P. z 2019 r. poz. 666).
6. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)
7. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r., poz. 913 z późn. zm.), której zapisy są zgodne z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L. z 2016 r. Nr 194, s. 1). Ustawa określa cele i podmioty objęte krajowym systemem cyberbezpieczeństwa. Podaje między innymi obowiązki podmiotów publicznych w zakresie zgłaszania i obsługi incydentów. Właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego dla sądów administracyjnych jest CSIRT GOV (Computer Security Incident Response Team Goverment).
8. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r., poz. 632), która określa zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej. W ustawie sklasyfikowano informacje niejawne oraz przedstawiono sposób organizowania ochrony i przetwarzania tychże informacji.

Wymienione powyżej przepisy oraz przepisy prawne dotyczące organizacji sądów administracyjnych oraz postępowania przed sądami administracyjnymi[380] mocno

[379] Art.12b ustawy z dnia 25 lipca 2002 r. Prawo o ustroju sądów administracyjnych (t.j. Dz. U. z 2022 r. poz. 2492 z późn. zm.).

determinują sposób zarządzania bezpieczeństwem informacji w tych organizacjach. Swoboda decyzyjna osób zarządzających bezpieczeństwem informacji jest bardziej ograniczona niż w świecie biznesu, na który to również w ostatnich latach nałożono obwarowania prawne, dbając przede wszystkim o zachowanie bezpieczeństwa danych osób pracujących, współpracujących oraz klientów firm.

Za ochronę informacji przetwarzanych w sądach administracyjnych odpowiedzialne są władze sądów, w szczególności prezesi[381] i dyrektorzy[382]. Wdrożeniem i utrzymaniem polityk i procedur związanych z bezpieczeństwem przetwarzania informacji oraz kontrolowaniem zgodności wewnętrznych regulacji z obowiązującymi przepisami w sądach administracyjnych zajmują się osoby pełniące funkcje Inspektora Ochrony Danych (dalej: IOD) oraz Administratora Systemu Informatycznego (dalej: ASI). Szczegółowe obowiązki osób pełniących ww. funkcje oraz pozostałych pracowników sądów zapisane są w wewnętrznych zarządzeniach wydawanych przez prezesów WSA. Procesy związane z ochroną informacji przetwarzanych w wojewódzkich sądach administracyjnych realizowane są we wszystkich komórkach organizacyjnych WSA.

3.4. Metody badawcze

3.4.1. Triangulacja metod, metody mieszane

Jako pierwszy[383] metody triangulacji opisał Norman K. Denzin. Zdefiniował on triangulację jako: „połączenie metod w badaniu tego samego zjawiska”[384]. Denzin wyróżnił następujące cztery typy triangulacji: triangulację danych (wykorzystanie w badaniu różnych źródeł), triangulację badaczy (prace prowadzone przez różnych badaczy), triangulację teorii (wykorzystanie wielu perspektyw i teorii do interpretacji wyników badania) oraz triangulację metod (wykorzystanie wielu metod do badania problemu badawczego). Ta ostatnia została zastosowana w dysertacji. Wyróżnikiem

[380] Art. 10 i art. 121 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz. U. z 2022 r., poz. 329 z późn. zm.).

[381] § 19 rozporządzenia Prezydenta Rzeczypospolitej Polskiej z dnia 5 sierpnia 2015 r. Regulamin wewnętrznego urzędowania wojewódzkich sądów administracyjnych (Dz. U. poz. 1177); art. 7. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922 z późn. zm.).

[382] § 10 pkt 2 rozporządzenia Prezydenta Rzeczypospolitej Polskiej z dnia 5 sierpnia 2015 r. Regulamin wewnętrznego urzędowania wojewódzkich sądów administracyjnych (Dz. U. poz. 1177).

[383] R.B. Johnson, A.J. Onwuegbuzie, L.A. Turner, *Toward a Definition of Mixed Methods Research*, „Journal of Mixed Methods Research” 2007, 1(2), s. 112–133.

[384] N.K. Denzin, *The research act: A theoretical introduction to sociological methods*, Praeger, New York 1978, s. 291.

triangulacji metod jest to, że mieszanie danych uzyskanych z wykorzystaniem równych metod badawczych następuje w momencie ich interpretacji[385].

Wychodząc z założeń przedstawionych w pracy Ł. Sułkowskiego[386], dotyczących wyboru paradygmatu badań i jego powiązań z problematyką i zastosowaną metodą badań oraz orientacją aksjologiczną, badania prowadzono w dwóch paradygmatach: funkcjonalno-systemowym oraz interpretatywnym. Pierwszy wymieniony jest paradygmatem dominującym, badany jest wpływ kultury organizacyjnej na dojrzałość zarządzania bezpieczeństwem informacji. Jest to badanie ilościowe zarówno w kontekście badania kultury organizacyjnej, gdzie zostało zastosowane narzędzie kwestionariusz OCAI, badający typ kultury organizacyjnej, jak i w kontekście badania dojrzałości zarządzania bezpieczeństwem informacji, gdzie przeprowadzona została analiza formalna[387] dokumentów ustanawiających i utrzymujących system zarządzania bezpieczeństwem informacji w badanych organizacjach.

Badania ilościowe kultury organizacyjnej wiążą się z funkcjonalistycznym podejściem i przekonaniem, że można kulturę obiektywnie obserwować, mierzyć i porównywać. Umożliwiają przewidywanie oraz wnioskowanie przyczynowo-skutkowe, a ich wyniki mogą być uogólniane. Do ich ograniczeń należą: koncentrowanie się na weryfikacji sformułowanych wcześniej hipotez, bez wnikliwych poszukiwań; nieujmowanie kontekstu badanego zjawiska oraz problemy związane z budową rzetelnych narzędzi badawczych[388] i wiarygodnością udzielanych przez badanych odpowiedzi. Metody ilościowe charakteryzują się tłumaczeniem zjawisk na język statystyki, biorąc pod uwagę tylko to, co typowe. Bywa, że odrzucane są dane ekstremalne i odmienne, aby obliczane miary statystyczne (np. średnia, odchylenie standardowe) nie ulegały zniekształceniu. Co więcej, podejście ilościowe opiera się na procedurach wnioskowania dedukcyjnego, w których formułuje się hipotezy przed rozpoczęciem badań, przy czym nie zawsze zjawisko jest na tyle znane, by móc sformułować poprawne hipotezy[389]. W dysertacji podjęta została próba weryfikacji

[385] M. Matejun, *Metody, techniki i narzędzia gromadzenia danych w badaniach mieszanych*, [w:] *Metody badań mieszanych w naukach o zarządzaniu*, (red.) Ł. Sułkowski, R. Lenart-Gansiniec, Wydawnictwo Naukowe Akademii WSB, Dąbrowa Górnicza 2023, s. 84.

[386] Ł. Sułkowski, *Paradygmaty*…, op. cit., s. 17–26.

[387] A. Austen, M. Kulikowska-Pawlak, *Analiza i interpretacja danych empirycznych w badaniach mieszanych*, [w:] *Metody badań mieszanych w naukach o zarządzaniu*, (red.) Ł. Sułkowski, R. Lenart-Gansiniec, Wydawnictwo Naukowe Akademii WSB, Dąbrowa Górnicza 2023.

[388] K. Januszkiewicz, *Od teorii naukowych do badania empirycznego — budowa narzędzi do badania zachowań ludzi w organizacji*, „Przegląd Organizacji" 2016, Nr 12 (923), s. 37–42.

[389] M. Kostera, P. Krzyworzeka, M. Połeć, op. cit., s. 29–30.

postawionych hipotez w celu dotarcia do obiektywnego poznania relacji pomiędzy kulturą organizacyjną a dojrzałością zarządzania bezpieczeństwem informacji.

Dopełnieniem badania w paradygmacie dominującym było badanie w nurcie interpretatywnym, w którym to podjęta była próba poznania zachowań i kultury organizacyjnej w trakcie rozmów z kierownictwem sądów[390]. Do tego typu badań zachęca w swojej pracy, krytykującej badania kultury organizacyjnej w paradygmacie funkcjonalistycznym[391], Ł. Sułkowski. Proponuje on w badaniu procesów kulturowych w zarządzaniu poszukiwania nowych inspiracji w rzadziej stosowanych nurtach, m.in. takich jak paradygmat interpretatywny, z zamiarem lepszego zrozumienia kultury organizacyjnej. W tym właśnie celu w wojewódzkich sądach administracyjnych zastosowano jako metodę badawczą wywiad, czyli kierowaną rozmowę, „gdzie kierowanie jest uznane i zaakceptowane przez obie strony"[392]. W literaturze wyróżniane są wywiady standaryzowane lub niestandaryzowane, strukturalizowane lub nieustrukturalizowane. Typową techniką dla badań etnograficznych jest wywiad niestandaryzowany nieustrukturalizowany, akceptowalny jest również, wykorzystany w tej dysertacji, wywiad standaryzowany nieustrukturalizowany[393]. W podejściu jakościowym służy on do zdobycia wiedzy w zakresie tego, jak osoby w terenie definiują pojęcia, których dotyczy badanie. Charakteryzuje się ustaloną listę pytań i kolejnością ich zadawania (standaryzacja), ale brzmienie pytań nie narzuca z góry żadnej kategoryzacji, która miałaby ograniczyć pole badań[394]. Brak ustrukturalizowania daje możliwość zrozumienia złożonych zachowań członków organizacji. Badacz stopniowo pogłębia swoją wiedzę na temat analizowanych zjawisk i na podstawie zebranych danych dokonuje systematycznych podsumowań w poszukiwaniu istniejących prawidłowości. Ten „oddolny" proces pogłębiania wiedzy pozwala na sformułowanie hipotez roboczych, które następnie podlegają weryfikacji poprzez dalsze badania, co pozwala na „ugruntowanie" wniosków i stworzenie propozycji teoretycznych, które są bezpośrednim wynikiem danych empirycznych. Ograniczeniem

[390] J.F. Molina-Azorín, M.D. López-Gamero, op. cit., s. 134–148; J.W. Creswell, A. Tashakkori, op. cit., s. 303–308; Ł. Sułkowski, R. Lenart-Gansiniec, *Metody*…, op. cit., s. 13.

[391] Ł. Sułkowski, *Funkcjonalistyczna wizja kultury organizacyjnej w zarządzaniu – dominujący paradygmat i jego krytyka / Functionalist vision in managing organizational culture – the dominant paradigm and its critics*, „Problemy Zarzadzania" 2013, 11, s. 20–33.

[392] B. Czarniawska, *Interviewes and organizational narratives* [w:] *Handbook of interviewing*, (red.) J.F. Gubrium, J. Holstein, Sage, Thousand Oaks 2002, s. 733–750.

[393] M. Kostera, P. Krzyworzeka, M. Połeć, op. cit., s. 144–145.

[394] A. Fontana, J.H. Frey, *Interviewing: The art of science*, [w:] *Collecting and interpretative qualitative materials*, (red.) B.K. Denzin, Y.S. Lincoln, Sage, London 1994, s. 47–78.

etnografii jest brak możliwości uogólniania wniosków w generalne teorie, zwłaszcza dotyczące całych populacji: „Za jej pomocą buduje się teorie mające charakter wzorców i teorie lokalne, które następnie można akumulować i porównywać między sobą”[395].

Tekst transkrypcji wywiadów został poddany analizie – zarówno ilościowej, jak i jakościowej. Technika badawcza analizy jakościowej treści pozwala na jakościową ocenę tekstu oraz umożliwia kategoryzację określonych treści, ocenę ich jakości i wpływu na rozpatrywany problem badawczy[396].

3.4.2. Plan badań

Aby uniknąć luk w przeprowadzanych badaniach, zastosowane zostały w pracy metody i techniki badawcze zarówno wykorzystywane w badaniach o charakterze jakościowym, jak ilościowym. Zastosowanie triangulacji metod wzbogaciło rozumienie zachodzących procesów w badanych organizacjach. Tabela 3.4 przedstawia zestawienie informacji dotyczące poszczególnych badań. Przeprowadzone badania empiryczne były trzecim etapem postępowania badawczego (Rysunek 0.1).

Tabela 3.4. Plan badań empirycznych

Badanie nr 1: indywidualne standaryzowane nieustrukturalizowane wywiady z dyrektorami wojewódzkich sądów administracyjnych	**– Badana grupa:** dyrektorzy wojewódzkich sądów administracyjnych lub osoby wytypowane przez dyrektorów do udzielenia wywiadów w ich imieniu **– Dobór próby:** badanie pełne **– Narzędzie badawcze:** kwestionariusz wywiadu (Załącznik nr 1) **– Sposób prowadzenia badania:** wywiad przeprowadzony osobiście, bezpośrednio lub z wykorzystaniem usługi internetowej umożliwiającej połączenia audio i wideo	P2. Jakie cechy kultury organizacyjnej są identyfikowane w wojewódzkich sądach administracyjnych? P3. Jakie działania zarządcze podejmowane są przez kierownictwo sądów w celu zapewnienia bezpieczeństwa informacji? P4. Jakie standardy i dobre praktyki zostały wdrożone w poszczególnych sądach administracyjnych? P5. Jaki poziom dojrzałości systemów zarządzania bezpieczeństwem informacji osiągają poszczególne wojewódzkie sądy

[395] M. Kostera, P. Krzyworzeka, M. Połeć, op. cit., s. 29–30.
[396] A. Austen, M. Kulikowska-Pawlak, op. cit.

		administracyjne? P6. Jakie cechy kultury organizacyjnej mają związek z dojrzałością systemów zarządzania bezpieczeństwem informacji?
Badanie nr 2: badanie dokumentów dotyczących SZBI wojewódzkich sądów administracyjnych	**– Dobór próby:** badanie pełne **– Narzędzie badawcze:** lista kontrolna do analizy formalnej dokumentów dotyczących SZBI (Załącznik nr 2) **– Sposób prowadzenia badania:** badanie przeprowadzone osobiście, w obecności pracownika WSA	P2. Jakie cechy kultury organizacyjnej są identyfikowane w wojewódzkich sądach administracyjnych? P3. Jakie działania zarządcze podejmowane są przez kierownictwo sądów w celu zapewnienia bezpieczeństwa informacji? P4. Jakie standardy i dobre praktyki zostały wdrożone w poszczególnych sądach administracyjnych? P5. Jaki poziom dojrzałości systemów zarządzania bezpieczeństwem informacji osiągają poszczególne wojewódzkie sądy administracyjne?
Badanie nr 3: ankieta wśród osób pracujących w wojewódzkich sądach administracyjnych	**– Badana grupa:** osoby pracujące w wojewódzkich sądach administracyjnych (n = 156) **– Dobór próby:** celowy **– Narzędzie badawcze:** kwestionariusz ankiety (Załącznik nr 3) **– Sposób prowadzenia badania:** CAWI	P1. Jakie są w ocenie pracowników dominujące profile kultury organizacyjnej wojewódzkich sądów administracyjnych? P2. Jakie cechy kultury organizacyjnej są identyfikowane w wojewódzkich sądach administracyjnych? P5. Jaki poziom dojrzałości systemów zarządzania bezpieczeństwem informacji osiągają poszczególne wojewódzkie sądy administracyjne? H: Istnieją różnice w zakresie

		identyfikowanej kultury organizacyjnej w sądach w zależności od grupy zawodowej.

W postawionej w dysertacji hipotezie używane jest pojęcie: grupy zawodowe, są to rodzaje subkultur występujących w wojewódzkich sądach administracyjnych.

3.5. Próba badawcza

3.5.1. Próba badawcza – wywiad

Po uzyskaniu zgody od prezesa Naczelnego Sądu Administracyjnego oraz zgód szesnastu prezesów wojewódzkich sądów administracyjnych, do badania zostali zaproszeni dyrektorzy tych sądów. W rozważaniach na temat zarządzania bezpieczeństwem informacji za najwyższe kierownictwo[397] uważa się prezesa wraz z wiceprezesami oraz dyrektora sądu. Umiejscowienie stanowiska dyrektora w strukturze organizacyjnej wojewódzkich sądów administracyjnych zostało przedstawione w podrozdziale 3.3.2. Badanie spełniało kryteria badania pełnego, gdyż obejmowało pełną próbę zbiorowości statystycznej[398].

3.5.2. Próba badawcza – badanie dokumentów

W szesnastu wojewódzkich sądach administracyjnych zostały poddane analizie dokumenty stanowiące wewnętrzne regulacje dotyczące systemów zarządzania bezpieczeństwem informacji. Było to badanie pełne, obejmowało swoim zasięgiem pełną próbę zbiorowości statystycznej[399].

3.5.3. Próba badawcza – ankieta

Badanie ankietowe było badaniem niepełnym. Próba badawcza została uzyskana bez wykorzystaniu losowego doboru próby, z użyciem kryterium wygody. Według uzyskanych informacji z Wydziału Spraw Osobowych w Kancelarii Prezesa Naczelnego Sądu Administracyjnego na dzień 31 grudnia 2022 r. we wszystkich wojewódzkich sądach administracyjnych, wraz z sędziami i asesorami, pracowało 1813

[397] PN-ISO/IEC 27000:2014-11 „2.84 Najwyższe kierownictwo – osoba lub grupa osób, która określa kierunek i steruje organizacją na najwyższym poziomie.

Uwaga 1 do zapisu: Kierownictwo ma prawo do delegowania władzy i zapewnienia zasobów w ramach organizacji.

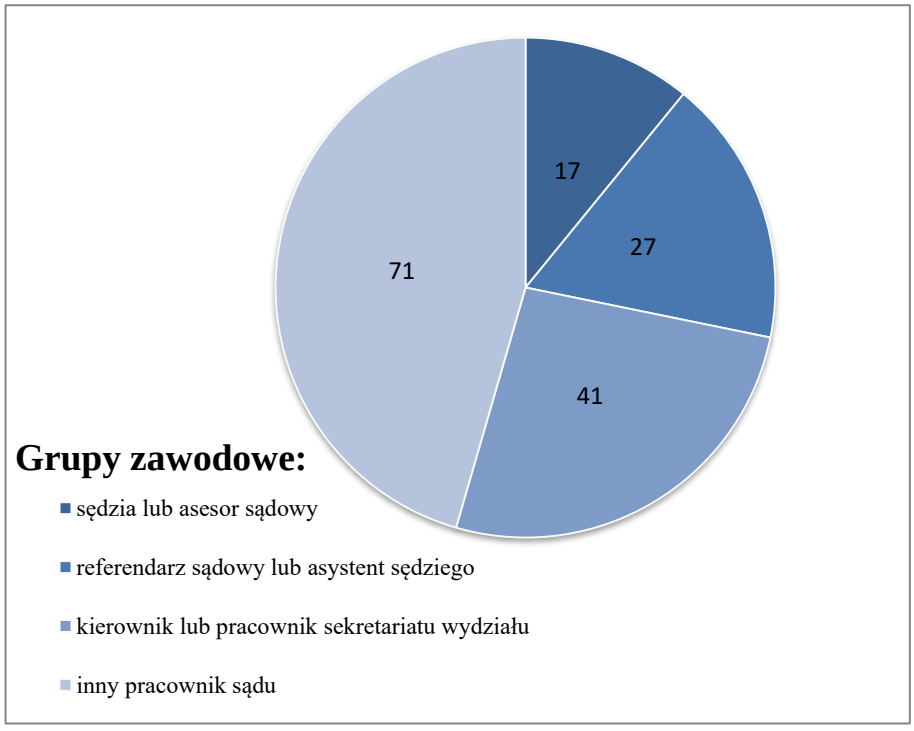
Uwaga 2 do zapisu: Jeżeli zakres systemu zarządzania obejmuje tylko część organizacji, najwyższe kierownictwo odnosi się do tych, którzy kierują i sterują tą częścią organizacji".

[398] D. Witkowska, *Wybrane metody ilościowe w finansach*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2023, s. 16.

[399] Ibidem.

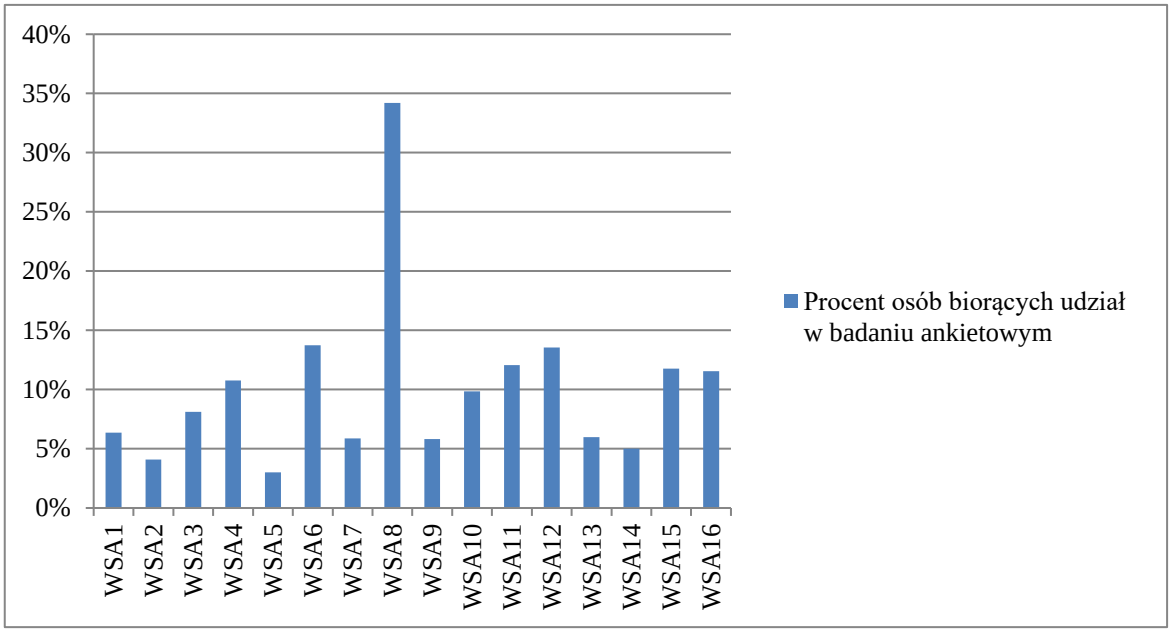
osób. Ankieta została udostępniona Przy tym stanie zatrudnienia uzyskano 156 wypełnionych kwestionariuszy. Wyniki badań ankietowych na tak dobranej próbie nie dały możliwości wnioskowania dla całej populacji, odzwierciedlały tylko stan postrzegania w badanej próbie respondentów. Rysunek 3.4 przedstawia liczbę osób z podziałem na grupy zawodowe. Biorący udział w badaniu określili swoją przynależność do jednej z grup zawodowych:

- Sędzia lub Asesor Sądowy
  (wykształcenie prawnicze, powołanie lub mianowanie na stanowisko przez Prezydent Rzeczypospolitej Polskiej)
- Referendarz Sądowy lub Asystent Sędziego
  (wykształcenie prawnicze, zatrudnienie na umowę o pracę)
- Kierownik lub Pracownik Sekretariatu Wydziału
  (brak wymogu wykształcenia prawniczego, zatrudnienie na umowę o pracę, pracownicy sekretariatów wydziałów)
- Inny Pracownik Sądu
  (brak konieczności posiadania wykształcenia prawniczego, zatrudnienie na umowę o pracę, pracownicy zatrudnieni w oddziałach sądów lub na stanowiskach samodzielnych).



Rysunek 3.4. Liczba respondentów z podziałem na grupy zawodowe
Źródło: opracowanie własne.

Powyższy podział wynika z: zakresów obowiązków, wymogu posiadania wykształcenia prawniczego, formy zatrudnienia. Podział ten opiera się na rozporządzeniu Prezydenta Rzeczypospolitej Polskiej z dnia 22 marca 2011 r. w sprawie stanowisk i wymaganych kwalifikacji urzędników sądowych i innych pracowników oraz szczegółowych zasad wynagradzania referendarzy sądowych, starszych referendarzy sądowych, asystentów sędziów, starszych asystentów sędziów, urzędników oraz innych pracowników wojewódzkich sądów administracyjnych (t.j. Dz. U. z 2024 r. poz. 822).



Rysunek 3.5.Procentowy udział osób pracujących w danym WSA w badaniu ankietowym
Źródło: opracowanie własne.

Na wykresie (Rysunek 3.5) przedstawiono dane dotyczące procentowego udziału osób pracujących w danym WSA w badaniu ankietowym.

3.6. Narzędzia badawcze

3.6.1. Opis narzędzi wykorzystanych w wywiadach

W przeprowadzonych rozmowach z dyrektorami sądów został wykorzystany kwestionariusz (arkusz) wywiadu standaryzowanego nieustrukturalizowanego (Załącznik 1. Kwestionariusz wywiadu). Wykorzystanie tego narzędzia badawczego miało przede wszystkim na celu zdobycie wiedzy o tym, jak kierownictwo sądu definiuje pojęcia, których dotyczy badanie, oraz uzyskanie odpowiedzi na pytania badawcze:

1) Jakie działania zarządcze podejmowane są przez kierownictwo sądów w celu zapewnienia bezpieczeństwa informacji?

2) Jakie cechy kultury organizacyjnej mają związek z dojrzałością systemów zarządzania bezpieczeństwem informacji?

Odpowiedzi udzielone przez dyrektorów na trzy pytania (pytania nr: 3, 5, 10 – Załącznik 1) miały wpływ na ocenę dojrzałości SZBI.

Tekst transkrypcji wywiadów został poddany analizie treści[400] z wykorzystaniem narzędzi zawartych w oprogramowaniu MAXQDA[401]. Zostało zastosowane kodowanie[402] indukcyjne. Kody zostały opracowane na podstawie wyrażeń i terminów używanych przez uczestników badania. Kodowanie wywiadów odbyło się w dwóch cyklach[403]. W pierwszym cyklu zastosowane zostały kody typu opisowego (analiza „pierwszego rzędu", tj. analiza wykorzystująca terminy i kody skoncentrowane na respondencie)[404], które zostały przypisane do fragmentów wypowiedzi dyrektorów. Kody te pomogły usystematyzować i skategoryzować uzyskane dane oraz wskazać znaczenie fragmentu danych w odniesieniu do pytań badawczych. Kody te zostały poddane drugiemu cyklowi kodowania, w którym z początkowej listy kodów zostały utworzone kody wyższego poziomu (analiza „drugiego rzędu", tj. wykorzystująca koncepcje, tematy i wymiary skupione na badaczu)[405], co pozwoliło na zintegrowanie i syntezę danych[406].

Odpowiedzi udzielone przez dyrektorów na trzy pytania (pytania nr: 3, 5, 10 – Załącznik 1) miały wpływ na ocenę dojrzałości SZBI, po uprzednim przeprowadzeniu

---

[400] A. Austen, M. Kulikowska-Pawlak, op. cit.

[401] MAXQDA oprogramowanie komputerowe wspomagające analizę danych jakościowych (ang. *Computer-Assisted Qualitative Data Analysis*, skrót: CAQDA); J. Sajdera, *Application of the "textual laboratory" tools of the MaxQda computer program in scientific research – comparative analysis of Polish and foreign research reports*, „E-mentor" 2023, Nr 1, s. 42–51.

[402] „Kodowanie to czynność polegająca na identyfikowaniu fragmentów znaczeniowych danych i etykietowaniu ich kodem, który można zdefiniować jako słowo lub krótką frazę, która symbolicznie przypisuje podsumowanie, istotność, uchwycenie esencji i/lub sugestywny atrybut części danych językowych lub wizualnych", źródło: J. Saldana, *The Coding Manual for Qualitative Researchers,* Thousand Oaks 2015, Sage Publications, s. 3.

„Kodowanie jest sposobem określenia tego, czego dotyczą analizowane dane. Polega na przypisaniu do jednego lub większej liczby akapitów określonego słowa bądź zwrotu", źródło: J. Niedbalski, *Komputerowe wspomaganie analizy danych jakościowych. Zastosowanie oprogramowania NVivo i Atlas.ti w projektach badawczych opartych na metodologii teorii ugruntowanej*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2014.

[403] M.S. Linneberg, S. Korsgaard, *Coding qualitative data: A synthesis guiding the novice*, „Qualitative Research Journal" 2019, Vol. 19, No. 3, s. 259–270.

[404] D.A. Gioia, K.G. Corley, A.L. Hamilton, *Seeking qualitative rigor in inductive research: Notes on the Gioia methodology*, Organizational Research Methods, Vol. 16(1), 2013, s. 15–31.

[405] Ibidem.

[406] J. Saldana, op. cit., s. 58.

transformacji danych jakościowych w dane ilościowe (tzw. kwantyfikowaniu danych jakościowych)[407]. Sposób przeprowadzenia oceny dojrzałości systemów zarządzania bezpieczeństwem informacji został przedstawiony w następnym podrozdziale (3.6.2), opisującym listę kontrolną do analizy formalnej dokumentów dotyczących SZBI w wojewódzkich sądach administracyjnych.

3.6.2. Lista kontrolna do analizy formalnej dokumentów oraz opis narzędzia oceniającego dojrzałość systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych

Lista kontrolna zastosowana do badania dokumentów SZBI (Załącznik 2) składała się 33 pytań, informacji o dacie przeprowadzenia badania i o siedzibie badanego sądu. Pytania – z wyjątkiem 2, 11 – zostały przygotowane na podstawie APO13 COBIT 2019[408] proponującego procesy związane z zarządzaniem bezpieczeństwem informacji wraz z kwalifikacją do odpowiedniego poziomu dojrzałości. Badanie było wykonane metodą analizy tekstu. W podejściu ilościowym[409] została przeprowadzona analiza formalna tekstu[410]. Badanie miało przede wszystkim na celu odpowiedź na pytanie badawcze: jaki poziom dojrzałości systemów zarządzania bezpieczeństwem informacji osiągają poszczególne wojewódzkie sądy administracyjne?

Ocena dojrzałości systemów zarządzania bezpieczeństwem informacji została dokonana na podstawie wyników zebranych w badaniu dokumentów oraz odpowiedzi na trzy pytania udzielone przez dyrektorów w trakcie wywiadów (Tabela 3.5). Biorąc pod uwagę po pierwsze fakt ustanowienia we wszystkich badanych sądach polityki bezpieczeństwa informacji, a po drugie – jak wynika z przeprowadzonych wywiadów z dyrektorami – prowadzenie nadzoru i wdrożenie działań zarządczych w tym zakresie, zakłada się, że wszystkie sądy osiągnęły co najmniej poziom pierwszy dojrzałości SZBI.

[407] A. Austen, M. Kulikowska-Pawlak, op. cit.

[408] COBIT® 2019 Framework: Governance and Management Objectives ISBN 978-1-60420-764-4, s. 12.

[409] K. Krippendorf, *Content analysis. An introduction to its methodology*, Wyd. II, Sage, Thousand Oaks 2004, s. 18–20.

[410] M. Matejun, op. cit., s. 84.

Tabela 3.5. Wymagania poziomów dojrzałości

Poziomy dojrzałości	Odpowiedzi brane pod uwagę	Minimalna liczba punktów
Poziom 2.	P1, P4 – P15, P17, P20, P21, W3	16 pkt
Poziom 3.	P16, P22 – P28	16 pkt + 7 pkt = 23 pkt
Poziom 4.	P18, P30 – P32	23 pkt + 4 pkt = 27 pkt
Poziom 5.	P33, W5, W10	27 pkt + 3 pkt = 30 pkt

Uwaga: wymogiem osiągnięcia poziomu wyższego było osiągnięcie poziomów niższych.
Źródło: opracowanie własne.

Odpowiedzi „tak" lub „nie" na pytania zamknięte (skrót: P) z listy kontrolnej przyjmują odpowiednio wartość liczbową 1 lub 0. W badaniu zakłada się, iż aby osiągnąć poziom 2. dojrzałości, organizacja musi zdobyć minimum 16 punktów z sumy punktów otrzymanych za odpowiedzi na pytania: P1, P4 – P15, P17, P20, P21 oraz W3 (W3 – pytanie nr 3 z kwestionariusza wywiadu), gdzie W3 przyjmuje wartość 1 lub 0 na podstawie informacji uzyskanej w trakcie wywiadu z dyrektorami na temat skuteczności informowania interesariuszy o obowiązujących przepisach dotyczących bezpieczeństwa informacji. Poziom 3. dojrzałości uzyskuje organizacja, która osiągnęła poziom 2. oraz której suma punktów za odpowiedzi na pytania: P16, P22 – P28 wynosi minimum 7 punktów. Poziom 4. dojrzałości wymaga osiągnięcia poziomu 3. dojrzałości oraz 4 punktów, będących sumą punktów za odpowiedzi na pytania P18, P30 – P32. Poziom 5. dojrzałości wymaga osiągnięcia poziomu 4. dojrzałości oraz uzyskania 3 punktów za: pozytywną odpowiedź na ostatnie 33. pytanie z listy kontrolnej, informację o zaangażowaniu w utrzymanie i optymalizację SZBI zarówno dyrektora, jak i prezesa sądu, istnieniu kultury świadomości bezpieczeństwa wśród pracowników (W5 – pytanie nr 5. W10 – pytanie nr 10 z kwestionariusza wywiadu). Na podstawie badania utworzono narzędzie do oceny dojrzałości systemów zarządzania bezpieczeństwem informacji w organizacji (Załącznik 6).

W celu sprawdzenia poprawności przeprowadzonej oceny poziomu dojrzałości SZBI został obliczony współczynnik Kurdera-Richardsona 20 (KR-20)[411], określający zgodność wewnętrzną wykorzystanego narzędzia do oceny poziomu dojrzałości SZBI. Wszystkie obliczone wartości przedstawiono w poniższym zestawieniu (Tabela 3.6).

[411] KR-20 to szczególny przypadek Alfy Cronbacha, w której pozycje są zmiennymi binarnymi (0 lub 1), źródło: https://www.ibm.com/support/pages/kuder-richardson-reliability-coefficients-kr20-and-kr21, dostęp: 11.05.2023 r.

Tabela 3.6. Analiza rzetelności narzędzia do oceny poziomu dojrzałości SZBI

Statystyki rzetelności

Alfa Cronbacha	Liczba pozycji
0,876	32

Statystyki pozycji Ogółem

	Średnia skali po usunięciu pozycji	Wariancja skali po usunięciu pozycji	Korelacja pozycji Ogółem	Alfa Cronbacha po usunięciu pozycji
P33	22,5000	24,667	0,752	0,862
W5	22,5625	26,396	0,412	0,872
W10	22,3125	25,429	0,573	0,868
P18	22,4375	25,996	0,458	0,871
P30	22,5625	25,196	0,671	0,865
P31	22,4375	26,129	0,431	0,872
P32	22,6250	25,983	0,541	0,869
P16	22,2500	25,933	0,484	0,870
P22	22,6875	26,629	0,447	0,871
P23	21,9375	27,396	0,455	0,872
P24	22,2500	25,533	0,567	0,868
P25	22,3125	25,296	0,600	0,867
P26	22,2500	24,867	0,709	0,863
P27	22,4375	26,129	0,431	0,872
P28	22,5000	25,067	0,666	0,865
P1	21,8750	28,650	0,000	0,877
P4	21,8750	28,650	0,000	0,877
P5	22,0000	27,733	0,222	0,876
P6	21,8750	28,650	0,000	0,877
P7	21,8750	28,650	0,000	0,877
P8	21,9375	27,396	0,455	0,872
P9	21,8750	28,650	0,000	0,877
P10	21,8750	28,650	0,000	0,877
P11	22,3750	26,383	0,377	0,874
P12	21,8750	28,650	0,000	0,877
P13	21,8750	28,650	0,000	0,877
P14	22,0625	27,529	0,227	0,876
P15	22,0625	26,863	0,389	0,873
P17	21,9375	27,396	0,455	0,872
P20	21,8750	28,650	0,000	0,877
P21	21,9375	27,396	0,455	0,872

W3	21,8750	28,650	0,000	0,877

2. poziom		3. poziom		4. poziom		5. poziom	
Statystyki rzetelności		**Statystyki rzetelności**		**Statystyki rzetelności**		**Statystyki rzetelności**	
KR-20	Liczba pozycji	KR-20	Liczba pozycji	KR-20	Liczba pozycji	KR-20	Liczba pozycji
0,522	17	0,809	8	0,696	4	0,774	3

Źródło: opracowanie własne.

Analiza wykazała dobrą rzetelność α = 0,876 dla wszystkich pozycji, słabą rzetelność α = 0,522 dla 2. poziomu dojrzałości, dobrą α = 0,809 dla 3. poziomu, wątpliwą α = 0,696 dla 4. poziomu i akceptowalną α = 0,774 dla 5. poziomu[412]. Na podstawie powyższych wyników narzędzie zostało uznane za rzetelne.

3.6.3. Kwestionariusz ankiety

W każdym z 16 sądów przeprowadzone zostało badanie ankietowe za pomocą kwestionariusza składającego się z dwóch części (Załącznik 3). Pierwsza część kwestionariusza ankiety badała profil kultury organizacyjnej narzędziem OCAI[413] (ang. *Organizational Culture Assessment Instrument*). OCAI mierzy sześć kluczowych wymiarów kultury organizacyjnej, które dotyczą następujących cech organizacji: przywództwa, zarządzania pracownikami, tego, co spaja organizację, strategii oraz sukcesu. Narzędzie OCAI składa się z dwóch kwestionariuszy: kwestionariusza do oceny kultury organizacji – stan obecny oraz kwestionariusza do oceny kultury organizacji – stan pożądany.

Dla każdego z sześciu wymiarów zadane zostało pytanie oraz przedstawiono cztery możliwe warianty udzielenia na nie odpowiedzi oznaczone literami: A, B, C, D. Pytania związane z wymiarami kultury organizacyjnej były następujące:

1. Jaka jest ogólna charakterystyka organizacji?
2. Jaki jest styl przywództwa w organizacji?
3. Jaki jest styl zarządzania pracownikami?
4. Co zapewnia spójność organizacji?
5. Na co kładzie się największy nacisk?

[412] D. George, P. Mallery, *IBM SPSS statistics 23 step by step: A simple guide and reference*, Routledge, New York 2016, s. 240.

[413] K.S. Cameron, R.E. Quinn, *Kultura*…, op. cit.

6. Jakie są kryteria sukcesu w organizacji?

Wypełniając kwestionariusz, respondent rozdzielał 100 punktów w zależności od tego, w jakim stopniu dana odpowiedź według niego opisywała sytuację w sądzie. Każdej odpowiedzi można było przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musiała wynosić 100 (w kwestionariuszu do oceny kultury organizacji – stan obecny). Analogiczne pytania zostały zadane respondentom na temat oczekiwanych przez nich cech kultury organizacyjnej – takich, które usprawniłyby funkcjonowanie sądu (w kwestionariuszu do oceny kultury organizacji – stan pożądany). Następnie obliczana była średnia arytmetyczna dla pytań z grupy A, B, C i D osobno dla informacji na temat stanu obecnego kultury i odrębnie dla kultury pożądanej. Na podstawie uzyskanych w ten sposób zmiennych ilościowych sporządzono interpretację graficzną wyników badania, obrazującą dominujący profil kultury w poszczególnych wymiarach, jak i dla całej organizacji zbierający wyniki sześciu wymiarów („ogółem"). Odpowiedzi oznaczone literą A powiązane były z cechami kultury typu KLAN, literą B z cechami kultury typu ADHOKRACJA, literą C z cechami kultury typu RYNEK oraz D z cechami kultury typu HIERARCHIA.

Druga część kwestionariusza zawiera 3 pytania dotyczące sposobu uzyskiwania informacji o zasadach bezpieczeństwa informacji obowiązujących w organizacji.

Pozycja 4. tej części kwestionariusza jest wskaźnikiem nazwanym w dalszych analizach „Bezpieczeństwo informacji", który składa z 3 pytań dotyczących odczuć respondentów związanych z bezpieczeństwem informacji w organizacji. Dla wskaźnika została przeprowadzona analiza rzetelności (Tabela 3.7) i wyliczono współczynnik Alfa Cronbacha, określający zgodność wewnętrzną – osiągnął on wartość $\alpha = 0{,}687$. Przyjmuje się, że wartości współczynnika wskazują na zadowalającą rzetelność, jeżeli mieszczą się w granicach między 0,7 a 0,95[414]. Julie Pallant[415] zauważa, że wartość Alfy Cronbacha jest zależna od liczby pozycji: gdy jest ich mała liczba (mniej niż 10), wartości Alfa Cronbacha mogą być niższe. Pomimo że wyliczony współczynnik α nie przekroczył progu 0,7 można uznać, że osiągnął wartość akceptowalną.

Tabela 3.7. Wynik analizy rzetelności dla wskaźnika „Bezpieczeństwo informacji"

Statystyki

[414] M. Tavakol, R. Dennick, *Making Sense of Cronbach's Alpha*, „International Journal of Medical Education" 2011, 2, s. 53–55; D. George, P. Mallery, op. cit., s. 240.

[415] J. Pallant, *SPSS Survival Manual: A step by step guide to data analysis using SPSS*, „Open University Press" Edycja 4, listopad 2010.

rzetelności

Alfa Cronbacha	Liczba pozycji
0,687	3

Statystyki pozycji Ogółem

	Średnia skali po usunięciu pozycji	Wariancja skali po usunięciu pozycji	Korelacja pozycji Ogółem	Alfa Cronbacha po usunięciu pozycji
BI_1	8,41	2,373	0,653	0,422
BI_2	8,57	2,105	0,410	0,778
BI_3	8,24	2,776	0,507	0,603

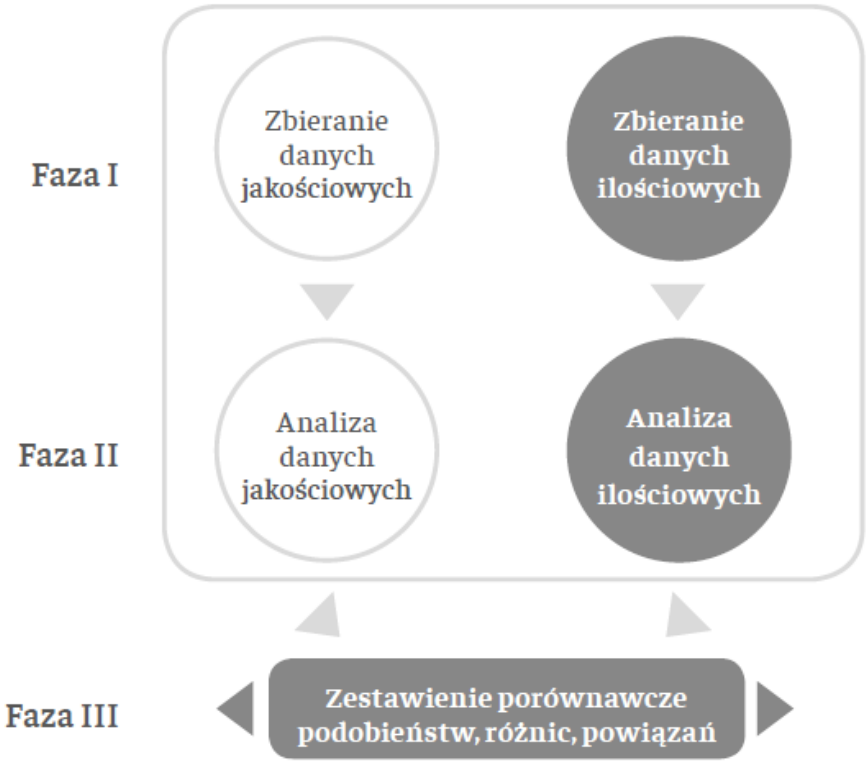
Źródło: opracowanie własne.

Zmienne w drugiej części kwestionariusza mają charakter jakościowy i są mierzone na skali nominalnej lub na skali porządkowej. Pytania metryczkowe dotyczą miejsca pracy oraz przynależności do grupy zawodowej respondenta.

3.7. Przebieg badań

W przeprowadzonym badaniu zastała przyjęta równoległa strategia triangulacyjna metod (Rysunek 3.6). Gromadzenie oraz analiza danych, zarówno jakościowych z wywiadów, jak i ilościowych z ankiet i badania dokumentów były prowadzone równolegle. Wybór strategii triangulacyjnej badań uzależniony był od dostępności respondentów. Mieszanie danych nastąpiło w momencie interpretacji, przeprowadzony został proces scalenia i integracji danych. Wiązał się on z przekształceniem danych jakościowych w ilościowe[416].

[416] Ibidem, s. 30.



Rysunek 3.6. Schemat realizacji badania – równoległa strategia triangulacyjna
Źródło: K. Kolasińska-Morawska, *Strategie badań mieszanych*, [w:] *Metody badań mieszanych w naukach o zarządzaniu*, (red.) Ł. Sułkowski, R. Lenart-Gansiniec, Wydawnictwo Naukowe Akademii WSB, Dąbrowa Górnicza 2023.

3.7.1. Przeprowadzenie wywiadów oraz analiza ich treści

Badanie zostało przeprowadzone w styczniu i lutym 2023 r. Dwa wywiady zrealizowano w trakcie osobistego spotkania z respondentem. Pozostałe czternaście wywiadów zostało przeprowadzonych przy użyciu oprogramowania WEBEX Meeting, służącego do komunikacji audiowizualnej na odległość[417]. Następnie wykonano transkrypcje wywiadów, które były wykorzystane do analizy jakościowej treści.

Kodowanie wywiadów odbyło się w dwóch cyklach z wykorzystaniem programu MAXQDA. W pierwszym cyklu zastosowane zostały kody typu opisowego uzyskane z przeglądu wyrazów i zwrotów używanych przez dyrektorów sądów w trakcie rozmowy (Rysunek 3.7).

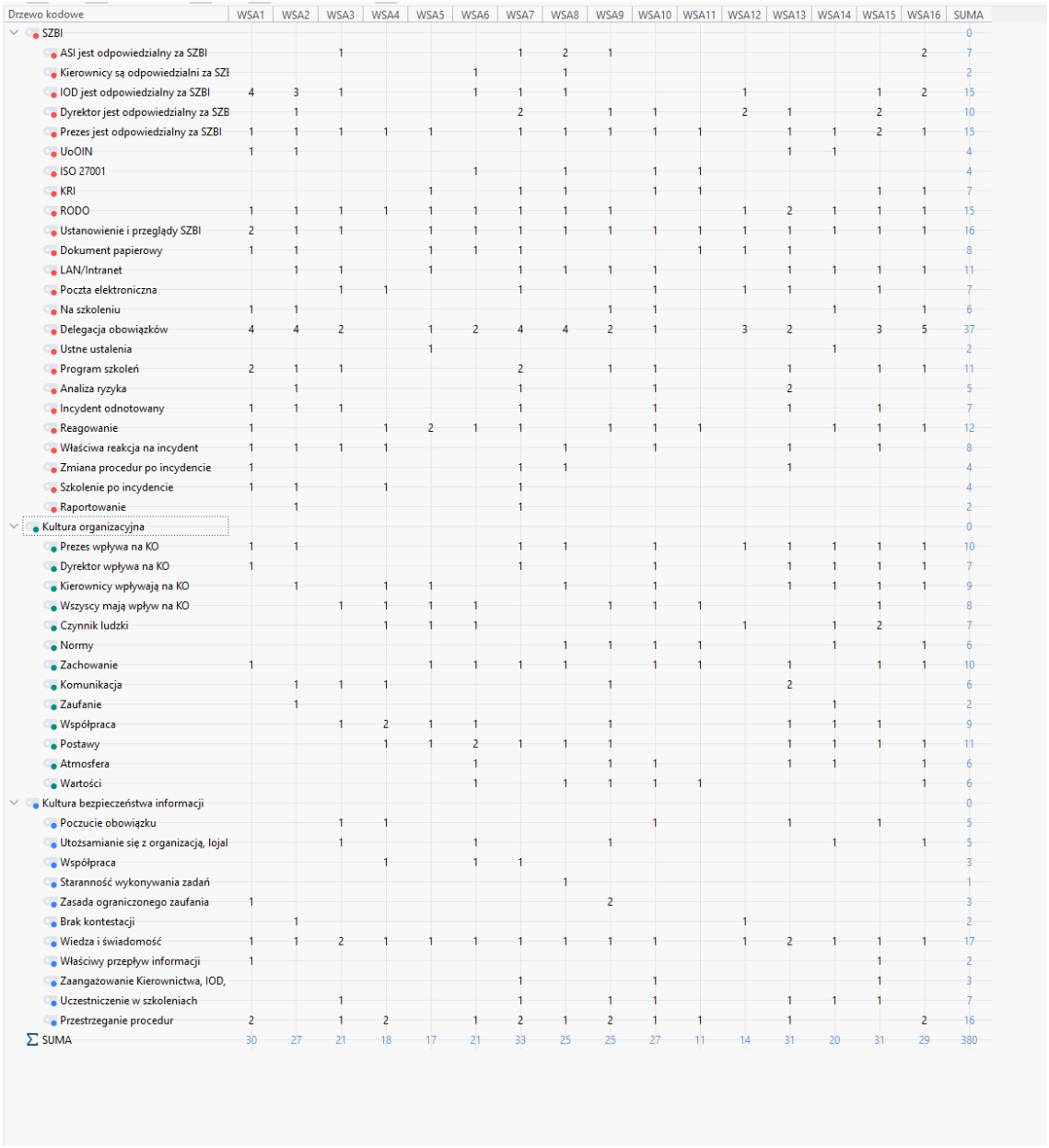
[417] P. Binder, *Wywiady online w badaniach jakościowych okresu pandemii: inkluzywny potencjał, zagrożenie wykluczeniem i jakość gromadzonych danych*, „Kultura i Edukacja" 2022, Nr 3 (137), s. 38–62.

Rysunek 3.7. Chmura słów najczęściej używanych przez respondentów
Źródło: opracowanie własne z wykorzystaniem programu MAXQDA.

Wypowiedzi zostały następnie poddane drugiemu cyklowi kodowania. Część kodów opisowych w wyniku przeprowadzonej analizy zostało wyeliminowanych, część zostało scalonych. Utworzono kody wyższego poziomu[418], integrujące kody opisowe, co pozwoliło na syntezę danych[419].

[418] D.A. Gioia, K.G. Corley, A.L. Hamilton, *Seeking qualitative rigor in inductive research:notes on the Gioia methodology*, „Organizational Research Methods" 2013, Vol. 16(1), s. 15–31.
[419] J. Saldana, op. cit., s. 58.

Tabela 3.8. Matryca kodów zastosowana w analizie treści



Drzewo kodowe	WSA1	WSA2	WSA3	WSA4	WSA5	WSA6	WSA7	WSA8	WSA9	WSA10	WSA11	WSA12	WSA13	WSA14	WSA15	WSA16	SUMA
SZBI																	0
ASI jest odpowiedzialny za SZBI			1				1	2	1							2	7
Kierownicy są odpowiedzialni za SZI						1		1									2
IOD jest odpowiedzialny za SZBI	4	3	1			1	1	1				1			1	2	15
Dyrektor jest odpowiedzialny za SZB		1					2		1	1		2	1		2		10
Prezes jest odpowiedzialny za SZBI	1	1	1	1	1		1	1	1	1	1		1	1	2	1	15
UoOIN	1	1											1	1			4
ISO 27001						1		1		1	1						4
KRI					1		1	1		1	1				1	1	7
RODO	1	1	1	1	1	1	1	1	1			1	2	1	1	1	15
Ustanowienie i przeglądy SZBI	2	1	1		1	1	1	1	1	1	1	1	1	1	1	1	16
Dokument papierowy	1	1			1	1	1				1	1	1				8
LAN/Intranet		1	1		1		1	1	1	1			1	1	1	1	11
Poczta elektroniczna			1	1			1			1		1	1		1		7
Na szkoleniu	1	1							1	1				1		1	6
Delegacja obowiązków	4	4	2		1	2	4	4	2	1		3	2		3	5	37
Ustne ustalenia					1									1			2
Program szkoleń	2	1	1				2		1	1			1		1	1	11
Analiza ryzyka		1					1			1			2				5
Incydent odnotowany	1	1	1				1			1			1		1		7
Reagowanie	1			1	2	1	1		1	1	1			1	1	1	12
Właściwa reakcja na incydent	1	1	1	1				1		1			1		1		8
Zmiana procedur po incydencie	1						1	1					1				4
Szkolenie po incydencie	1	1		1			1										4
Raportowanie		1					1										2
Kultura organizacyjna																	0
Prezes wpływa na KO	1	1					1	1		1		1	1	1	1	1	10
Dyrektor wpływa na KO	1						1			1			1	1	1	1	7
Kierownicy wpływają na KO		1		1	1			1		1			1	1	1	1	9
Wszyscy mają wpływ na KO			1	1	1	1			1	1	1				1		8
Czynnik ludzki				1	1	1						1		1	2		7
Normy								1	1	1	1			1		1	6
Zachowanie	1				1	1	1	1		1	1		1		1	1	10
Komunikacja		1	1	1					1				2				6
Zaufanie		1												1			2
Współpraca			1	2	1	1			1				1	1	1		9
Postawy				1	1	2	1	1	1				1	1	1	1	11
Atmosfera						1			1	1			1	1		1	6
Wartości						1		1	1	1	1					1	6
Kultura bezpieczeństwa informacji																	0
Poczucie obowiązku			1	1						1			1		1		5
Utożsamianie się z organizacją, lojal			1			1			1					1		1	5
Współpraca				1		1	1										3
Staranność wykonywania zadań								1									1
Zasada ograniczonego zaufania	1								2								3
Brak kontestacji		1										1					2
Wiedza i świadomość	1	1	2	1	1	1	1	1	1	1		1	2	1	1	1	17
Właściwy przepływ informacji	1														1		2
Zaangażowanie Kierownictwa, IOD,							1			1					1		3
Uczestniczenie w szkoleniach			1				1		1	1			1	1	1		7
Przestrzeganie procedur	2		1	2		1	2	1	2	1	1		1			2	16
SUMA	30	27	21	18	17	21	33	25	25	27	11	14	31	20	31	29	380

Źródło: opracowanie własne z wykorzystaniem programu MAXQDA.

Tabela 3.8 przedstawia matrycę występowania kodów opisowych i kodów wyższego poziomu w wypowiedziach dyrektorów poszczególnych sądów (WSA1 – WSA16). Wykorzystując uzyskany podział w rozdziale 4 (Podrozdział 4.1), została przedstawiona analiza danych pozyskanych na drodze wywiadów. Pierwszy kod wyższego poziomu to *SZBI* (skrót od systemu zarządzania bezpieczeństwem informacji), do którego zostały przypisane kody dotyczące procesów związanych z: tworzeniem, dostosowaniem, doskonaleniem, monitorowaniem i realizacją SZBI. Znajdują się tu również kody dotyczące pełnionych ról, nałożonych odpowiedzialności

i zaangażowania w utrzymaniu SZBI. *Kultura organizacyjna* to kod, którym zakodowane były fragmenty wypowiedzi zawierające informacje na temat rozumienia pojęcia kultury organizacyjnej przez respondentów oraz ich poglądy na temat tego, kto ma wpływ na kształtowanie się kultury w organizacji. Trzeci kod wyższego poziomu to *kultura bezpieczeństwa informacji*. Pojęcie to zostało wyodrębnione na podstawie przeprowadzonego systematycznego przeglądu literatury (Rozdział 3.1.2), dotyczącego związku kultury organizacyjnej z zarządzaniem bezpieczeństwem informacji. Agregował on kody sprzyjające kształtowaniu się kultury bezpieczeństwa informacji w organizacji.

3.7.2. Badanie dokumentów

Badanie zostało przeprowadzone w 16 WSA przy uczestnictwie pracownika danego WSA odpowiedzialnego za przegląd SZBI. W 10 przypadkach tą osobą był inspektor ochrony danych, w 4 administrator systemu informatycznego, a w 2 dyrektor sądu. Zebrane dane zostały przeanalizowane i wykorzystane do oceny dojrzałości SZBI badanych organizacji oraz poddane analizie statystycznej.

3.7.3. Badanie ankietowe

Badanie prowadzone było techniką CAWI w dniach 17 stycznia – 18 lutego 2023 r. Link do ankiety został przekazany do dyrektorów wszystkich sądów, następnie został przez nich przesłany pracownikom na ich służbowe konta pocztowe lub udostępniony w intranecie. Zebrane dane poddano ocenie i przedstawiono w postaci graficznej przy wykorzystaniu edytora arkuszy kalkulacyjnych oraz poddane analizie statystycznej.

4. Wyniki

4.1. Wyniki badania – wywiad

4.1.1. Systemy zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych

Podczas przeprowadzanych wywiadów trzynastu dyrektorów wskazało prezesów sądów jako osoby odpowiedzialne za SZBI. W ich wypowiedziach pojawiła się informacja, że prezes jako kierownik jednostki jest administratorem danych osobowych[420], a z uwagi na fakt, że w WSA przetwarzane są informacje zawierające również dane osobowe, był on wskazywany jako osoba odpowiedzialna za bezpieczeństwo informacji.

„Tak naprawdę w naszej jednostce te zadania są skupione, myślę, głównie u prezesa i u pracowników jemu podległych bezpośrednio. Częściowo scedowane na mnie. Bo jesteśmy w sumie jednostką stosunkowo niedużą, stąd wiele rzeczy jest tak porozkładanych. Wiadomo, ochrona danych osobowych, prezes jako administrator danych osobowych. Cała sfera podlega prezesowi, na czele IOD. Podobnie z bezpieczeństwem informacji niejawnych. Część obowiązków, które w przepisach nie są wprost przypisane kierownikowi jednostki, prezes ceduje częściowo na mnie – zależy, jakiego obszaru bezpieczeństwa dotyczy. Co do bezpieczeństwa fizycznego budynku – to wiadomo, że to jest bardziej działka dyrektora i podległych mu oddziałów. W skrócie tak to wygląda".

Źródło: Cytat z wywiadu w WSA15.

Tylko w jednym sądzie, WSA6, dyrektor uważał, że za system zarządzania bezpieczeństwem informacji odpowiadają kierownicy komórek organizacyjnych na wszystkich szczeblach zarządzania. W dwóch sądach (WSA12, WSA7) dyrektorzy wskazywali siebie jako główne osoby odpowiedzialne za SZBI.

„U nas jest nietypowo, bo jestem ja – dyrektor odpowiedzialna, ale ja uważam to za niewłaściwe, to poprzedni prezes wydał takie zarządzenie. Ja osobiście mam odrębne zdanie i prezes miał to zmienić, bo to już za poprzednika się zadziało(…). Nawet

[420] Art. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, s. 1 z późn. zm.); ustawa z dnia 25 lipca 2002 r. Prawo o ustroju sądów administracyjnych (t.j. Dz. U. z 2022 r., poz. 2492).

miałam doczytać, ale się już znudziłam tym tematem, Prezes tego do dzisiaj nie zmienił".

Źródło: Cytat z wywiadu w WSA12.

Wypowiedzi wszystkich dyrektorów świadczyły o zaangażowaniu we wdrażanie, utrzymywanie i kontrolowanie systemu zarządzania bezpieczeństwem informacji. Czterech z nich (WSA2, WSA7, WSA8, WSA9) wymieniło siebie, zaraz po prezesie sądu, jako osoby odpowiedzialne za SZBI.

„Pan prezes. Zapewne ja, w jakiejś mierze, większej lub mniejszej. Zapewne administrator systemów informatycznych i inspektor ochrony danych. Przypuszczam, że również nasza kierownik Oddziału Spraw Ogólnych i Osobowych".

Źródło: Cytat z wywiadu, WSA8.

„Prezes oraz dyrektor. Mam uprawnienia do przyjmowania upoważnień dotyczących przetwarzania danych osobowych".

Źródło: Cytat z wywiadu, WSA2.

W jednym przypadku dyrektor WSA4 stwierdził, że pełni tylko rolę wykonawcy ustaleń.

„Rola dyrektora jest trochę rolą służebną. Wszystkie te zmiany przechodzą przez inspektora i przez prezesa. W sumie też jako ostatnie ogniwo, słyszę oczywiście o nich, że tam coś będziemy zmieniać, coś robić. (…) Powiem, że gdzieś tam do konsultacji dostawałem te ustalenia, ale to wszystko przechodzi przez prezesa".

Źródło: Cytat z wywiadu, WSA4.

We wszystkich sądach zarządzenie prezesa wprowadziło regulacje dotyczące SZBI. Według wiedzy dyrektorów zostały one utworzone w zgodności z następującymi dokumentami (Tabela 4.1): Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Rozporządzenie Ogólne o Ochronie Danych Osobowych, skrót: RODO; General Data Protection Regulation, skrót: GDPR); Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów

teleinformatycznych (skrót: KRI, t.j. Dz. U. z 2017 r., poz. 2247), norma PN-ISO/IEC 27001 oraz Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (skrót: UoOIN, t.j. Dz. U. z 2024 r., poz. 632).

Tabela 4.1. Zestawienie dokumentów według zaleceń, których zostały opracowane SZBI w wojewódzkich sądach administracyjnych

Drzewo kodowe	WSA1	WSA2	WSA3	WSA4	WSA5	WSA6	WSA7	WSA8	WSA9	WSA10	WSA11	WSA12	WSA13	WSA14	WSA15	WSA16	SUMA
UoOIN	■	■											■	■			4
ISO 27001						■		■		■	■						4
KRI					■		■	■		■	■				■	■	7
RODO	■	■	■	■	■	■	■	■	■			■	■	■	■	■	14
SUMA	2	2	1	1	2	2	2	3	1	2	2	1	2	2	2	2	29

Źródło: opracowanie własne z wykorzystaniem programu MAXQDA.

We wszystkich jednostkach prowadzi się rejestr i zbiór zarządzeń w formie papierowej. Zarządzenia udostępniane są w sieci lokalnej, a w niektórych sądach rozsyłane są na indywidualne konta poczty elektronicznej (Tabela 4.2). We wszystkich sądach każda nowa osoba rozpoczynająca pracę przechodzi wstępne szkolenia, w trakcie których przekazywane są informacje na temat obowiązujących regulacji dotyczących bezpieczeństwa informacji.

„Mamy tak, po pierwsze jest to tradycyjna forma papierowa. Nasze zarządzenia są w formie elektronicznej dostępne dla wszystkich pracowników. W zasobie sieciowym, w naszej sieci wewnętrznej, są one dostępne. Oprócz formy papierowej są rozsyłane w formie elektronicznej. Tak, obecnie papierowa jest na etapie konsultacji, a potem przybiera formę elektroniczną – w tej postaci jest rozsyłana, ale nie zawsze każdemu, przynajmniej kierownikowi jednostki organizacyjnej, a następnie umieszczana w sieci, w zbiorze zarządzeń prezesa”.

Źródło: Cytat z wywiadu, WSA13.

„D: Zawieszane są w takiej zakładce, naszej wewnętrznej stronie intranetowej, jest taka zakładka z różnymi zarządzeniami, procedurami. Generalnie są dostarczane do kierowników sekretariatów do oddziałów i są dalej przekazywane do pracowników. Staramy się dostarczać papierowo. Czuwają nad tym kierownicy.

A: Czy sędziowie, asesorowie są też informowani?

D: Pracownicy w szerokim znaczeniu”.

Objaśnienie: D – dyrektor, A – autor dysertacji.

Źródło: Cytat z wywiadu, WSA5.

Wszyscy pracujący w wojewódzkich sądach administracyjnych mieli możliwość zapoznania się ze SZBI oraz jego aktualizacjami. Tabela 4.2 przedstawia sposoby informowania o regulacjach w poszczególnych sądach. Uzyskane odpowiedzi od respondentów wpłynęły na ocenę dojrzałości SZBI, gdyż wymogiem osiągnięcia 2. poziomu dojrzałości[421] jest skuteczne poinformowanie interesariuszy o aktualnych przepisach związanych z bezpieczeństwem informacji.

Tabela 4.2. Sposób informowania osób pracujących w wojewódzkich sądach administracyjnych o przepisach dotyczących SZBI

Drzewo kodowe	WSA1	WSA2	WSA3	WSA4	WSA5	WSA6	WSA7	WSA8	WSA9	WSA10	WSA11	WSA12	WSA13	WSA14	WSA15	WSA16	SUMA
Dokument papierowy	■	■			■	■	■				■	■	■				8
LAN/Intranet		■	■		■		■	■	■	■			■	■	■	■	11
Poczta elektroniczna			■	■			■			■		■	■		■		7
Na szkoleniu	■	■							■	■				■		■	6
Σ SUMA	2	3	2	1	2	1	3	1	2	3	1	2	3	2	2	2	32

Źródło: opracowanie własne na podstawie wywiadów z dyrektorami WSA z wykorzystaniem programu MAXQDA.

We wszystkich badanych sądach aktualizacja przepisów dotyczących SZBI nastąpiła w 2018 r. w związku z obowiązkiem rozpoczęcia stosowania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Zarówno w artykule 24 ust. 1 wymienionego aktu prawnego, jak i w odwołującym się w temacie SZBI do normy PN-ISO/IEC 27001, §20 ust. 3 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zapisane są wymogi ustanowienia w regularnych odstępach czasu przeglądów[422] i uaktualnień SZBI, aby zapewnić skuteczność wdrożonych środków technicznych i organizacyjnych. Tylko

[421] COBIT® 2019 Framework: Governance and Management Objectives, s. 139.

[422] PN-ISO/IEC 27000:2014-11 „3.5.1 Przegląd.

Organizacja powinna podjąć następujące kroki w zakresie ustanowienia, monitorowania, utrzymania i doskonalenia swojego SZBI:

a) identyfikować aktywa informacyjne i związane z nimi wymagania bezpieczeństwa informacji;
b) oszacować ryzyka w bezpieczeństwie informacji oraz odpowiednio z nimi postępować;
c) wybierać i wdrażać odpowiednie zabezpieczenia, aby zarządzać nieakceptowalnymi ryzykami;
d) monitorować, utrzymywać i doskonalić skuteczność zabezpieczeń z aktywami informacyjnymi organizacji.

W celu zapewnienia, że SZBI skutecznie chroni aktywa informacyjne organizacji w sposób ciągły, konieczne jest ciągłe powtarzanie punktów (a)-(d), aby zidentyfikować zmiany ryzyk, strategii organizacji lub celów biznesowych".

w 7 sądach dyrektorzy twierdzili, że przeglądy wykonywane są przynajmniej raz w roku, w 2 sądach dyrektorze nie znali częstotliwości przeprowadzania przeglądów. W pozostałych przypadkach rozmówcy informowali, że przeglądy wykonywane są bez wyznaczonego z góry harmonogramu. Istnieją pewne rozbieżności pomiędzy informacjami uzyskanymi podczas wywiadów a badaniem dokumentacji związanej ze SZBI (Tabela 4.3).

„D: To znaczy, nie ma terminu, w razie potrzeby na sygnał. Nie ma cykliczności.
A: Kto wysyła taki sygnał?
D: Proszę pani, taki sygnał jest wysyłany prezesowi przez osobę, pracownika oddziału kadr[423], który na bieżąco śledzi zmiany przepisów. W przypadku takich korekt ma obowiązek prezesa poinformować, a dalej prezes podejmuje decyzję albo poprzez wydanie zarządzenia, albo jakiegoś pisma informacyjnego. Tu jest opcjonalność działania. Ma obowiązek przeglądać i informować mnie jako dyrektora i prezesa o tym. Ta informacja jest jakby częścią zarządzania".

Objaśnienie: D – dyrektor, A – autor dysertacji.

Źródło: Cytat z wywiadu, WSA5.

Tabela 4.3. Rozbieżności pomiędzy informacjami uzyskanymi podczas wywiadów a badaniem dokumentacji związanej ze SZBI

WSA	**Zapis z dokumentach SZBI**	**Wywiad z dyrektorem**
WSA1	Przynajmniej raz w roku	Przynajmniej raz w roku
WSA2	Bez harmonogramu	Nie wiem
WSA3	Przynajmniej raz w roku	Bez harmonogramu
WSA4	Bez harmonogramu	Nie wiem
WSA5	Przynajmniej raz w roku	Bez harmonogramu
WSA6	Bez harmonogramu	Bez harmonogramu
WSA7	Przynajmniej raz w roku	Przynajmniej raz w roku
WSA8	Przynajmniej raz w roku	Przynajmniej raz w roku
WSA9	Bez harmonogramu	Bez harmonogramu
WSA10	Przynajmniej raz w roku	Przynajmniej raz w roku
WSA11	Przynajmniej raz w roku	Przynajmniej raz w roku
WSA12	Bez harmonogramu	Bez harmonogramu
WSA13	Przynajmniej raz w roku	Przynajmniej raz w roku
WSA14	Bez harmonogramu	Bez harmonogramu
WSA15	Przynajmniej raz w roku	Przynajmniej raz w roku

[423] W strukturze wojewódzkich sądów administracyjnych oddział kadr to Oddział Spraw Ogólnych i Osobowych.

WSA	Zapis z dokumentach SZBI	Wywiad z dyrektorem
WSA16	Przynajmniej raz w roku	Bez harmonogramu

Źródło: opracowanie własne na podstawie wywiadów z dyrektorami WSA i informacji uzyskanych z dokumentów dotyczących SZBI.

Prezes WSA sprawuje nadzór nad działalnością sądu, m.in. podpisując zarządzenia usprawniające organizację i techniki pracy w sądzie. Czynnością świadczącą o zaangażowaniu w utrzymanie SZBI było wydawanie zarządzenia wprowadzającego lub aktualizującego przepisy dotyczące bezpieczeństwa informacji. Osoby, które miały w zakresie swoich obowiązków przeprowadzanie przeglądów SZBI, konsultowały się z interesariuszami, a następnie przygotowywały treści wewnętrznych przepisów.

„Myślę, że głównie to polega na bieżącej współpracy i wymianie informacji kierownictwa z pracownikami, którzy określonym obszarem się zajmują i za niego odpowiadają, czyli znowu powrócę do naszego Inspektora Ochrony Danych czy Administratora Systemu Informatycznego w naszej strukturze, pani pełnomocnik do informacji niejawnych. Aby nic nie przeoczyć, żeby być ciągle na bieżąco i by nasze procedury były dostosowane do aktualnego stanu prawnego, te osoby mają przypisany taki obowiązek, aby w ramach zmian w przepisach czy potrzeby korekty tych dokumentów, sygnalizowały. Na zasadzie bieżącej współpracy i kontaktu.
Prezes się zapoznaje z raportami – jak są jakieś zalecenia czy uwagi, to też są stosowne dalsze informacje dla pracowników, żeby je wdrożyć czy się ustosunkować. Tak to wygląda".
Źródło: Cytat z wywiadu, WSA15.

„Prezes zawsze znajduje czas na rozmowę w sprawie bezpieczeństwa informacji. Każdą sprawę można przedyskutować, wspólnie znaleźć rozwiązanie problemu".
Źródło: Cytat z wywiadu, WSA14.

„Jak są przeglądy wszystkich zarządzeń. Na jakimś forum jest to konsultowane. Prezes oczywiście zarządzenia podpisuje, jak jest zmiana zarządzenia po przeglądowa.
Można powiedzieć, że każde zarządzenie jest analizowane pod kątem jego aktualności, konieczności wprowadzenia zmian. Przy tym świadome bądź nieświadome jakieś analizy ryzyka są podejmowane".
Źródło: Cytat z wywiadu, WSA13.

„Kierownictwo sądu angażuje się w utrzymanie SZBI na poziomie strategicznym. Na tym poziomie prowadzone jest zarządzanie strategią rozwoju i doskonalenia SZBI w oparciu o wyniki analizy ryzyka w odniesieniu do zmieniającego się otoczenia prawnego, technologicznego i społecznego. Określane są kierunki rozwoju SZBI, zapewniane są niezbędne środki i zasoby, prowadzony jest nadzór nad SZBI".
Źródło: Cytat z wywiadu, WSA10.

„Do kierownictwa spływają sprawozdania, z którymi się zapoznaje. Do końca roku roczne sprawozdanie składa IOD. Co kwartał pełnomocnik do informacji niejawnych. Informatycy kwartalnie, co jest połączone z kontrolą zarządczą".
Źródło: Cytat z wywiadu, WSA2.

„Jeżeli jest potrzeba, powiedzmy, no nie wiem, zakupu jakiś urządzeń, korekty zachowań – to się wtedy podejmuje działanie".
Źródło: Cytat z wywiadu, WSA5.

Z przedstawionych wypowiedzi dyrektorów sądów wynika, że byli oni współtwórcami SZBI, poza jednym wyjątkiem dyrektorem WSA4. Prezesi byli zapoznawani ze sprawozdaniami i postulatami zmian. Nie byli oni inicjatorami wprowadzanych rozwiązań, uczestniczyli w końcowej fazie powstawania SZBI. Podpisywali zarządzenia, które wprowadzały w organizacji przepisy dotyczące zarządzania bezpieczeństwem informacji. W 5 z badanych sądów zaangażowanie prezesów w utrzymanie SZBI wyróżniało się od pozostałych, wykraczało poza zapoznawanie się z przygotowanymi propozycjami dokumentów i ich podpisywanie.

Na pytanie dotyczące zapamiętanego incydentu związanego z bezpieczeństwem informacji i opinii na temat tego, jak sprawdziły się procedury dotyczące zgłaszania incydentów, reagowania i wdrażania programów naprawczych, 7 dyrektorów sądów odpowiedziało, że nie zaistniał lub nie pamiętają, aby zdarzył się jakikolwiek incydent.

„W sądzie nie było incydentu bezpieczeństwa informacji, rozumianego w myśl przyjętej w Polityce Bezpieczeństwa Informacji definicji, jako naruszenie bezpieczeństwa informacji przetwarzanej w sądzie ze względu na poufność, dostępność i integralność".
Źródło: Cytat z wywiadu, WSA16.

„Nie przychodzi mi na myśl żaden incydent".
Źródło: Cytat z wywiadu, WSA5.

Można przypuszczać, że procedury były na tyle skuteczne, że ograniczyły występowanie incydentów czy naruszeń lub najwyższe kierownictwo sądu nie było powiadamiane.

Pozostali dyrektorzy przedstawili opinię na temat procedur związanych z obsługą incydentów. W ramach programów naprawczych przeprowadzano szkolenia oraz zmiany procedur.

„Mechanizmy zadziałały. Do błędu przyczynił się czynnik ludzki. Podjęte zostało działanie reaktywne. Incydent zgłoszony był do GIODO. Po incydencie – doszkalanie".
Źródło: Cytat z wywiadu, WSA2.

„Reakcje osób odpowiedzialnych na powstały incydent były szybkie i właściwe, zgodne z wdrożoną »Kartą naruszeń ochrony danych«, opracowaną przez IOD. Po incydencie postawiono nacisk na zwiększenie wiedzy i świadomości pracowników w zakresie zagrożeń płynących z sieci – w szczególności na rozpoznawanie i właściwe reagowanie na podejrzane wiadomości mailowe oraz próby wyłudzeń danych. Opracowano odpowiednie procedury".
Źródło: Cytat z wywiadu, WSA1.

„System zadziałał zgodnie z procedurą opisaną w Polityce Reagowania na Incydenty oraz Naruszenia Ochrony Danych Osobowych (PRINODO). Incydent i reakcja na niego zostały przeanalizowane, potwierdzono skuteczność działań podjętych zgodnie z wdrożoną procedurą i zdecydowano, że wprowadzenie zmian w SZBI jest zbędne".
Źródło: Cytat z wywiadu, WSA10.

„Zadziałał myślę tak sobie system. A może sam system nie jest wadliwy, ale czynnik ludzki zadziałał. Możemy postawić do sprawdzania zamiast dwóch osób trzy, ale trzecia też może się pomylić. Sam system zadziałał. Incydent został zgłoszony do NSA, osoby odpowiedzialne za sytuację brały czynny udział w wyjaśnianiu, Prezes również się zaangażował. Kierownictwo z tego incydentu wyciągnęło wnioski".
Źródło: Cytat z wywiadu, WSA8.

W 9 sądach, w których dyrektorzy zapamiętali zaistniały w przeszłości incydent, w ich odczuciu reakcja pracowników sądów na zaistniały problem była właściwa. Został on zgłoszony odpowiednim osobom, zadziałały procedury, wyciągnięte zostały wnioski oraz wprowadzono zmiany, jeżeli zaistniała taka potrzeba.

4.1.2. Postrzeganie roli kultury organizacyjnej w organizacji przez kierownictwo sądu

Odpowiedzi na zadane pytania w zakresie tego, czym dla respondentów jest kultura organizacyjna, były zróżnicowane. Celem wyeksponowania tej różnorodności poniżej zaprezentowano wszystkie udzielone odpowiedzi. Dyrektorzy artykułowali, że mają trudność w sformułowaniu odpowiedzi, czym jest dla nich kultura organizacyjna. Potwierdza to opinie przedstawione w podrozdziale 4.2, z której wynika, że pojęcie kultury organizacyjnej jest trudne do zdefiniowania.

„Zadała mi pani dosyć trudne pytanie. Jak to poniekąd zdefiniować. Cóż to jest kultura organizacyjna? To zarówno podział obowiązków, przepływy pomiędzy osobami, a także stosunki ludzkie czy relacje ludzkie przy okazji tych czynności.
Tak to postrzegam, tak na gorąco. Podział obowiązków ma być jasny, granice możliwie ostre, co jest dobrym rozwiązaniem w tego typu organizacji. Żeby nie było sfery budzącej zbyt duże wątpliwości. Więc ten podział obowiązków pomiędzy komórkami, jak i pomiędzy pracownikami. Jest równie ważne, żeby dana komórka, a tym samym w jakiejś mierze i sąd, funkcjonowały dobrze (…) – w danej komórce obowiązki muszą być dobrze podzielone. Pewne procesy, które przebiegają, muszą mieć ustalony porządek i kolejność, ludzie w tym uczestniczący, to jest bardzo ważne. Ja mam doskonałą sytuację, no prawie doskonałą. Ważna jest w kulturze organizacyjnej – w tej części, którą ja kieruję, stoję na czele, pozytywna współpraca pomiędzy kierownikami oddziałów, nie ma konkurencji”.
Źródło: Cytat z wywiadu, WSA13.

„Zespół pewnych cech, może nie cech, wartości, ludzi, procedur istniejących w naszej organizacji. Możemy mieć oczekiwania, że ta kultura jest dobra, pożądana. Staramy się być, nie wiem, czy to jest dobre słowo, powściągliwi w swoich emocjach. Oczywiście, każdemu może się zdarzyć lepszy, gorszy dzień, wybuch. Ktoś jest bardziej ekspresyjny, ktoś mniej. Ktoś jest ekstrawertykiem, ktoś introwertykiem. Ale rzeczywiście te normy społeczne tutaj tak ogólnie przyjęte i rozumiane jako postawa służbowa, którą fajnie byłoby reprezentować sobą, tak dobrze rozumiana postawa służbowa. To myślę, że akurat u nas to znajduje jak najbardziej odzwierciedlenie”.
Źródło: Cytat z wywiadu, WSA8.

„W takim szerszym ujęciu całej naszej tutaj organizacji. Myślę, że jest to, powinna być to – w moim odczuciu – właśnie taka dobra współpraca wszystkich pracowników. Szczególnie osób może takich funkcyjnych. Odpowiedzialność też i poczucie odpowiedzialności, sprawczości w pewnych też obszarach, tak aby one w ostateczności zadziałały skutecznie, właściwie w określonych sytuacjach. Bez szkody, z pożytkiem dla organizacji".

Źródło: Cytat z wywiadu, WSA15

„Nigdy się nie zastanawiałem, ale kultura organizacyjna dla mnie to jest sposób funkcjonowania jednostki, w sposób dosyć empatyczny i zarówno do współpracowników, jak i do wykonywanych przez nich obowiązków, jak i kompetencji kierowniczych swoich przełożonych".

Źródło: Cytat z wywiadu, WSA5.

„Kultura to współpraca między innymi pomiędzy pracownikami, pomiędzy inspektorem ochrony danych, pomiędzy prezesem czy kierownictwem. Wszystkimi pracownikami, to bym nazywał tą kulturą. Przepływ informacji pomiędzy pracownikami a kierownictwem".

Źródło: Cytat z wywiadu, WSA4.

„Jakby to ubrać w słowa. Kultura, no nie wiem, co mam powiedzieć".

Źródło: Cytat z wywiadu, WSA3.

„Zaufanie, przepływ informacji, motywowanie, kontrola zarządcza".

Źródło: Cytat z wywiadu, WSA2.

„To usystematyzowany system postępowania obejmujący cały zakres działania, w tym przypadku w jednostce".

Źródło: Cytat z wywiadu, WSA1.

Wypowiedź dyrektora WSA7 świadczyła, że kultura organizacyjna może być utożsamiana z kulturą osobistą pracowników.

„Ja długo już pracuję. (…) Obserwuję, że coraz gorzej z tą kulturą osobistą. Młodzi ludzie są tacy, że wszystko wiedzą. Jakby nas sprawdzają trochę. Nie lubią »papierologii«, ale te zarządzenia, procedury, dokumenty pozwalają nam okiełznać tych nowych ludzi. Potem oni wiedzą, oni nie wiedzą, dlatego te potwierdzenia, ta otoczka jest potrzebna, ale to wszystko zależy od ludzi. Z biegiem lat kultura tych osób jest

coraz wyższa. Oni po roku czasu poznają procedury i poznają zasady obowiązujące w sądzie. Oni to doceniają, uczą się, wiedzą, że takie kompendium wiedzy jest pomocne i łatwiej to odnajdą. (…) Młodzi domagają się podstawy prawnej, szanują swój podpis".
Źródło: Cytat z wywiadu, WSA7.

Rysunek 4.1. Słowa kojarzone z pojęciem kultura organizacyjna
Źródło: opracowanie własne z wykorzystaniem programu MAXQDA.

Analizując Rysunek 4.1, który przedstawia słowa użyte przez dyrektorów w udzielonych przez nich odpowiedziach na pytania, oraz zamieszczone poniższej wypowiedzi, można zauważyć, że część dyrektorów podało definicje bliskie funkcjonalistycznej koncepcji kultury organizacyjnej. Można przypuszczać, że wynikało to z przygotowania się do wywiadu po wcześniejszym zapoznaniu się z jego tematyką.

„Kultura organizacyjna to zbiór wewnętrznych praktyk i norm współpracy. Kultura organizacji to zestaw wartości, przekonań, zachowań i postaw, który pomaga pracownikom sądu zrozumieć i realizować przypisane im zadania. Kultura organizacyjna to także atmosfera panująca w firmie, systemy wartości właściwe dla instytucji sądownictwa oraz postawy kierownictwa i pracowników".
Źródło: Cytat z wywiadu, WSA16.

„Kulturę organizacyjną utożsamiam z ładem korporacyjnym. Każdy powinien wiedzieć, jakie ma zadanie w organizacji. Ważne są wiedza, kompetencje potrzebne na danym stanowisku. Oczywiście kultura organizacyjna ta również relacje, te pomiędzy pracownikami, jak również te pomiędzy kierownikiem a pracownikiem".
Źródło: Cytat z wywiadu, WSA14.

„Zbiór norm, zachowań, systemów wartości".
Źródło: Cytat z wywiadu, WSA11.

„Kultura organizacyjna jest zgodnie ze SZBI aktywem, wartością niematerialną stanowiącą wartość dla sądu i podlegającą ochronie. Na kulturę organizacyjną składają się normy społeczne i wartości, które wpływają na zachowania i działania kierownictwa, kierowników komórek organizacyjnych oraz pracowników, a także klimat organizacyjny, sposób zarządzania oraz standardy zachowania, mające znaczenie dla zrozumienia przez pracowników misji i celów sądu".
Źródło: Cytat z wywiadu, WSA10.

„Jest jednym z ważniejszych elementów, które tworzą sąd. Jest to m.in.: zespół wewnętrznych praktyk, norm, jak również atmosfera, komunikacja, systemy wartości oraz postawy pracowników, które zwiększają poczucie przynależności wśród pracowników oraz ujednolicają metody współpracy".
Źródło: Cytat z wywiadu, WSA9.

„Dla mnie to przede wszystkim ogólna atmosfera panująca w sądzie, rytuały zespołowe, systemy wartości sądu oraz postawy pracowników".
Źródło: Cytat z wywiadu, WSA6.

Według 75% dyrektorów kulturę organizacyjną można zmieniać, a największy wpływ na jej kształtowanie ma najwyższe kierownictwo sądu.
„Kadra zarządzająca jest tym elementem, który tworzy i kształtuje kulturę organizacyjną w największym stopniu, poprzez wybór i komunikowanie wartości istotnych dla sądownictwa".
Źródło: Cytat z wywiadu, WSA16.

„Specyfika pracy, naszych obowiązków jest taka, że w stosunkowo sztywnym obszarze się obracamy – jakiś ram formalnych i przepisów. Z pewnością, jak i na wiele spraw kierownictwo jednostki ma i musi mieć wpływ, również ma udział w kształtowaniu tej

kultury. Chciałabym, żeby to nie była utopia, ale różnie się to układa w realiach naszych. Też bym oczekiwała i też bym chciała, żeby faktycznie ten chociażby średni szczebel kierowniczy też miał jakieś poczucie, potrzeby i chęci w kształtowaniu tej kultury. Co, nie ukrywam, w tych czasach obecnych, które nie są łatwe dla wszystkich z różnych względów i globalnych, i krajowych, często może jest też utrudnione. Rośnie może też ludzkie zmęczenie, obciążenie obowiązkami, tak jak patrzę czasami na załogę. Sama też doświadczam natłoku pracy, niejednokrotnie jakiejś frustracji zawodowej. I to nie są elementy, które ułatwiają kształtowanie tego obszaru, o który pani pyta. I to jest taka moja świeża refleksja. Kulturę organizacyjną powinniśmy tworzyć my, pracownicy, ludzie w danej organizacji. Jeżeli dany element ludzki nie działa, że tak powiem, sprawnie, właściwie i wydajnie, to następuje zachwianie, które się w tym drobnym elemenciku przekłada się potem na całość funkcjonowania" .

Źródło: Cytat z wywiadu, WSA15.

„Góra: prezes, dyrektor. Ryba psuje się od głowy. Pracownik na dole nie zmieni »góry«. Kierownictwo ma wpływ na to, co dzieje się w sądzie".

Źródło: Cytat z wywiadu, WSA14.

„Prezes, kierownictwo stawia wymagania co do zachowania pewnych postaw".

Źródło: Cytat z wywiadu, WSA2.

„Osoby z najwyższego szczebla zarządzania w jednostce".

Źródło: Cytat z wywiadu, WSA1.

Wśród dyrektorów, którzy uważali, że najwyższe kierownictwo odgrywa największą rolę w kształtowaniu się kultury organizacyjnej, czterech z nich uważało, że wpływ mają również kierownicy niższego szczebla.

„Największy wpływ na kształtowanie się kultury organizacyjnej w sądzie ma kierownictwo sądu, a także – w mniejszym zakresie – kierownicy komórek organizacyjnych oraz pracownicy sądu".

Źródło: Cytat z wywiadu, WSA10.

Czterech dyrektorów nie wskazało wyłącznie kadry zarządzającej jako mającej szczególny wpływa na kulturę organizacyjną – uznali oni, że wszyscy pracownicy sądów na nią oddziałują.

„Wszyscy pracownicy mają wpływ na kulturę organizacyjną. To jest bardzo istotne, to właśnie nasze zachowanie w stosunku do drugiego człowieka. Uważam, że tutaj jest zawarte wszystko. Bo jeżeli człowiek potrafi rozmawiać z drugim człowiekiem, to zawsze droga się znajdzie: droga i rozwiązanie, i wspólna praca. A jak nie ma tego porozumienia, nie ma rozmowy, no to wszystko już wtedy się, że tak powiem, sypie".
Źródło: Cytat z wywiadu, WSA3.

„Oczywiście cała załoga sądu, to, jak będzie nam się pracowało, zależy od nas samych, naszych kompetencji, humorów".
Źródło: Cytat z wywiadu, WSA6.

„Na kulturę organizacyjną mają wpływ wszyscy. Kierownictwo, czyli przełożeni, powinni być uczuleni. Kiedy pojawi się jakiś konflikt, powinni podjąć działanie, aby nie rozwijał się szerzej. Sami pracownicy powinni się szanować, być względem siebie koleżeńscy".
Źródło: Cytat z wywiadu, WSA5.

„Kulturę organizacyjną tworzą wszyscy pracownicy, dlatego też należy otworzyć się na potrzeby i uwagi wszystki*ch* zatrudnionych, co w konsekwencji prowadzi do wypracowania najlepszych praktyk i zasady współpracy".
Źródło: Cytat z wywiadu, WSA9.

Dyrektorzy z dwóch sądów w WSA13 i WSA3 zauważyli, że bardzo istotnym elementem kultury organizacyjnej jest przepływ informacji, wzajemny sposób komunikowania się.

„Największy wpływ mają najwyżsi w hierarchii, kierownicy. Pierwszy prezes. Łatwiej mi wypowiadać się za moją część, to powiem drugi jest dyrektor i potem już kierownicy. Widzę tu pewien problem, w przypadku przewodniczących wydziałów nie zawsze oni dostrzegają, albo nie wszyscy dostrzegają, że są nie tylko sędziami, tylko są kierownikami dosyć dużych komórek organizacyjnych i odpowiadają za te komórki, chociażby za przepływ informacji. I on nieraz szwankuje w ramach tych komórek organizacyjnych. To tak postrzegam".
Źródło: Cytat z wywiadu, WSA13.

Jeden z dyrektorów zauważył, że na kulturę organizacyjną mają wpływ takie narzędzia w rękach przełożonych, jak system ocen pracowniczych i system motywacyjny.

„Na kulturę organizacyjną wpływ ma system ocen pracowniczych, system motywacyjny. Wpływają one na postawy. Kierownictwo wyznacza sposób działania".
Źródło: Cytat z wywiadu, WSA8.

4.1.3. Cechy kultury organizacyjnej wojewódzkich sądów związane z dojrzałością systemów zarządzania bezpieczeństwem informacji w sądach

Wszyscy respondenci zauważyli związek kultury organizacyjnej z zarządzaniem bezpieczeństwem informacji w sądzie. Najczęściej wymienianymi składowymi kultury były postawy, w tym lojalność pracowników. Zarządzanie bezpieczeństwem informacji bazuje na zaufaniu do przetwarzających informacje w sądach.

„Istota kultury organizacyjnej obejmuje wiele elementów, takich jak: deklarowana i przestrzegana hierarchia wartości, wartościowanie pracy, lojalność pracowników, sposób sprawowania władzy, relacje pomiędzy kierownictwem a pracownikami. To wszystko ma istotny i realny wpływ na szeroko rozumiane bezpieczeństwo, w tym bezpieczeństwo informacji".
Źródło: Cytat z wywiadu, WSA16.

„Kultura organizacyjna na wpływ na zarządzanie bezpieczeństwem informacji. Najważniejsze, jakimi ludźmi są pracownicy, jakie mają charaktery. Ważna jest lojalność w stosunku do pracodawcy. Bazujemy na zaufaniu do pracowników".
Źródło: Cytat z wywiadu, WSA14.

Dyrektorzy zauważali również, że w aspekcie bezpieczeństwa informacji ważne są wzory zachowań, które są wynikiem upowszechniania się postaw ukształtowanych przez wartości i normy społeczne akceptowalne w sądach.

„Wdrożenie odpowiednich środków ochrony, w tym zasad i czynności, które należy realizować, aby ograniczyć ryzyko naruszenia bezpieczeństwa, oraz ugruntowanie prawidłowych postaw i zachowań budują przekonanie, że to właśnie pracownicy są ważnym filarem bezpieczeństwa. Poprzez kulturę organizacji kreowane są również

zachowania i postawy pracownicze, które pomagają w wypracowaniu właściwego sposobu reagowania na pojawiające się ciągle nowe niebezpieczeństwa".
Źródło: Cytat z wywiadu, WSA9.

„Częściowo może mieć. Nie wykluczone, że gdyby niewłaściwie funkcjonowała kultura organizacyjna, to mogłaby powstać luka w bezpieczeństwie informacji".
Źródło: Cytat z wywiadu, WSA15.

Dyrektor WSA7 zauważył, że formalizacja działania, oparcie na przepisach i regulacjach, powinny sprzyjać skutecznemu zarządzaniu bezpieczeństwem informacji.

„Czym bardziej kultura organizacyjna organizacji jest bardziej sformalizowana, to ma to pozytywne przełożenie na system zarządzania bezpieczeństwem informacji".
Źródło: Cytat z wywiadu,WSA7.

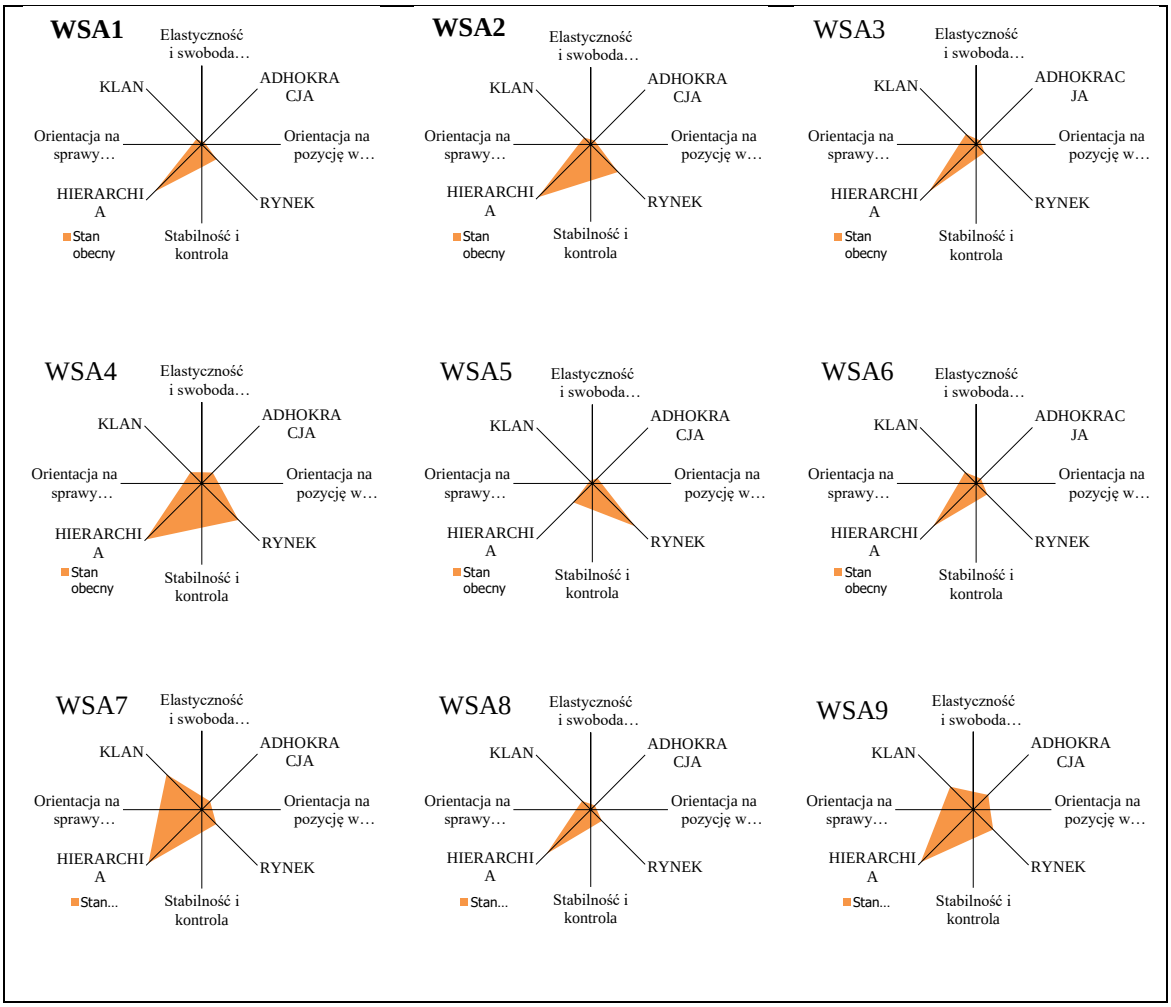
Skutecznemu zarządzaniu bezpieczeństwem informacji sprzyjała również zwiększająca się wśród pracowników świadomość występowania zagrożeń związanych z bezpieczeństwem informacji oraz wiedza o możliwościach przeciwdziałania tym zagrożeniom. Respondenci zapytani, czy można mówić o kulturze bezpieczeństwa informacji i danych osobowych, dzielili się na tych, którzy sądzili, że o takiej kulturze można mówić w ich sądach oraz na tych, którzy uważali, że kultura bezpieczeństwa informacji dopiero się kształtuje w ich organizacjach. Dziewięciu dyrektorów uważało, że zastosowane rozwiązania, w tym system szkoleń, sprawiły, że znacznie wzrosła świadomość zagrożeń w ich sądach. Twierdzili oni, że wśród pracowników utrwaliły się właściwe postawy i – pomimo pewnych uciążliwości w związku z zapewnieniem bezpieczeństwa informacji – widoczne jest odpowiednie zachowanie oraz można mówić o kulturze bezpieczeństwa informacji. W siedmiu sądach dyrektorzy wskazywali wdrażane rozwiązania, które wpływały na zmianę postaw i zachowań pracowników w stosunku do działań zmierzających do zapewnienia bezpieczeństwa informacji, ale jeszcze nie mogą jednoznacznie powiedzieć o kulturze bezpieczeństwa w tych WSA. Istnienie kultury bezpieczeństwa ma wpływ na pożądane zachowania i rzeczywiste wdrożenie polityki bezpieczeństwa[424] w organizacji, świadczy ona również o wysokim poziomie dojrzałości SZBI.

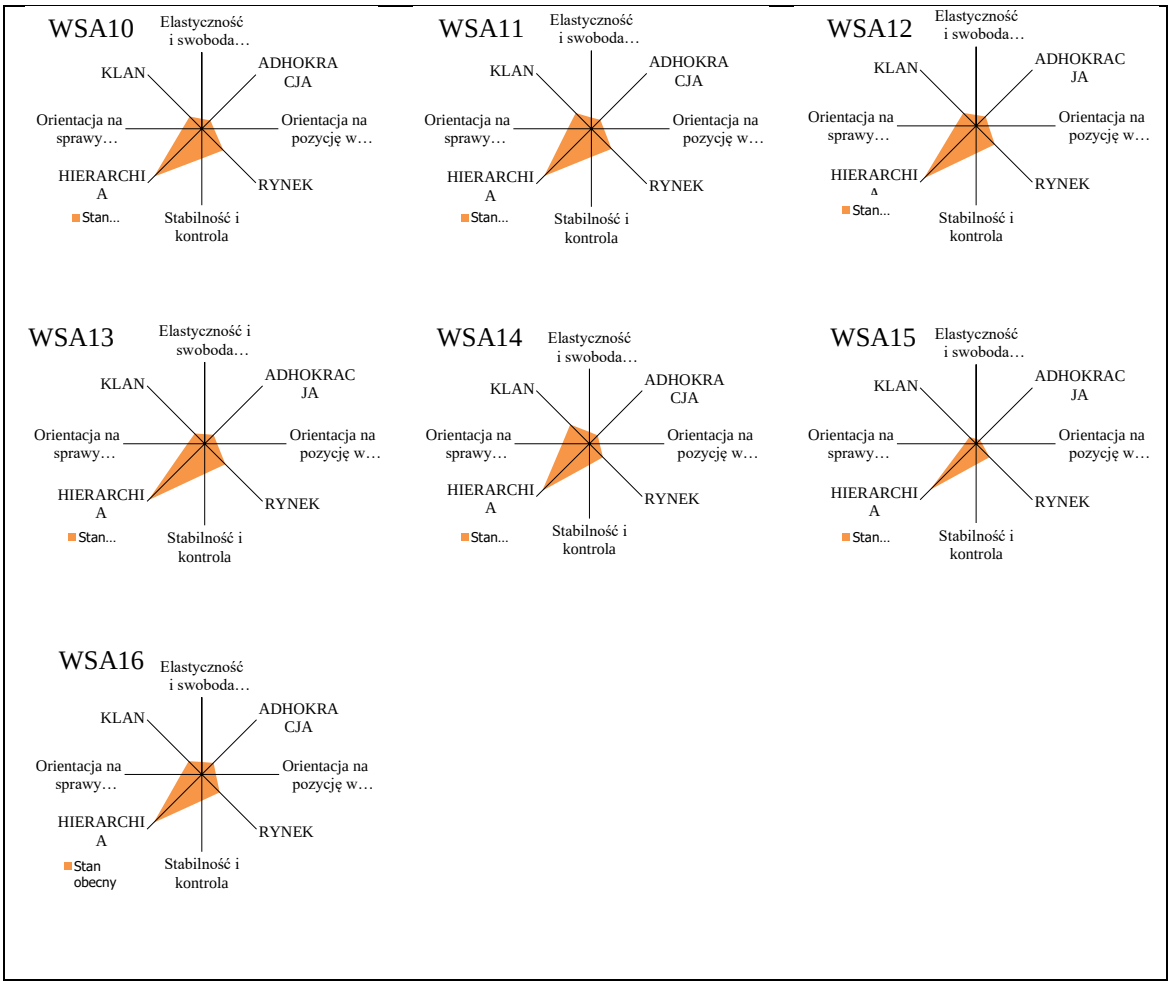
[424] COBIT® 2019 Framework: Governance and Management Objectives, s. 142.

4.2. Wyniki z ankiety realizowanej wśród pracowników wojewódzkich sądów administracyjnych

4.2.1. Badanie profilu kultury organizacyjnej

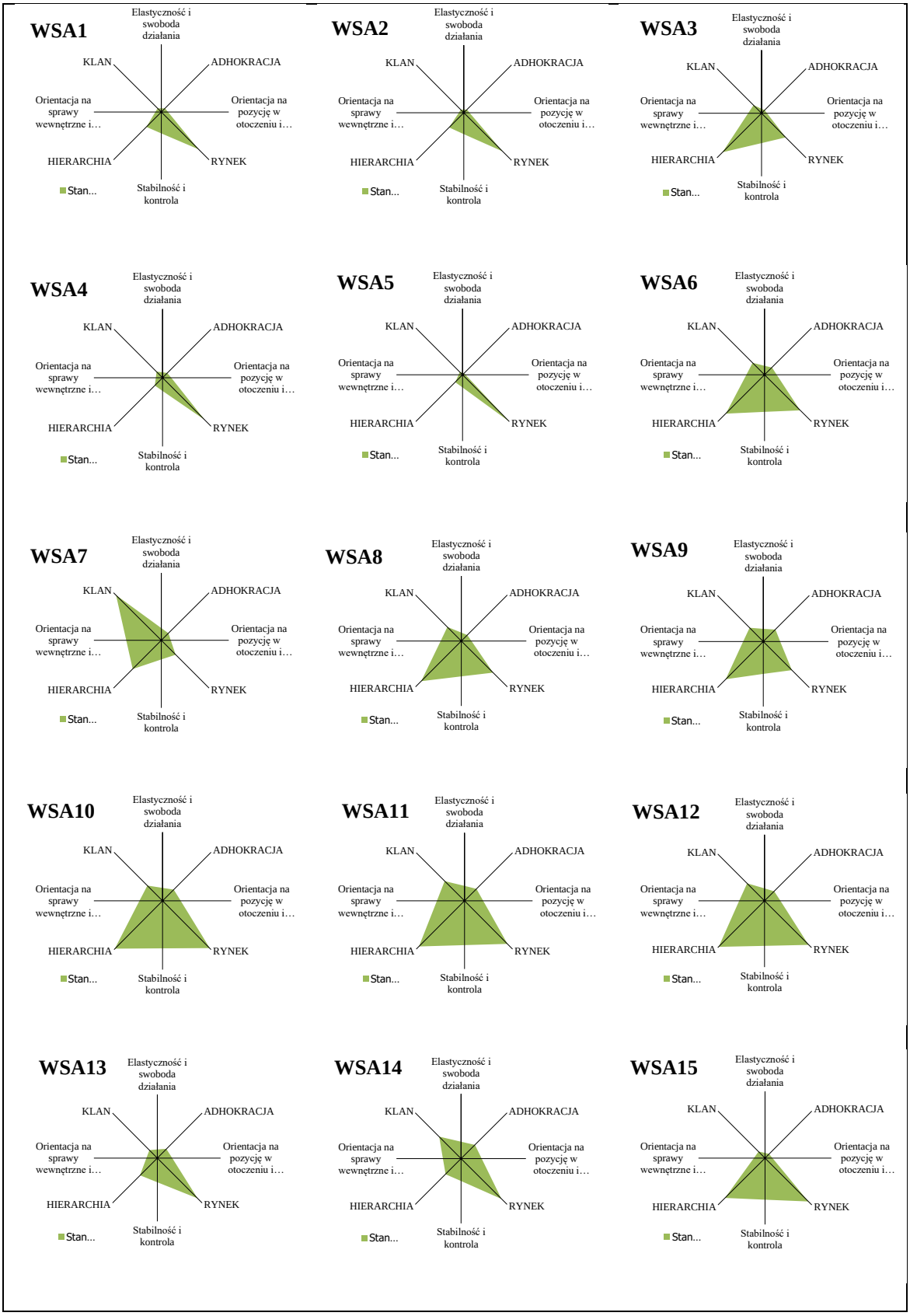
Pierwsza część narzędzia w badaniu ankietowym zawierała kwestionariusz OCAI. Za jego pomocą zostały zidentyfikowane profile kultury organizacyjnej, jakie są postrzegane przez respondentów jako dominujące w wojewódzkich sądach administracyjnych (Załącznik 7). W 15 wojewódzkich sądach administracyjnych dominującym profilem kultury organizacyjnej, który stanowi średnią z sześciu badanych wymiarów, był profil „hierarchia", tylko w jednym sądzie WSA5 zidentyfikowano inny dominujący profil – „rynek" (Rysunek 4.2).

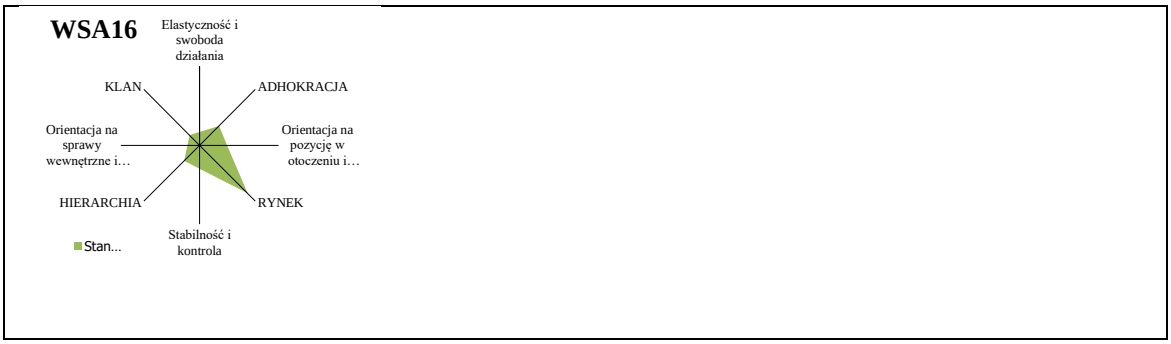




Rysunek 4.2. Profile kultury organizacyjnej poszczególnych wojewódzkich sądów administracyjnych
Źródło: opracowanie własne.

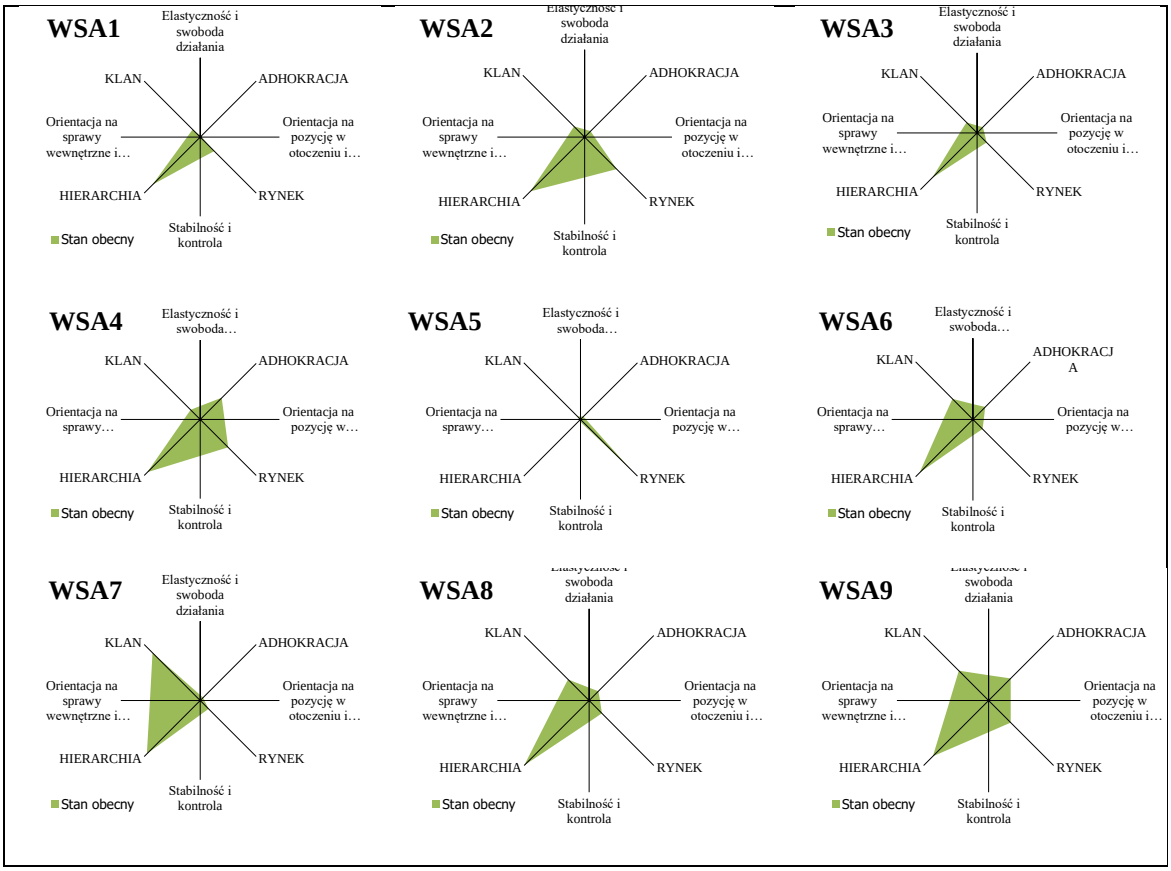
Różnice pomiędzy sądami widoczne były w poszczególnych wymiarach kultury organizacyjnej, w szczególności w wymiarze „przywództwo w organizacji" (Rysunek 4.3). W wymiarze tym w 50% badanych sądów zauważanymi przez respondentów jako dominujące były cechy charakterystyczne dla profilu kultury rynkowej. Oznacza to, że kierownicy byli postrzegani jako pełniący przede wszystkim funkcje nadzorcze, motywujące do działań i osiągania wyznaczonych celów. W jednym z sądów WSA7 dominowały cechy kultury klanowej. Przełożeni byli w tej organizacji widziani jako twórcy zespołów realizujących wspólne cele, osoby służące pomocą i wsparciem. W pozostałych sądach cechy rynkowej kultury osiągały zbliżone wartości wskaźników do cech kultury hierarchicznej. Oznacza to, że stabilność i kontrola działań w tych sądach były ważne, jednakże porównywalnie ważne było takie zarządzanie organizacją, aby osiągać wymierne sukcesy bez utraty reputacji.

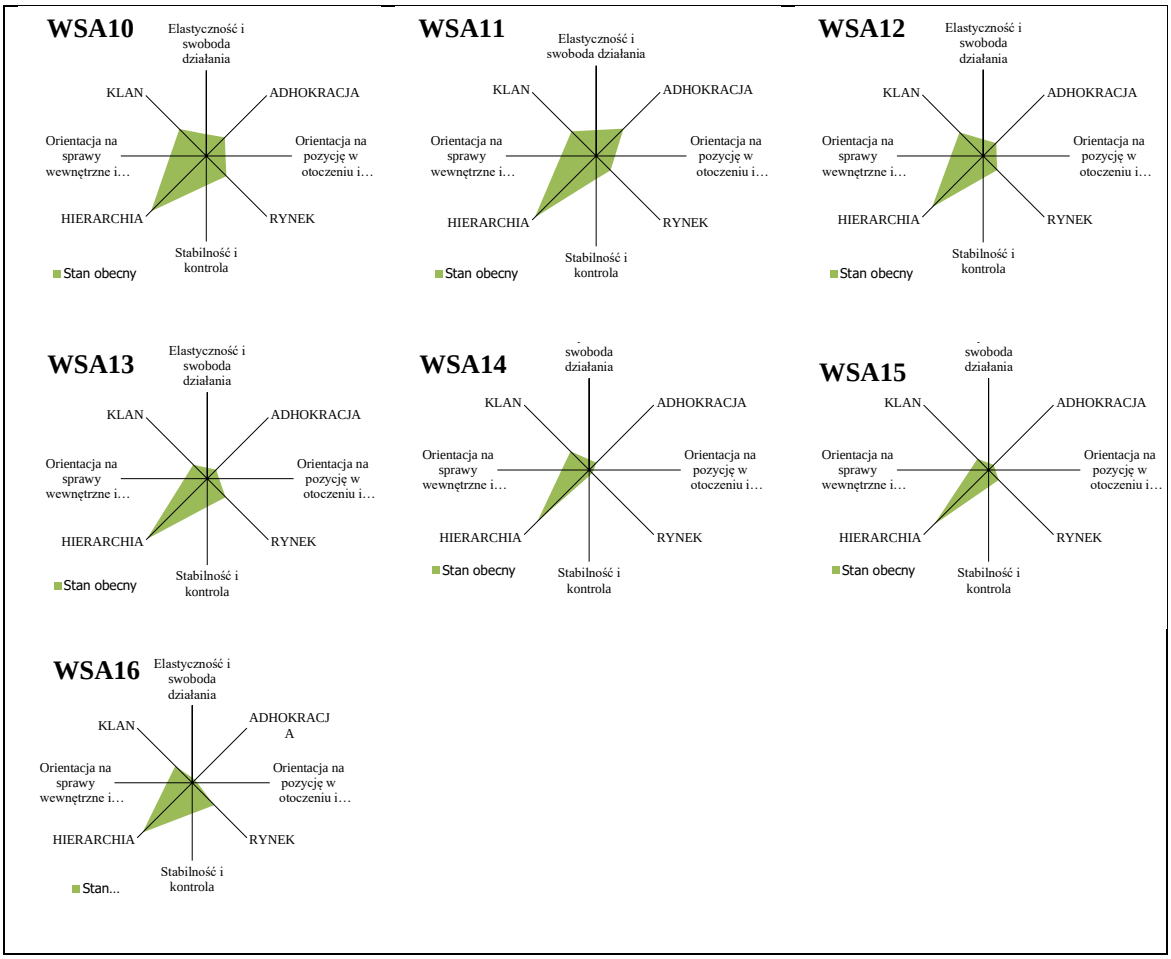

WSA1
WSA2
WSA3
WSA4
WSA5
WSA6
WSA7
WSA8
WSA9
WSA10
WSA11
WSA12
WSA13
WSA14
WSA15
Elastyczność i swoboda działania
ADHOKRACJA
Orientacja na pozycję w otoczeniu i…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy wewnętrzne i…
KLAN
Stan...



Rysunek 4.3. Wymiar kultury organizacyjnej „przywództwo w organizacji" w wojewódzkich sądach administracyjnych
Źródło: opracowanie własne.

Różnice widoczne są również w wymiarze „zarządzanie pracownikami" (Rysunek 4.4). W sądzie WSA5 dominowały cechy kultury rynkowej, czyli rywalizacja, stawianie wysokich wymagań pracownikom i presja na osiągnięcie celów. Wyróżniały się również wyniki badań uzyskanych z sądu WSA7. Oprócz cech charakterystycznych dla kultury hierarchicznej (tj. bezpieczeństwo zatrudnienia, podporządkowanie przełożonym, przewidywalność i niezmienność stosunków) respondenci zauważali, że w sądzie tym występowały cechy kultury klanowej o dużym nasileniu, czyli istotne były również w nim praca zespołowa, zaangażowanie w działania i dążenie do powszechnej zgody.





Rysunek 4.4. Wymiar kultury organizacyjnej „zarządzanie pracownikami" w wojewódzkich sądach administracyjnych
Źródło: opracowanie własne.

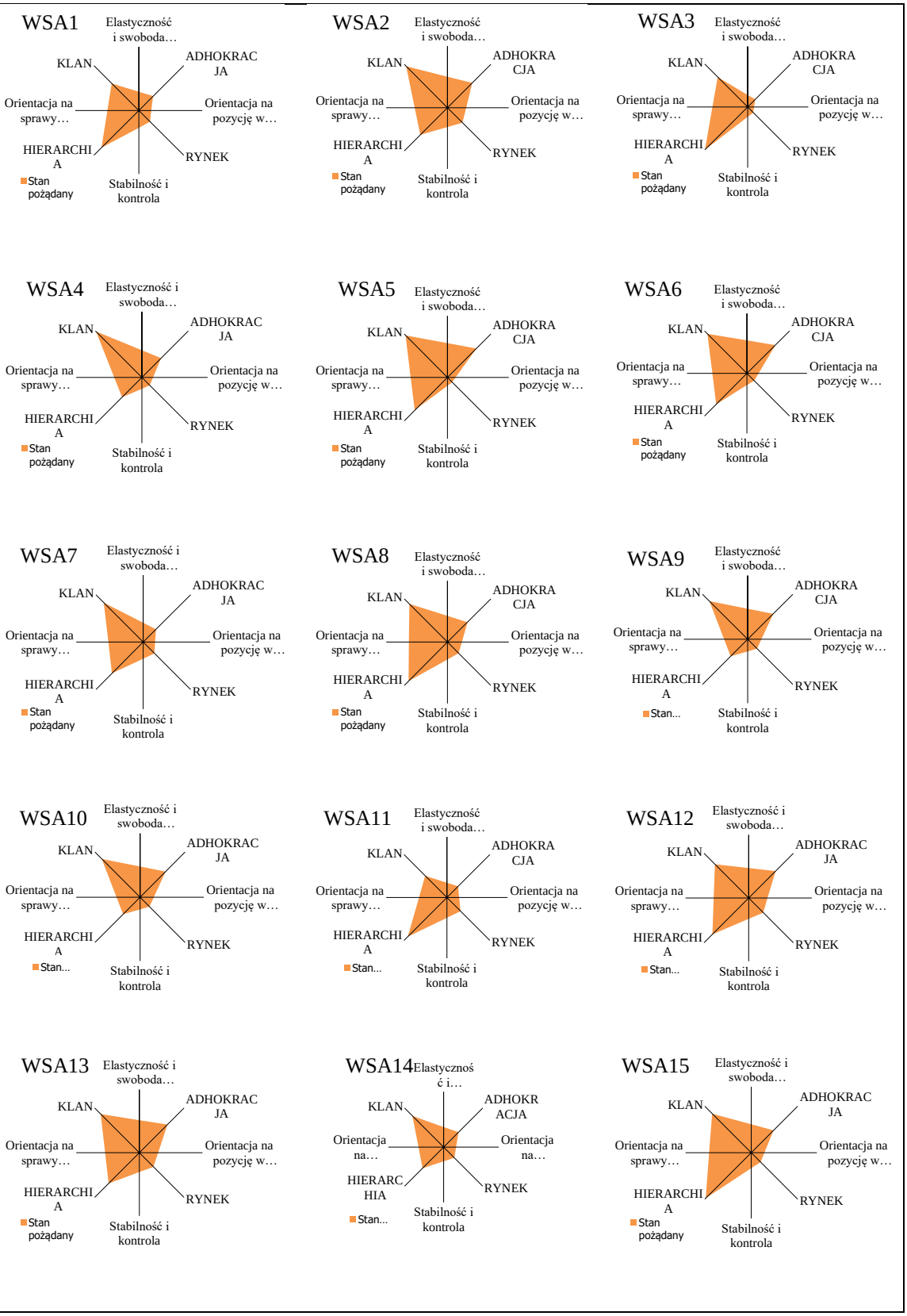
W pozostałych czterech wymiarach dominujące dla respondentów były cechy kultury hierarchicznej (wyjątek stanowi WSA5), czyli orientacja w organizacji na sprawy wewnętrzne i integrację, docenianie takich wartości, jak stabilność funkcjonowania organizacji, bezpieczeństwo zatrudnienia i sformalizowane zasady działania. Zestawienia graficzne wyników badań pozostałych czterech wymiarów kultury organizacyjnej w wojewódzkich sądach administracyjnych zostały zaprezentowane w załącznikach:

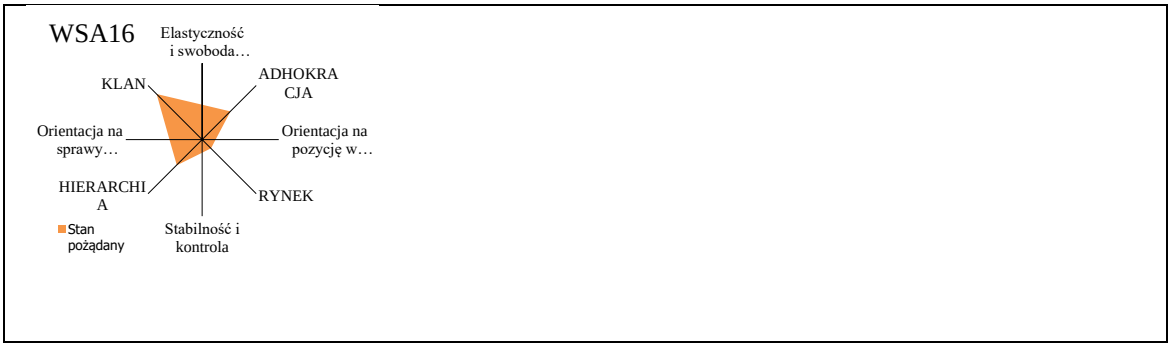
Załącznik 8. Wymiar kultury organizacyjnej „Charakterystyka organizacji".

Załącznik 9. Wymiar kultury organizacyjnej „Co zapewnia spójność?".

Załącznik 10. Wymiar kultury organizacyjnej „Na co kładzie się nacisk?"

Załącznik 11. Wymiar kultury organizacyjnej „Kryteria sukcesu".


WSA1
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan pożądany
WSA2
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan pożądany
WSA3
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan pożądany
WSA4
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan pożądany
WSA5
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan pożądany
WSA6
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan pożądany
WSA7
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan pożądany
WSA8
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan pożądany
WSA9
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan...
WSA10
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan...
WSA11
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan...
WSA12
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan...
WSA13
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan pożądany
WSA14
Elastyczność i…
ADHOKRACJA
Orientacja na…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na…
KLAN
Stan...
WSA15
Elastyczność i swoboda…
ADHOKRACJA
Orientacja na pozycję w…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan pożądany



Rysunek 4.5. Pożądany stan kultury organizacyjnej wojewódzkich sądów administracyjnych
Źródło: opracowanie własne.

W wynikach odnoszących się do oczekiwanego przez respondentów profilu kultury organizacyjne (stan pożądany) zauważalne było wśród respondentów pragnienie zmiany kultury organizacyjnej w kierunku kultury klanowej (Rysunek 4.5). Jest to kultura, podobnie jak hierarchiczna, zorientowana na sprawy wewnętrzne, ale członkowie mają większe szanse rozwoju osobistego i zawodowego oraz mogą korzystać z dużej niezależności i swobody działania.

4.2.2. Testy statystyczne dotyczące profili kultury organizacyjnej w wojewódzkich sądach administracyjnych

W niniejszym podrozdziale oraz w następnych częściach pracy z powodu braku rozkładów normalnych dla badanych zmienny analizy statystyczne zostały oparte o testy nieparametryczne. W pierwszym kroku przetestowano różnice pomiędzy aktualną a pożądaną kulturą organizacyjną w badanej grupie. W tym celu wykonano test znaków rangowanych Wilcoxona (Tabela 4.4).

Tabela 4.4. Porównanie kultury organizacyjnej w stanie obecnym a pożądanym

Kultura organizacyjna	Kultura obecna		Kultura pożądana		*Z*	*p*	*r*
	Me	*IQR*	*Me*	*IQR*			
Klan	10,00	17,83	35,00	15,63	–10,52	**<0,001**	–0,60
Adhokracja	4,17	13,33	21,25	15,83	–10,03	**<0,001**	–0,57
Rynek	18,33	17,17	9,92	10,83	–8,12	**<0,001**	–0,46
Hierarchia	59,92	34,17	27,58	20,42	–9,98	**<0,001**	–0,57

Źródło: opracowanie własne.

Wyniki testu okazały się istotne statystycznie. Z przedstawionych wartości wynika, że w sądach częściej, niż chcieliby respondenci, występowały takie cechy kultury organizacyjnej, jak rynek i hierarchia. Z kolei badani wskazywali na zbyt mało cech kultury organizacyjnej klanu i adhokracji.

Następnie przetestowano różnice w zakresie obecnej kultury organizacyjnej w zależności od grupy zawodowej (Hipoteza H: Istnieją różnice w zakresie identyfikowanej kultury organizacyjnej w sądach w zależności od grupy zawodowej) przy użyciu testu Kruskala-Wallisa. Wyniki analizy okazały się nieistotne statystycznie. Może to świadczyć o braku różnic w postrzeganiu kultury organizacyjne przez przedstawicieli różnych grup zawodowych wojewódzkich sądów administracyjnych biorących udział w badaniu. W zestawieniu zawarte zostały wyniki przeprowadzonej analizy (Tabela 4.5).

Tabela 4.5. Różnice w zakresie kultury organizacyjnej w zależności od grupy zawodowej

Kultura organizacyjna (obecna)	**Grupa zawodowa**	**średnia ranga**	***Me***	***IQR***	***H*(3)**	***p***	**η²**
Klan	Sędzia lub asesor sądowy (*n* = 17)	81,18	13,33	12,92	4,83	0,185	0,03
	Referendarz sądowy lub asystent sędziego (*n* = 27)	68,96	6,67	12,17			
	Kierownik lub pracownik sekretariatu wydziału (*n* = 41)	70,13	6,67	13,33			
	Inny pracownik sądu (*n* = 71)	86,32	13,33	21,67			
Adhokracja	Sędzia lub asesor sądowy (*n* = 17)	80,29	3,33	15,42	3,13	0,373	0,01
	Referendarz sądowy lub asystent sędziego (*n* = 27)	64,89	1,67	9,17			
	Kierownik lub pracownik sekretariatu wydziału (*n* = 41)	82,87	5,00	10,50			
	Inny pracownik sądu (*n* = 71)	80,73	5,00	15,00			
Rynek	Sędzia lub asesor sądowy (*n* = 17)	77,44	18,33	21,25	4,55	0,208	0,03
	Referendarz sądowy lub asystent sędziego (*n* = 27)	72,43	17,50	18,33			
	Kierownik lub pracownik sekretariatu wydziału (*n* = 41)	91,22	23,33	17,25			
	Inny pracownik sądu (*n* = 71)	73,72	17,50	18,33			
Hierarchia	Sędzia lub asesor sądowy (*n* = 17)	79,18	56,67	18,33	5,08	0,166	0,04
	Referendarz sądowy	96,00	70,00	30,83			

Kultura organizacyjna (obecna)	Grupa zawodowa	średnia ranga	*Me*	*IQR*	*H*(3)	*p*	η²
	lub asystent sędziego (*n* = 27)						
	Kierownik lub pracownik sekretariatu wydziału (*n* = 41)	74,16	56,67	30,00			
	Inny pracownik sądu (*n* = 71)	74,19	55,00	43,00			

Źródło: opracowanie własne.

4.2.3. Szkolenia i opinie o bezpieczeństwie informacji osób pracujących w wojewódzkich sądach administracyjnych

Sprawdzono, czy występuje związek pomiędzy bezpieczeństwem informacji a dojrzałością SZBI. W tym celu przeprowadzona została analiza korelacji rang *rho* Spearmana. Wyniki tej analizy są istotne statystycznie: r_s = 0,18; p = 0,027. Korelacja ta jest dodatnia i słaba, co oznacza, że im wyższy jest poziom dojrzałości SZBI, tym większe jest bezpieczeństwo informacji w organizacji.

Analogicznie sprawdzono, czy bezpieczeństwo informacji współwystępuje z kulturą organizacyjną w badanej grupie. Przeprowadzono więc analizy korelacji rang *rho* Spearmana. Wyniki analizy zostały przedstawione poniżej (Tabela 4.6).

Tabela 4.6. Korelacje wskaźników bezpieczeństwa informacji ze wskaźnikami kultury organizacyjnej

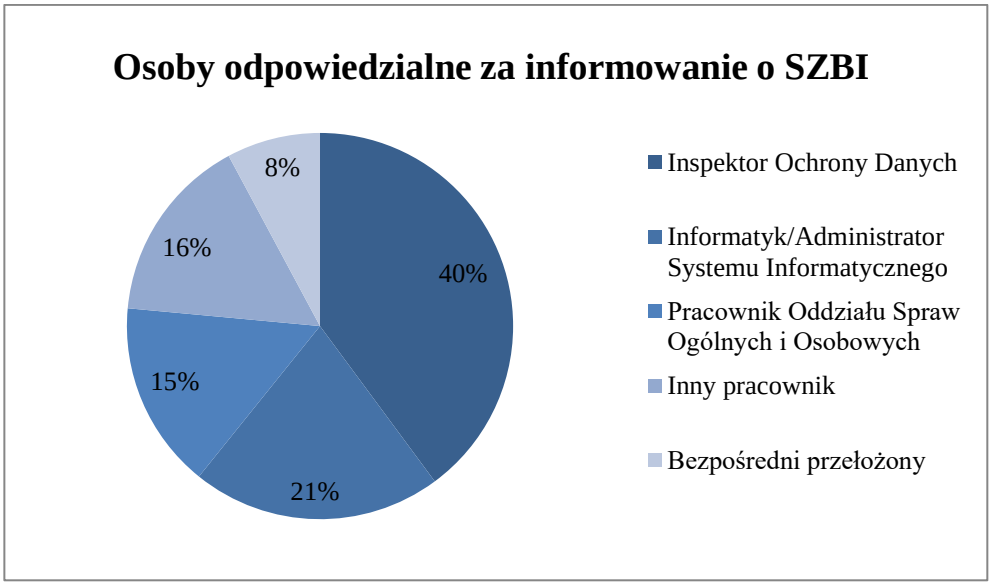
Kultura organizacyjna		Bezpieczeństwo informacji
Klan	*rho* Spearmana	**0,19**
	istotność	**0,015**
Adhokracja	*rho* Spearmana	0,05
	istotność	0,528
Rynek	*rho* Spearmana	–0,14
	istotność	0,084
Hierarchia	*rho* Spearmana	–0,01
	istotność	0,873

Źródło: opracowanie własne.

Analiza wykazała, że bezpieczeństwo informacji jest powiązane z kulturą klanową. Relacja ta jest dodatnia i słaba. Wynika z tego, że im większe nasilenie klanowej kultury odnotowano w sądzie, tym wyższy jest wskazywany przez

respondentów poziom bezpieczeństwa informacji. Pozostałe kultury organizacyjne nie są skorelowane z bezpieczeństwem informacji.

Pierwsze informacje o przepisach dotyczących bezpieczeństwa przetwarzanych informacji w sądzie w 40% respondenci uzyskali od inspektorów ochrony danych (Rysunek 4.6). Najczęściej odbywało się to w pierwszym dniu pracy w trakcie indywidualnego szkolenia przez upoważnionego pracownika (38%) lub w trakcie grupowego szkolenia (26%).



Rysunek 4.6. Osoby udzielające informacji o przepisach dotyczących bezpieczeństwa przetwarzanych informacji
Źródło: opracowanie własne.

Tabela 4.7 przedstawia rozkład uczestnictwa w szkoleniach dotyczących bezpieczeństwa informacji w zależności od osiągniętego poziomu dojrzałości SZBI.

Tabela 4.7. Uczestnictwo w szkoleniach w zależności od poziomu dojrzałości SZBI

		Poziom dojrzałości SZBI				
		1.	*2.*	*3.*	*5.*	Ogółem
Tak, szkolenia są regularne	Liczebność	11	17	34	3	65
	% z poziomu dojrzałość SZBI	36.7%	24.6%	64.2%	75.0%	41.7%
	% z ogółem	7.1%	10.9%	21.8%	1.9%	41.7%
Tak, szkolenie było jednorazowe	Liczebność	11	31	13	1	56
	% z poziomu dojrzałość SZBI	36.7%	44.9%	24,5%	25%	35,9%
	% z ogółem	7.1%	19.9%	8,3%	0,6%	35,9%
Nie	Liczebność	8	21	6	0	35

	% z poziomu dojrzałość SZBI	26.7%	30.4%	11.3%	0.0%	22.4%
	% z ogółem	5.1%	13.5%	3.8%	0.0%	22.4%
Ogółem	Liczebność	30	69	53	4	156
	% z ogółem	19.2%	44.2%	34.0%	2.6%	100.0%

Objaśnienie: % z poziomu dojrzałość SZBI – udział procentowy liczby respondentów o jednakowych odpowiedziach do liczby wszystkich respondentów z sądów o tym samym poziomie dojrzałości SZBI.
Źródło: opracowanie własne.

Zarówno w sądach, które osiągnęły trzeci i piaty poziom dojrzałości SZBI, odsetek respondentów uczestniczących regularnie w szkoleniach jest wysoki (odpowiednio 64,2% i 75%). Odsetek respondentów nieuczestniczących w szkoleniach w sądach, które osiągnęły trzeci poziom dojrzałości SZBI, wynosi 11,3%, a w sądzie o piątym poziomie dojrzałości 0%. W całej grupie respondentów nie uczestniczyło w szkoleniach dotyczących bezpieczeństwa informacji aż 22,4% osób.

4.2.4. Cechy kultury organizacyjnej wojewódzkich sądów administracyjnych a dojrzałość systemów zarządzania bezpieczeństwem informacji

Przetestowano związek pomiędzy wykazanymi w kwestionariuszu OCAI wymiarami kultury („Charakterystyka organizacji", „Przywództwo w organizacji", „Zarządzanie pracownikami", „Co zapewnia spójność w organizacji?", „Na co się kładzie nacisk?", „Kryteria sukcesu") a dojrzałością systemów zarządzania bezpieczeństwem informacji. W tym celu wykonano analizy korelacji rang *rho* Spearmana. Tylko w dwóch wymiarach: „Przywództwo w organizacji" (Tabela 4.10) i „Zarządzanie pracownikami" (Tabela 4.11) analizy potwierdziły statystycznie istotne korelacje pomiędzy cechami kultury a dojrzałością SZBI.

W dysertacji głównie przyjmuje się następującą interpretację uzyskanych wyników: im większe jest nasilenie cech danej kultury organizacyjnej, tym zmniejsza się lub zwiększa się poziom dojrzałości SZBI. Założenie to przyjmuje się ze świadomością, że w wykonanej analizie korelacji rang rho Spearmana badane było jedynie współwystępowanie zmiennych (bez związku przyczynowo-skutkowego), zatem poprawna może być interpretacja w drugim kierunku: im wyższy lub niższy był poziom dojrzałości SZBI, tym większe było nasilenie cech danej kultury organizacyjnej. Przyjęta w dysertacji interpretacja wynikała z przeprowadzonej analizy literatury oraz sprzyjała osiągnięciu celu praktycznego prowadzonych badań, tj. wyodrębnienia cech kultury organizacyjnej mających potencjalny związek

z dojrzałością systemów zarządzania bezpieczeństwem informacji. Ponadto, wynikające z ograniczeń doboru próby, przedstawione w tym podrozdziale wyniki opisują występowanie zjawisk w badanej próbie bez możliwości uogólnienia na całą populację.

Tabela 4.8. Korelacje wskaźników wymiaru kultury organizacyjnej „Przywództwo w organizacji" z dojrzałością SZBI

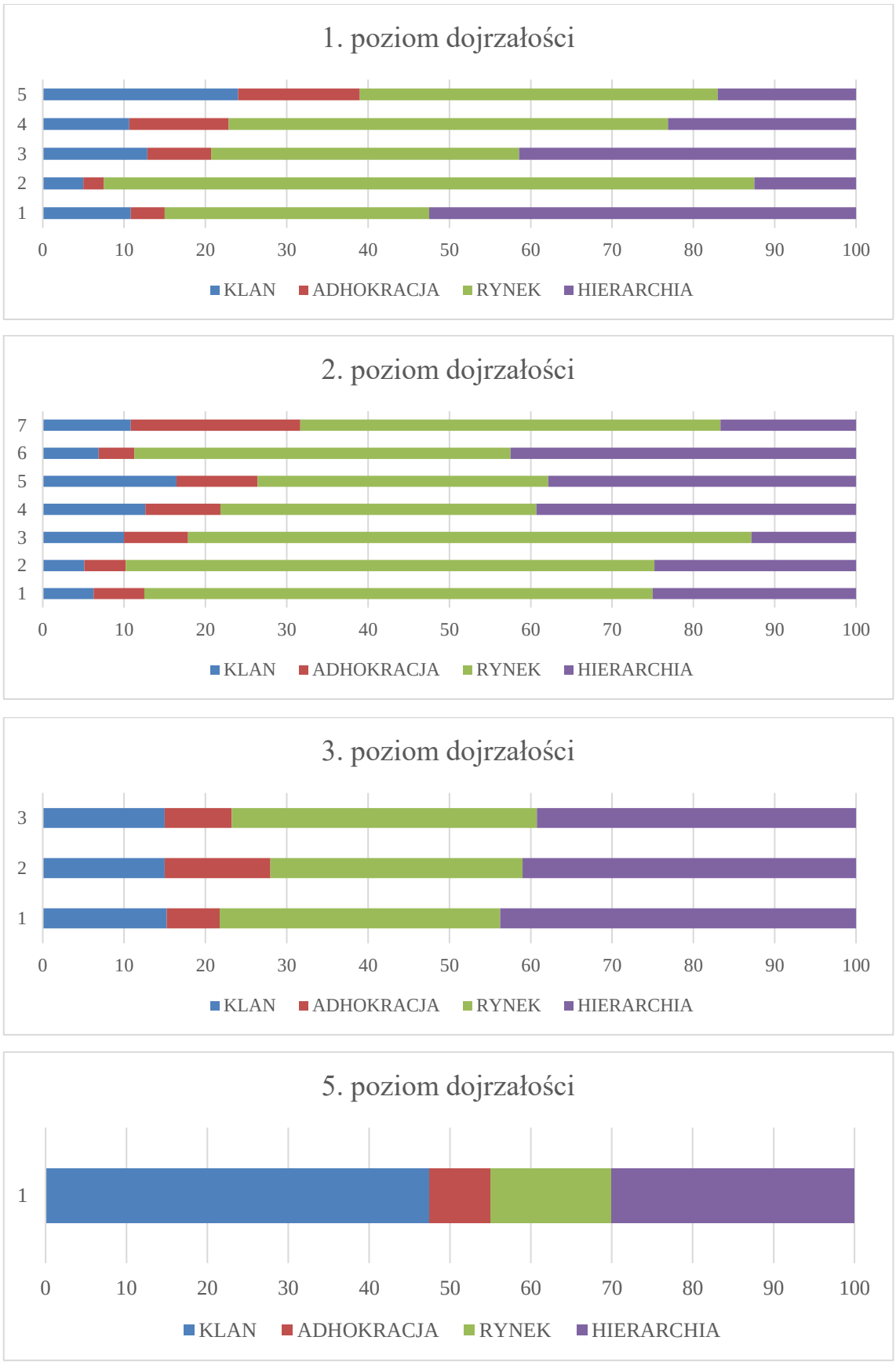
Przywództwo w organizacji		Dojrzałość SZBI
Klan	*rho* Spearmana	0,157
	Istotność	0,051
Adhokracja	*rho* Spearmana	–0,043
	Istotność	0,596
Rynek	*rho* Spearmana	**–0,208**
	Istotność	**0,009**
Hierarchia	*rho* Spearmana	**0,211**
	Istotność	**0,008**

Źródło: opracowanie własne.

Analiza wykazała istotną statystycznie, ujemną korelację pomiędzy dojrzałością SZBI a przywództwem w organizacji, utożsamianym ze stanowczością, ekspansywnością, orientacją na wyniki. Są to cechy rynkowej kultury organizacyjnej. Wynika z tego, że w sądach, w których dominuje styl przywództwa charakterystyczny dla profilu kultury rynkowej, maleje poziom dojrzałości SZBI.

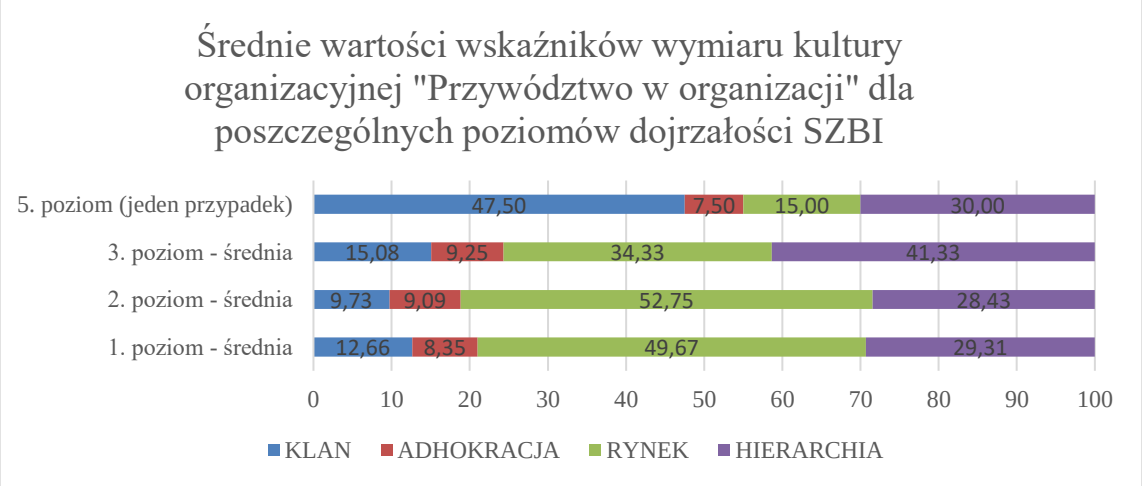
Analiza wykazała również istotną statystycznie, dodatnią korelację pomiędzy dojrzałością SZBI a przywództwem w organizacji, utożsamianym z koordynowaniem, sprawnym organizowaniem, stwarzaniem harmonijnych warunków do osiągania dobrych wyników. Są to cechy stylu przywództwa charakterystyczne dla hierarchicznej kultury organizacyjnej. Oznacza, to, że koordynowanie, sprawne organizowanie i stabilne warunki funkcjonowania organizacji sprzyjają dojrzałości SZBI. Pozostałe korelacje okazały się nieistotne statystycznie. Nie można zatem wnioskować związku innych stylów przywództwa z dojrzałością SZBI.

Dodatkowo dla wymiaru „Przywództwo w organizacji" przeprowadzono analizę profili kultur organizacyjnych dla wszystkich sądów w podziale na grupy według poziomów dojrzałości SZBI (Rysunek 4.7).



Rysunek 4.7. Profile kultury organizacyjnej dla wymiaru „Przywództwo w organizacji" w podziale na grupy według osiągniętej dojrzałości SZBI w wojewódzkich sądach administracyjnych
Źródło: opracowanie własne.

W wymiarze „Przywództwo w organizacji” w 50% badanych sądów dominującymi cechami były te przypisywane kulturze rynkowej. W sądzie, który uzyskał najwyższy poziom dojrzałości, respondenci wskazywali jako dominujące te cechy, które dotyczą kultury klanowej. W pozostałych sądach dominowały cechy kultury hierarchicznej.



Rysunek 4.8. Średnie wartości wskaźników wymiaru kultury organizacyjnej „Przywództwo w organizacji” dla poszczególnych poziomów dojrzałości SZBI
Źródło: opracowanie własne.

W sądach, które osiągnęły poziom dojrzałości 1. oraz 2. cechy kultury rynkowej były widoczne przez respondentów jako dominujące (Rysunek 4.8). W sądach, które osiągnęły poziom dojrzałości 3., dominowały cechy kultury hierarchicznej i były silniej niż w sądach o poziomie dojrzałości SZBI 1. i 2. widoczne cechy kultury klanowej. W sądzie, który uzyskał najwyższy poziom dojrzałości, dominowały cechy kultury klanowej.

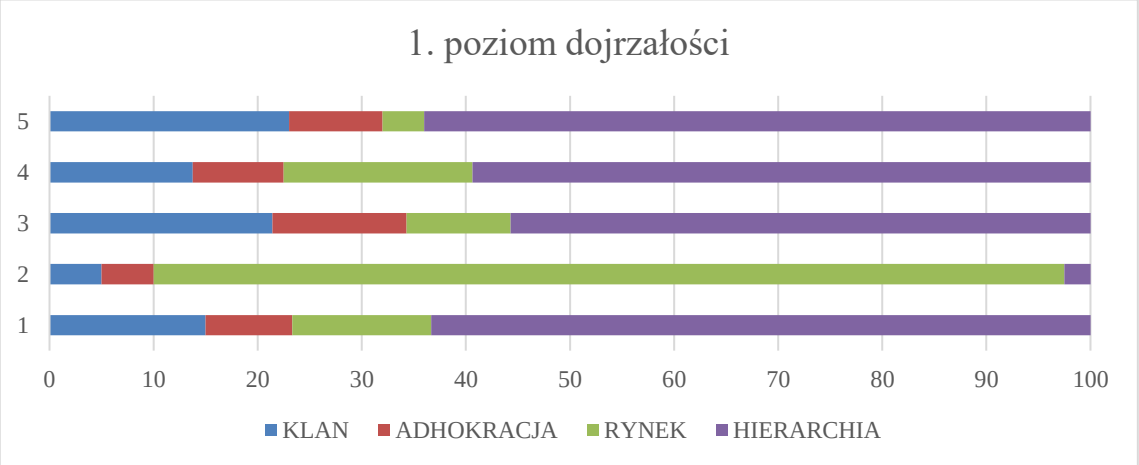
Tabela 4.9. Korelacje wskaźników wymiaru kultury organizacyjnej „Styl zarządzania” z dojrzałością SZBI

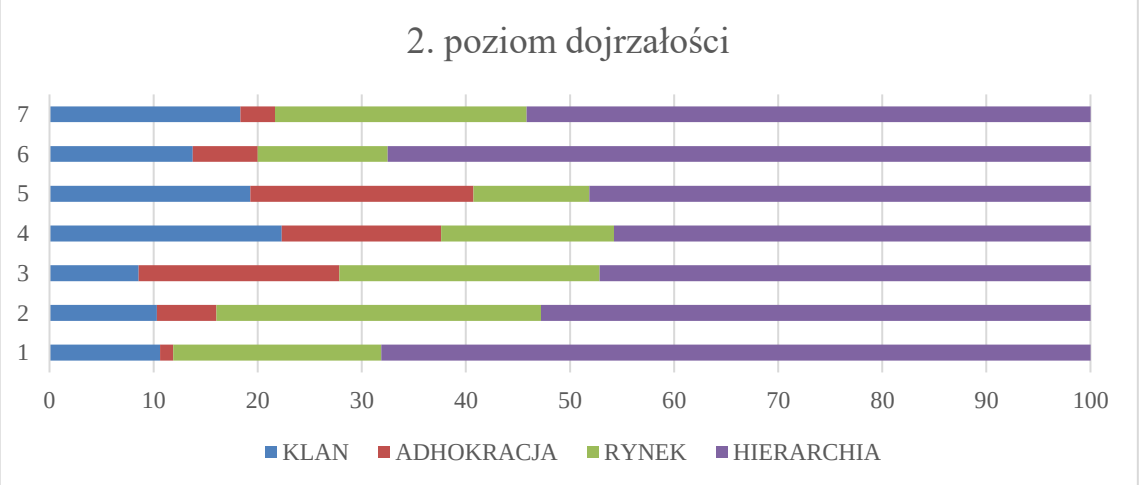
Styl zarządzania		Dojrzałość SZBI
Klan	*rho* Spearmana	**0,172**
	istotność	**0,032**
Adhokracja	*rho* Spearmana	–0,037
	istotność	0,649
Rynek	*rho* Spearmana	–0,107
	istotność	0,184
Hierarchia	*rho* Spearmana	0,037
	istotność	0,642

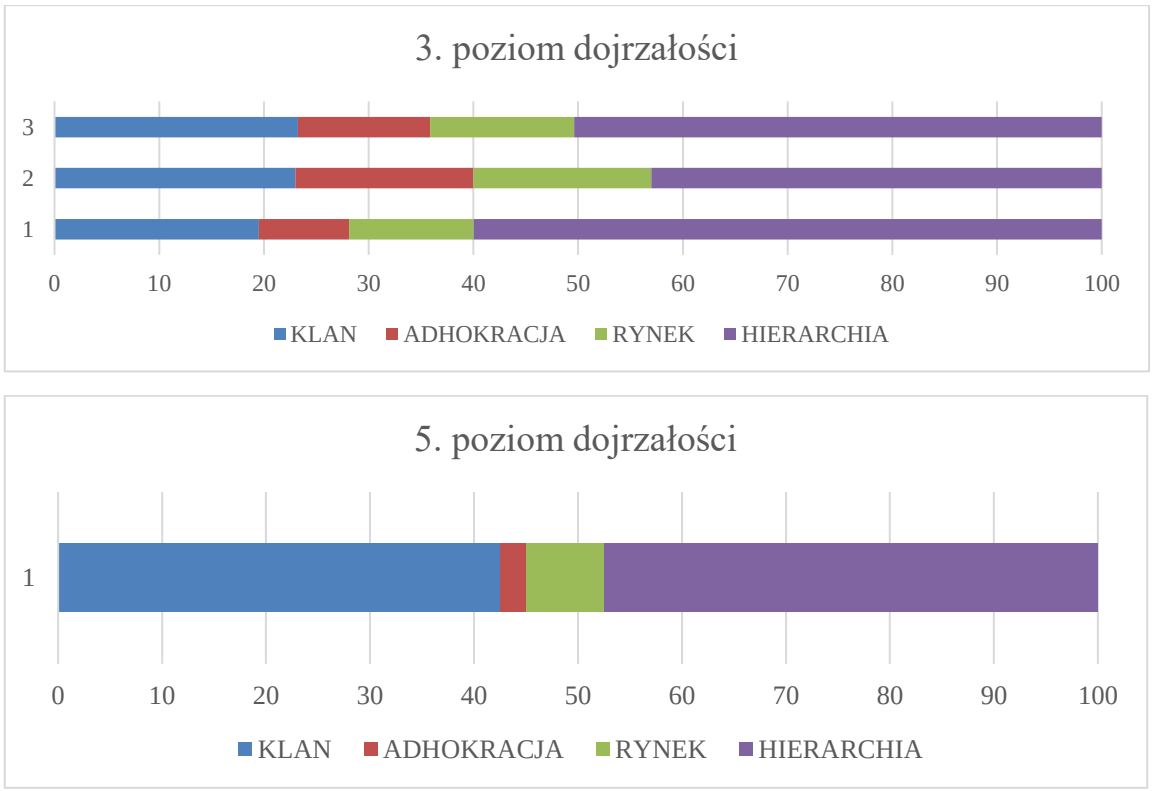
Źródło: opracowanie własne.

Analiza wykazała istotną statystycznie, dodatnią korelację pomiędzy dojrzałością SZBI a stylem zarządzania, w którym to preferuje się pracę zespołową, dąży do powszechnej zgody i uczestnictwa. Są to cechy stylu zarządzania charakterystyczne dla klanowej kultury organizacyjnej. Oznacza to, że współpraca, zaangażowanie i dzielenie się doświadczeniem oraz wiedzą mogą wpływać korzystnie na dojrzałość SZBI. Pozostałe korelacje okazały się nieistotne statystycznie. Nie można zatem wnioskować wpływu innych stylów zarządzania na dojrzałość SZBI.

Dodatkowo dla wymiaru „Styl zarządzania" przeprowadzono analizę profili kultur organizacyjnych dla wszystkich sądów w podziale na grupy według poziomów dojrzałości SZBI (Rysunek 4.9).

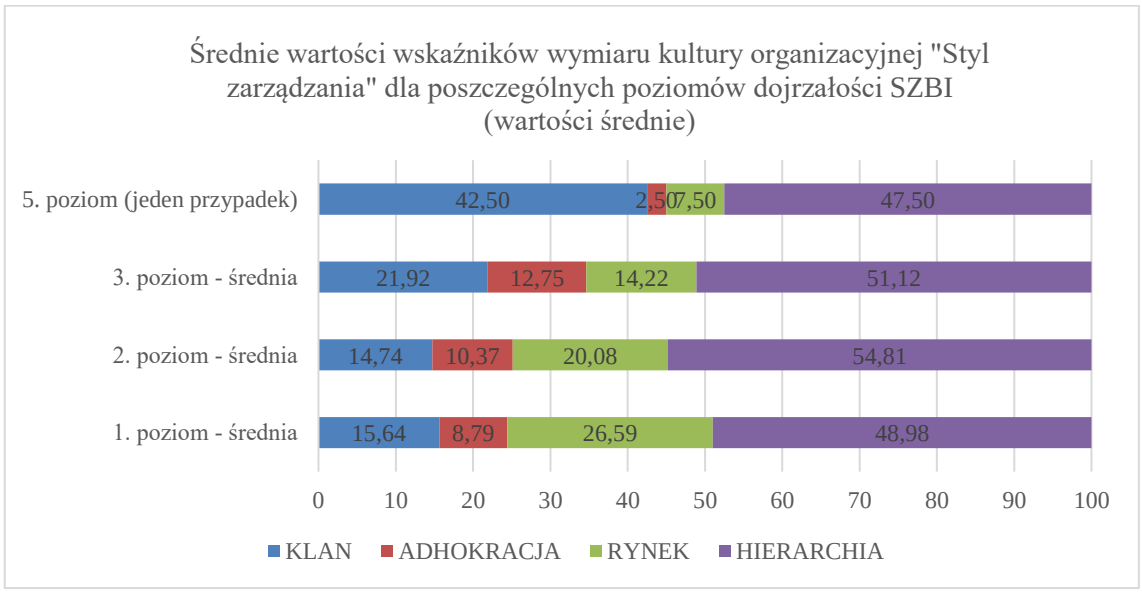






Rysunek 4.9. Profile kultury organizacyjnej dla wymiaru „Styl zarządzania" w podziale na grupy według osiągniętej dojrzałości SZBI w wojewódzkich sądach administracyjnych
Źródło: opracowanie własne.

We wszystkich (z wyjątkiem jednego WSA5) sądach dominującą kulturą organizacyjną w wymiarze „Styl zarządzania" jest hierarchia. Różnice występowały w odniesieniu do drugiej po dominującej kulturze organizacyjnej (Rysunek 4.10)



Rysunek 4.10. Średnie wartości wskaźników wymiaru kultury organizacyjnej „Przywództwo w organizacji" dla poszczególnych poziomów dojrzałości SZBI
Źródło: opracowanie własne.

W sądach, które osiągnęły poziom dojrzałości 1. oraz 2., cechy kultury rynkowej dla wymiaru „Styl zarządzania" były widoczne jako drugie, za cechami kultury hierarchicznej. W sądach, które osiągnęły poziom dojrzałości 3. oraz 5. (pojedynczy sąd o najwyższym stopniu dojrzałości) cechy kultury klanowej były widoczne jako drugie, za cechami kultury hierarchicznej.

4.3. Wyniki badania dokumentów dotyczących systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych

Rezultatem badania dokumentów było określenie poziomu dojrzałości SZBI osiągniętego przez poszczególne wojewódzkie sądy administracyjne. Przy ocenie dojrzałość SZBI, oprócz odpowiedzi na pytania znajdujące się w liście kontrolnej do analizy formalnej dokumentów SZBI, zostały uwzględnione odpowiedzi na trzy pytania zadane podczas wywiadów przeprowadzonych z dyrektorami sądów (narzędzie opisano w podrozdziale 3.6.2). Proces ten wiązał się z przekształceniem danych jakościowych w ilościowe[425]. kreślone poziomy dojrzałości zostały zaprezentowane w tabeli (Tabela 4.10).

Tabela 4.10. Zestawienie uzyskanej liczby punktów przez poszczególne WSA w badaniu dokumentów dotyczących Systemu Zarządzania Bezpieczeństwem Informacji oraz informacja o uzyskanym poziomie dojrzałości SZBI

WSA	2. poziom	3. poziom	4. poziom	5. poziom	POZIOM DOJRZAŁOŚCI
WSA1	16	3	2	1	2
WSA2	17	2	0	2	2
WSA3	15	4	2	0	1
WSA4	17	2	0	0	2
WSA5	13	1	0	0	1
WSA6	15	4	1	0	1
WSA7	**17**	**8**	**4**	**3**	**5**
WSA8	17	8	3	2	3
WSA9	16	7	0	1	3
WSA10	17	5	1	3	2
WSA11	16	5	1	1	2
WSA12	16	7	3	1	3
WSA13	13	0	0	0	1

[425] K. Kolasińska-Morawska, op. cit., s. 30.

WSA	2. poziom	3. poziom	4. poziom	5. poziom	POZIOM DOJRZAŁOŚCI
WSA14	15	5	1	3	1
WSA15	17	6	4	3	2
WSA16	16	3	1	0	2

Źródło: opracowanie własne.

W pięciu sądach dojrzałość zarządzania była zdiagnozowana na 1. poziomie. Procesy związane z zarządzaniem bezpieczeństwem informacji w mniejszym lub większym stopniu osiągały swój cel. Wstępne działania zostały podjęte, jednakże istniały luki i pewne obszary zarządzania bezpieczeństwem informacji nie były uregulowane. Przepisy nie były aktualizowane lub działania w tym zakresie nie były przeprowadzane regularnie. Najliczniejsza grupa składająca się z siedmiu sądów osiągnęła 2. poziom dojrzałości zarządzania bezpieczeństwem informacji. W tych organizacjach procesy składające się na SZBI osiągały swój cel poprzez zastosowanie podstawowego, ale kompletnego zestawu działań. Procesy były zarządzane, miało miejsce planowanie i pomiar wydajności procesów, jednakże nie w sposób znormalizowany. W trzech sądach dojrzałość SZBI osiągnęła 3. Poziom – oznacza to, że procesy działały w znacznie bardziej uporządkowany sposób niż na poziomach niższych. WSA7 uzyskał najwyższy 5. poziom dojrzałości – procesy związane ze SZBI osiągały swój cel, były dobrze zdefiniowane, ich wydajność była mierzona w celu poprawy i ciągłego doskonalenia.

4.4. Wyniki triangulacji metod badawczych

Stosując się do zasad równoległej strategii triangulacyjnej metod badawczych, w niniejszym podrozdziale przedstawiono wyniki przeprowadzonych badań w postaci zestawień i porównań wyników analizy danych jakościowych i ilościowych.

4.4.1. Identyfikacja dominujących cech kultury organizacyjnej w wojewódzkich sądach administracyjnych – pierwszy cel przeprowadzonych badań

Pierwszym celem poznawczym prowadzonych badań była identyfikacja dominujących cech kultury organizacyjnej w wojewódzkich sądach administracyjnych. Badanie ilościowe przeprowadzone za pomocą kwestionariusza OCAI wskazało cechy kultury hierarchicznej jako dominujące w 15 na 16 badanych sądach. Tylko w jednym sądzie dominującym profilem kultury organizacyjnej była kultura rynkowa.

Dominację cech kultury hierarchicznej potwierdzają również badania prowadzone w nurcie interpretatywnym. Wypowiedzi dyrektorów świadczą o tym, że wojewódzkie sądy administracyjne są organizacjami z jasno zdefiniowanymi strukturami, procedurami i rolami. Zaangażowanie kierownictwa polega na organizowaniu i kontrolowaniu procesów, tak aby sądy funkcjonowały stabilnie i zgodnie z wymaganiami prawnymi. W wypowiedziach brakowało odniesień do zewnętrznych interesariuszy, uwaga dyrektorów była skupiona na koordynowaniu działań pracowników, co świadczy o orientacji na sprawy wewnętrzne organizacji i integrację. Potwierdza to również przedstawione zestawienie słów (Tabela 4.12), które miały wysoki wskaźnik częstotliwości występowania w treści wypowiedzi dyrektorów sądów.

Tabela 4.12. Częstotliwość występowania wybranych słów w wywiadach z dyrektorami wojewódzkich sądów administracyjnych

	Słowo	Częstotliwość występowania słowa	Udział słowa w treści wywiadów %	Liczba wywiadów, w których występowało słowo	Udział słowa w liczbie wywiadów %
1	pracownik	139	2,50	15	93,75
2	prezes	113	2,03	16	100,00
3	zarządzenie	89	1,60	11	68,75
4	obowiązek	57	1,02	9	56,25
5	procedury	51	0,92	11	68,75
6	kierownik	50	0,90	10	62,50
7	kierownictwo	48	0,86	12	75,00
8	ryzyko	47	0,84	6	37,50
9	zarządzać	41	0,74	13	81,25
10	dyrektor	40	0,72	9	56,25

Źródło: opracowanie własne z wykorzystaniem programu MAXQDA.

Na podstawie przeprowadzonej analizy statystycznej nie można było stwierdzić różnic w zakresie kultury organizacyjnej w sądach w zależności od grupy zawodowej. Oznacza to, że sformułowana hipoteza badawcza została zdyskonfirmowana.

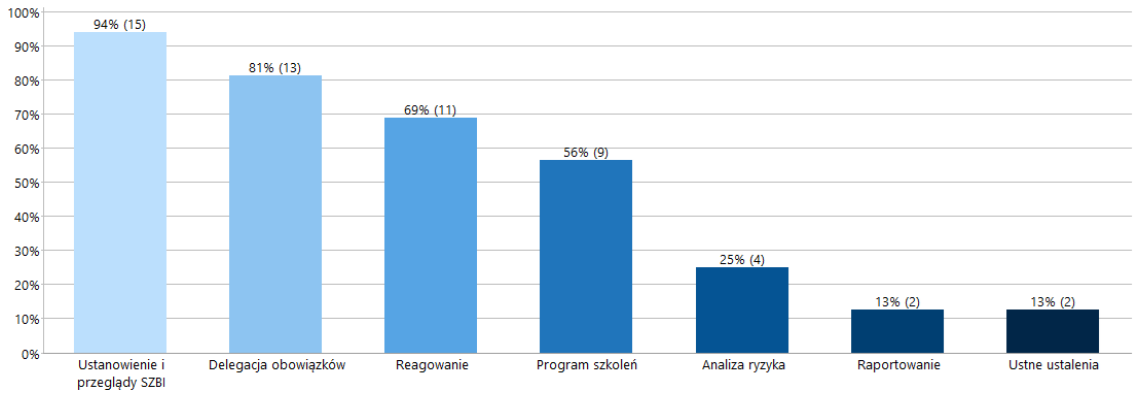
4.4.2. Rozpoznanie i analiza istniejącego stanu systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych – drugi cel przeprowadzonych badań

Następnym celem poznawczym było rozpoznanie i analiza istniejącego stanu systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych. W trakcie analizy treści transkrypcji wywiadów, podczas procesu

kodowania, wyodrębniono następujące działania najwyższego kierownictwa podejmowane w celu zapewnienia bezpieczeństwa informacji:

1. Ustanowienie i przeglądy SZBI – najwyższe kierownictwo było zaangażowane w ustanowienie SZBI i koordynowanie przeglądów SZBI.
2. Delegacja obowiązków – najwyższe kierownictwo zdefiniowało role i obowiązki dotyczące zarządzania bezpieczeństwem informacji w sądzie.
3. Reagowanie – najwyższe kierownictwo podejmowało działania w sprawach dotyczących bezpieczeństwa informacji, np. nadzór nad realizacją SZBI, modyfikacje procedur w wyniku zaistniałych incydentów, zapewnianie środków finansowych.
4. Raportowanie – najwyższe kierownictwo ustanowiło wymogi cyklicznych raportów z przeglądów, audytów SZBI oraz przeprowadzonych analiz ryzyka związanych z bezpieczeństwem informacji.
5. Program szkoleń – najwyższe kierownictwo wprowadziło obowiązek uczestnictwa w szkoleniach uświadamiających zagrożenia związane z bezpieczeństwem informacji.
6. Ustne ustalenia – najwyższe kierownictwo koordynowało utrzymanie SZBI za pomocą komunikacji werbalnej.

Poniżej przedstawiona została liczba wywiadów, w których poruszone były wyodrębnione działania najwyższego kierownictwa związane ze SZBI (Rysunek 4.11).



Rysunek 4.11. Podejmowane działania najwyższego kierownictwa wskazane podczas wywiadów z dyrektorami WSA
Źródło: opracowanie własne.

Z danych uzyskanych z ankiet wynika, że osobami odpowiedzialnymi za informowanie o funkcjonujących zasadach dotyczących bezpieczeństwa

przetwarzanych informacji są przede wszyscy inspektorzy ochrony danych (40%) oraz administratorzy systemów informatycznych (21%). Potwierdzają to również dane z wywiadów z dyrektorami sądów, najczęściej wymienianymi przez dyrektorów przepisami, które wpłynęły na SZBI jest RODO (w 14 sądach). W trakcie rozmów podkreślana była również konieczność ochrony danych osobowych oraz rola inspektora ochrony danych w procesach z związanych bezpieczeństwem przetwarzanych informacji.

Żaden z sądów nie poddał swojego systemu zarządzania bezpieczeństwem informacją certyfikacji ISO/IEC 27001. O tym, że wymagania normy były uwzględniane w wewnętrznych regulacjach informowali dyrektorzy czterech sądów (Tabela 4.1). Podstawą tworzenia SZBI w wojewódzkich sądach administracyjnych było przede wszystkim zachowanie zgodności z przepisami prawa polskiego i europejskiego:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L z 2016 r. Nr 119, str. 1 z późn. zm.).
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r., poz. 2247).

4.4.3. Ocena dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych – trzeci cel przeprowadzonego badania

Praktycznym celem badawczym była ocena dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych. W celu jej przeprowadzenia utworzone zostało narzędzie badawcze (Podrozdział 3.6.2), które na podstawie analizy statystycznej zostało uznane za rzetelne. Badanie wykazało, że pięć sądów osiągnęło pierwszy poziom dojrzałości, siedem sądów poziom drugi, trzy sądy poziom trzeci oraz jeden sąd poziom najwyższy, piąty. Każdy osiągnięty poziom

dojrzałości wiązał się z podjęciem działań odpowiadających danemu poziomowi oraz działań z poprzedzających poziomów (Tabela 4.13).

Tabela 4.13. Kontrolowane działania z związku z przeprowadzoną oceną dojrzałości SZBI

Poziomy dojrzałości	*Działania w związku ze SZBI*
Poziom 2. *powtarzalny*	Ustanowiono SZBI w postaci formalnego dokumentu . Określono, jakim informacjom należy zapewnić bezpieczeństwo. Uwzględniono zewnętrzne przepisy prawne. Uwzględniono wewnętrzne regulacje. Wskazano techniki wykorzystywane do zapewnienia bezpieczeństwa informacji. Określono interesariuszy SZBI. Określono zasady wymiany informacji między organizacją a innymi organizacjami. Umieszczono zapisy o zasadach przydzielania i odbioru uprawnień do systemów informatycznych. Podjęto działania w związku ze zmianą wymogów. Ustanowiono dodatkowe regulacje dotyczące bezpieczeństwa danych osobowych przetwarzanych w sądzie. Ustanowiono procedury zgłaszania incydentów dotyczących bezpieczeństwa informacji i prywatności. Opisano plan ciągłości działania. Ustanowiono procedury odzyskiwania kluczowych systemów. Kierownictwo wskazało osobę (lub osoby) do wdrożenia, monitorowania zmian w regulacjach wewnętrznych i przepisach prawa dotyczących SZBI oraz aktualizowania SZBI. Zdefiniowano role i obowiązki dotyczące zarządzania bezpieczeństwem informacji. Wskazano role z podziałem na osoby odpowiedzialne za wykonanie procesu (R) oraz osoby sprawujące nadzór nad tym procesem (A). Informowanie interesariuszy o ustanowionym SZBI i jego zmianach.
Poziom 3. *zdefiniowany*	Zintegrowano planowanie, projektowanie, wdrażanie i monitorowanie procedur bezpieczeństwa informacji i prywatności. Wskazano częstotliwość uczestnictwa w obowiązkowych szkoleniach uświadamiających zagrożenia związane z bezpieczeństwem informacji. Sformułowano plan postępowania z ryzykiem w zakresie bezpieczeństwa informacji dostosowany do celów i struktury organizacyjnej. Wdrożono plan postępowania z ryzykiem w zakresie bezpieczeństwa informacji dostosowany do celów i struktury organizacyjnej. Zapewniono, że plan (postępowania z ryzykiem w zakresie bezpieczeństwa informacji) określa odpowiednie praktyki zarządzania i rozwiązania w zakresie bezpieczeństwa, biorąc pod uwagę zasoby, odpowiedzialność i priorytety, w zakresie zarządzania zidentyfikowanym ryzykiem bezpieczeństwa informacji. Ustanowiono sposób zarządzania ryzykiem związanym z bezpieczeństwem informacji. Zarządzanie ryzykiem związanym z bezpieczeństwem informacji jest składową zarządzania ryzykiem działalności organizacji. Określono sposób pomiaru skuteczności praktyk dotyczących zarządzania bezpieczeństwem informacji.
Poziom 4. *zarządzany*	Udokumentowano dokonywanie przeglądów dokumentacji SZBI. Udokumentowano przeprowadzenie przeglądów skuteczności SZBI w zaplanowanych odstępach czasu. Udokumentowano audyty SZBI w zaplanowanych odstępach czasu. Udokumentowano regularne przeglądy SZBI przez najwyższe kierownictwo

Poziom 5. *optymalizowany*	Udokumentowano wkład najwyższego kierownictwa w utrzymanie SZBI. Wykazano zaangażowania najwyższego kierownictwa w optymalizację SZBI. Zaistniała kultura bezpieczeństwa informacji i danych osobowych w organizacji.

Źródło: opracowanie własne.

Ograniczeniem badania dojrzałości systemów zarządzania bezpieczeństwem informacją był brak możliwości zastosowania obserwacji uczestniczących w każdym z sądów w celu poznania działania procesów opisanych w badanych dokumentach. Kolejnym ograniczeniem wynikającym z natury badanych dokumentów był limitowany czas badania w związku z koniecznością analizy dokumentów w obecności pracownika danego sądu.

W wywiadach dyrektorzy wojewódzkich sądów administracyjnych opisywali działania podejmowane przez najwyższe kierownictwo, mające na celu utrzymanie SZBI. Poniżej przedstawione zostało zestawienie tych działań z poziomem dojrzałości osiągniętym przez SZBI (Tabela 4.14).

Tabela 4.14. Częstotliwość udzielania w wywiadach informacji dotyczących poszczególnych działań w zestawieniu z osiągniętymi poziomami dojrzałości SZBI

	POZIOM DOJRZAŁOŚCI = 1	POZIOM DOJRZAŁOŚCI = 2	POZIOM DOJRZAŁOŚCI = 3	POZIOM DOJRZAŁOŚCI = 5	Suma
Ustanowienie i przeglądy SZBI	5	6	3	1	15
Delegacja obowiązków	4	5	3	1	13
Ustne ustalenia	2				2
Program szkoleń	2	5	1	1	9
Analiza ryzyka	1	2		1	4
Reagowanie	3	6	1	1	11
Raportowanie		1		1	2
Σ SUMA	17	25	8	6	56
# N = Dokumenty	5 (31,3%)	7 (43,8%)	3 (18,8%)	1 (6,3%)	16 (100,0%)

Źródło: opracowanie własne.

Przedstawione informacje były zbierane podczas standaryzowanych, ale nieustrukturalizowanych wywiadów, tak więc brak w wypowiedziach informacji o podjętych działaniach nie oznacza braku tych działań w organizacji. Jednakże można przyjąć, że ich wystąpienie w wypowiedzi świadczyło o ważności tych działań dla respondenta i jego zaangażowaniu w te działania.

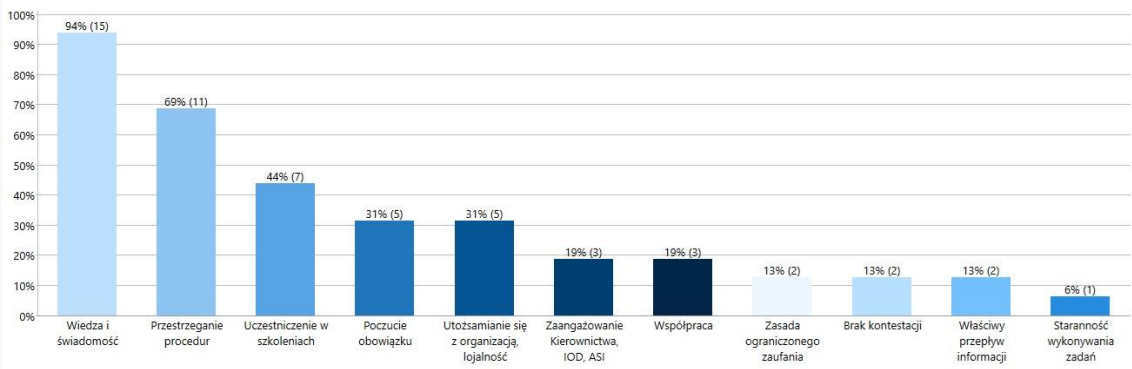
Z wypowiedzi dyrektora sądu, który uzyskał najwyższy stopień dojrzałości, wynika, że według niego podstawą powstania dojrzałego SZBI jest przeprowadzanie systematycznych analiz ryzyka i audytów dotyczących bezpieczeństwa informacji w celu doskonalenia SZBI. Według dyrektora istotne było zaangażowanie prezesa sądu, dobry przepływ informacji pomiędzy najwyższym kierownictwem a pracownikami oraz system szkoleń uświadamiających zagrożenia. Sposób wysławiania się, trzymanie się tematu rozmowy i najdłuższy czas trwania wywiadu (1 godzina i 50 min) świadczył o

dużym zaangażowaniu ze strony dyrektora tego sądu i wiedzy na temat procesów informacyjno-decyzyjnych dotyczących SZBI.

4.4.4. Wyodrębnienie cech kultury organizacyjnej mających potencjalny związek z dojrzałością systemów zarządzania bezpieczeństwem informacji – czwarty cel przeprowadzonych badań

Ostatnim celem badawczym było wyodrębnienie cech kultury organizacyjnej mających związek z dojrzałością systemów zarządzania bezpieczeństwem informacji. W przeprowadzonej analizie statystycznej, której ograniczeniem był brak doboru próby zgodnie z metodą reprezentacyjną doboru próby, zidentyfikowane zostały cechy kultury organizacyjnej pozytywnie wpływające na dojrzałość SZBI, tj.: koordynowanie i sprawne organizowanie działań, stabilne i harmonijne warunki funkcjonowania organizacji, współpraca, powszechna zgoda, zaangażowanie, dzielenie się doświadczeniem i wiedzą pomiędzy pracownikami. Dojrzałości SZBI sprzyjała orientacja na sprawy wewnętrzne w organizacji i integracja współpracowników. Zidentyfikowano również cechy kultury negatywnie wpływające na dojrzałość SZBI. Są one związane ze stanowczością kierownictwa, z kładzeniem nacisku na ekspansywność organizacji i presją na osiąganie możliwie najlepszych wyników.

O czynnikach wpływających na dojrzałość SZBI można wnioskować także na podstawie analizy danych jakościowych otrzymanych z transkrypcji wywiadów. W procesie kodowania wyodrębnione zostały czynniki wpływające pozytywnie na kulturę bezpieczeństwa informacji (Rysunek 4.12).



Rysunek 4.12. Czynniki wpływające na kulturę bezpieczeństwa informacji wyodrębnione podczas wywiadów z dyrektorami WSA
Źródło: opracowanie własne.

W wywiadach najczęściej podkreślana była potrzeba ciągłego kształcenia w zakresie bezpieczeństwa informacji w związku z dynamicznym wzrostem zagrożeń.

Wiedza i świadomość oraz dzielenie się ze współpracownikami informacjami o możliwych zagrożeniach, według respondentów, zmniejszają ryzyko wystąpienia incydentów. Przestrzeganie wdrożonych procedur, brak ich kontestowania to zachowania, które sprzyjają bezpieczeństwu informacji. Dyrektorzy zauważali, że takie postawy, jak: pozytywne ustosunkowanie się do inicjatyw szkoleniowych, poczucie obowiązku, chęć współpracy oraz lojalność w stosunku do organizacji, miały korzystny wpływa na kulturę bezpieczeństwa informacji. Dostrzegana była również potrzeba zaangażowania kierownictwa w utrzymanie SZBI i właściwy przepływ informacji.

5. Dyskusja

W literaturze przedmiotu, poruszającej problemy dojrzałości systemów zarządzania bezpieczeństwem, zawarto między innymi wyniki badań, które realizowane były za pomocą narzędzi badawczych wykorzystujących dobre praktyki APO13 ujęte w COBIT 2019. W tych badaniach[426] organizacje uzyskiwały ocenę dojrzałości SZBI na poziomie drugim lub trzecim. Również w wojewódzkich sądach administracyjnych były to najczęściej osiągane poziomy dojrzałości. Aż w pięciu sądach SZBI był zdiagnozowany na niskim, pierwszym poziomie dojrzałości. Tylko jeden sąd uzyskał w badaniu poziom najwyższy, piąty. Głównym problemem w zarządzaniu bezpieczeństwem informacji w sądach o najniższym zdiagnozowanym poziomie był brak dostatecznego nadzoru najwyższego kierownictwa nad utrzymaniem i optymalizacją SZBI. Z ustaleń poczynionych w niniejszej dysertacji oraz analizy wyników innych badań[427] można wnioskować, że brak zaangażowania najwyższego kierownictwa może skutkować powstaniem SZBI o niskim poziomie dojrzałości i kultury organizacyjnej o niskim poziom egzekwowania istniejących polityk bezpieczeństwa.

Żaden WSA nie uzyskał dla swoich SZBI certyfikatu zgodności z normą ISO 27001, której wymagania zostały wskazane w przepisach krajowych[428] obowiązujących organizacje sektora publicznego. Same wymagania normy zostały, przynajmniej częściowo, wdrożone we wszystkich diagnozowanych sądach, jednakże żaden z niech nie przystąpił do oceny formalnej wdrożonych procedur. Z badań niemieckich organizacji[429] wynika, że czynnikami wpływającymi na brak certyfikowanego SZBI są wysokie koszty wdrożenia i braku silniej presji ze strony interesariuszy zewnętrznych, ustawodawców krajowych i najwyższego kierownictwa. Pomimo że wszystkie badane sądy mają tę samą strukturę i pełnią tę samą funkcję w polskim systemie sądowym, wyniki oceny dojrzałości systemów zarządzania bezpieczeństwem informacji były różne. Można przypuszczać, że zdiagnozowane różnice w dojrzałości SZBI związane

[426] Y. Megasyah, A. Arifnur, *Academic information system security audits using COBIT 5 framework domains APO12, APO13 and DSS05*, „Journal of Applied Engineering and Technological Science" 2020, Vol. 1(2), s. 124–135; P. Widharto, Z. Suhatman, R.F. Aji, *Measurement of information technology governance capability level: a case study of PT Bank BBS*, „TELKOMNIKA Telecommunication Computing Electronics and Control" 2022, Vol. 20, No. 2, s. 296–306.

[427] K.J. Knapp, T.E. Marshall, R.R. Kelly, F.F. Nelson, op. cit., s. 24–36.

[428] Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2024 r., poz. 773).

[429] M. Mirtsch, *Adoption*…, op. cit., s. 747–768.

były z cechami kultury organizacyjnej tych sądów. W opinii respondentów z piętnastu sądów dominujący był profil kultury hierarchicznej. Z badań przeprowadzonych w greckich organizacjach[430] wynika, że przewaga cech profilu kultury hierarchicznej jest charakterystyczna dla sektora publicznego i członkowie greckich organizacji postulowali zmianę dominującego profilu kultury organizacyjnej na kulturę klanową, na co wskazują również wyniki badań własnych ujęte w tej dysertacji, a dotyczące polskich organizacji. Badacze[431] wskazują, że hierarchiczny profil kultury organizacyjnej najskuteczniej sprzyja przestrzeganiu polityki bezpieczeństwa informacji przez pracowników. Z badania wojewódzkich sądów administracyjnych wynika, że identyfikowane przez respondentów cechy hierarchicznej kultury nie były jedynymi czynnikami wpływającym na dojrzałość systemu zarządzania bezpieczeństwem informacji. Oprócz istotności przestrzegania przepisów w kształtowania kultury bezpieczeństwa informacji ważne jest również pozytywne postrzeganie polityki bezpieczeństwa informacji funkcjonującej w organizacji. Nie bez znaczenia są również motywacje pracowników czy ich wewnętrzne przekonania do celowości postępowania zgodnie z przepisami[432]. Z badań literatury[433] można wnioskować, że kulturę bezpieczeństwa informacji, w związku z jej naturą, należy kultywować, a nie sztywno projektować. W organizacjach o cechach kultury klanowej zwraca się większą uwagę na osobiste zaangażowanie jej członków w podejmowane działania i współpracę. Sprzyja temu charakterystyczny dla kultury klanowej styl przywództwa, który opiera się na doradztwie i służeniu pomocą. Pracownicy WSA, który osiągnął najwyższy poziom dojrzałości SZBI, dostrzegali w swojej organizacji jako dominujące cechy kultury charakterystyczne zarówno dla profilu kultury hierarchicznej, jak i klanowej. Zatem można wnioskować, że połączenie cech tych dwóch profili kultur organizacyjnych przyczyniło się do powstania dojrzałego systemu zarządzania bezpieczeństwem

[430] P. Boufounou, M.D. Argyrou, *Changing the organizational culture to transform the economy: The case of Greece*, „Frontiers in Research Metrics and Analytics ", 2022, 7:1050544.

[431] H.-J. Kam, T. Mattson, D.J. Kim, *The "Right" Recipes for Security Culture: A Competing Values Model Perspective*, „Information Technology & People" 2021, Vol. 34 (5), s. 1490–1512; M. Karlsson, F. Karlsson, J. Åström, T. Denk, op. cit., s. 382–401.

[432] S. Sharma, E. Aparicio, *Organizational and Team Culture as Antecedents of Protection Motivation among IT Employees*, „Computers & Security" 2022, 120; R.F. Ali, P.D.D. Dominic, S.E.A. Ali, M. Rehman, A. Sohail, *Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance*, „Applied Science" 2021, Vol. 11 (8).

[433] J. Chmura, *The impact of positive organisational culture values on information security management in the company*, „Journal of Positive Management" 2016, Vol. 7 (1), s. 87–98; B. Uchendu, J.R.C. Nurse, M. Bada, S. Furnell, *Developing a Cyber Security Culture: Current Practices and Future Needs*, „Computers & Security" 2021, Vol. 109.

informacji, co może sprzyjać kształtowaniu się kultury bezpieczeństwa informacji w organizacji.

Biorąc pod uwagę ograniczenia badania własnego, można stwierdzić, że potwierdziło ono zauważoną w badaniu Martina Karlssona, Fredrika Karlssona, Joachima Åströma i Thomasa Denka[434] zależność, że zmiana organizacji w kierunku orientacji na klienta i urynkowienia, czyli odwrócenie się od orientacji wewnętrznej, może mieć negatywne konsekwencje dla bezpieczeństwa informacji organizacji. W wojewódzkich sądach administracyjnych, w których respondenci postrzegali jako dominujące cechy profilu kultury rynkowej, poziom dojrzałości systemu zarządzania bezpieczeństwem informacji był niski.

[434] M. Karlsson, F. Karlsson, J. Åström, T. Denk, op. cit., s. 382–401.

6. Rekomendacje

Na podstawie wyodrębnionych w badaniu wojewódzkich sądów administracyjnych cech kultury organizacyjnej związanych z dojrzałością systemów zarządzania bezpieczeństwem informacji (Podrozdział 4.4.4), oceny dojrzałości SZBI, badań literaturowych oraz wniosków płynących z wywiadu z dyrektorem sądu o najwyższym poziomie dojrzałości SZBI podjęta została próba przedstawienia rekomendacji dotyczących rozwijania kultury bezpieczeństwa informacji w organizacji. Wzmocnienie kultury bezpieczeństwa informacji zwiększa odporność organizacji na incydenty zagrażające bezpieczeństwu jej zasobów informacyjnych. Rekomendacje przeznaczone są dla najwyższego kierownictwa oraz osób odpowiedzialnych za bezpieczeństwo informacji w organizacji (Tabela 4.11).

Tabela 4.11. Rekomendowane działania dotyczące rozwoju kultury bezpieczeństwa informacji w organizacji.

lp.	***rekomendacje***
1	sformalizowanie zasad dotyczących bezpieczeństwa informacji oraz rozdzielenie ról i odpowiedzialności zgodnie z kompetencjami członków organizacji
2	zaangażowanie w utrzymanie i kontrolę systemu zarządzania bezpieczeństwem informacji
3	inicjowanie regularnych szkoleń zwiększających świadomość członków organizacji o zagrożeniach dotyczących bezpieczeństwa informacji, jak i o pozytywnych efektach przestrzegania procedur związanych z bezpieczeństwem informacji
4	usprawnienie przepływu informacji o działaniach związanych z bezpieczeństwem informacji
5	stwarzanie warunków do wzbudzania lojalności w stosunku do organizacji i poczucia obowiązku wśród członków organizacji
6	dążenie do łagodzenia konfliktów wśród członków organizacji i motywowanie do współpracy
7	stwarzanie sprzyjających warunków do dzielenia się wiedzą na tematy związane z bezpieczeństwem informacji

Źródło: opracowanie własne.

Zaprezentowane rekomendacje powiązane są z kulturą organizacyjną zorientowaną na sprawy wewnętrzne i współpracę między członkami organizacji. Na podstawie badań przedstawionych w niniejszej dysertacji można wnioskować, że ta

orientacja sprzyja dojrzałości systemów zarządzania bezpieczeństwem informacji. Według modelu wartości konkurujących[435] profile kultury organizacyjnej o orientacji na sprawy wewnętrzne i integrację to kultura hierarchiczna i klanowa.

Rekomendacja pierwsza powiązana jest z cechami kultury hierarchicznej[436]. Organizacje o profilu kultury hierarchicznej charakteryzują się wysokim sformalizowaniem działań. O istotności sformalizowania zasad dotyczących bezpieczeństwa informacji oraz rozdzielenia ról i odpowiedzialności zgodnie z kompetencjami członków organizacji mówił m.in. w wywiadzie dyrektor sądu, w którym SZBI uzyskał najwyższy poziom dojrzałości. Formalizacja zasad powinna polegać na stworzeniu, na podstawie przeprowadzonej analizy ryzyka, dokumentu lub zbioru dokumentów[437] z ustaleniami na temat: typu informacji, jakim należy zapewnić bezpieczeństwo, zdefiniowanych ról i odpowiedzialności, uwzględnionych zewnętrznych przepisów prawnych, branych pod uwagę wewnętrznych regulacji, technik wykorzystywanych do zapewnienia bezpieczeństwa informacji, interesariuszy SZBI, standardów wymiany informacji, zasad przydzielania i odbioru uprawnień do systemów informatycznych, regulacji związanych z bezpieczeństwem danych osobowych, sposobu zgłaszania incydentów dotyczących bezpieczeństwa informacji i prywatności, planu ciągłości działania, procedur odzyskiwania kluczowych systemów, częstotliwości przeprowadzania przeglądów i audytów, systemu szkoleń, planu postępowania z ryzykiem w zakresie bezpieczeństwa informacji i sposobu pomiaru skuteczności praktyk dotyczących zarządzania bezpieczeństwem informacji.

Rekomendowane jest zaangażowanie najwyższego kierownictwa w utrzymanie i kontrolę systemu zarządzania bezpieczeństwem informacji. Zalecenie poparte jest, tak jak poprzednie, przeprowadzonym badaniem literaturowym[438] oraz wynikiem badań własnych. W sądzie, którego SZBI uzyskał najwyższy poziom dojrzałości, udokumentowane zostało zaangażowanie najwyższego kierownictwa w jego utrzymanie. Audyty i przeglądy systemu zarządzania bezpieczeństwa informacji w tym sądzie były regularnie zlecane, raporty z ich przebiegu były analizowane i omawiane przez najwyższe kierownictwo, a na podstawie wniosków płynących z powyższych

[435] K.S. Cameron, R.E. Quinn, op. cit., s. 40.

[436] H.-J. Kam, T. Mattson, D.J. Kim, op. cit., s. 1490–1512; M. Karlsson, F. Karlsson, J. Åström, T. Denk, op. cit., s. 382–401.

[437] Dokument w sądzie o najwyższym poziomie dojrzałości SZBI liczył 244 strony, przy średniej wartości 83,3 strony dokumentacji SZBI z 16 WSA.

[438] K.J. Knapp, T.E. Marshall, R.R. Kelly, F.F. Nelson, *Information Security: Management's Effect on Culture and Policy*, „Information Management & Computer Security" 2006, Vol. 14 (1), s. 24–36.

czynności wprowadzano zmiany procedur. Zaangażowanie w nadzór nad audytem i utrzymaniem SZBI oraz pozytywny przykład ze strony najwyższego kierownictwa są działaniami rekomendowanymi w celu rozwijania w organizacji kultury bezpieczeństwa informacji.

Trzecia rekomendacja służy zwiększaniu świadomości członków organizacji o zagrożeniach dotyczących bezpieczeństwa informacji, jak i o pozytywnych efektach przestrzegania procedur związanych z bezpieczeństwem informacji. Z badań w wojewódzkich sądach administracyjnych można wnioskować, iż inicjowanie regularnych szkoleń wpływa na dojrzałość SZBI i rozwój kultury bezpieczeństwa informacji. W sądach, które osiągnęły trzeci i piaty poziom dojrzałości SZBI, odsetek respondentów uczestniczących regularnie w szkoleniach był stosunkowo wysoki (odpowiednio 64,2% i 75%). Według respondentów sądu o najwyższym poziomie dojrzałości wszystkie osoby przynajmniej raz uczestniczyły w szkoleniu. Dyrektorzy 15 sądów w wywiadach podnosili kwestię ważności dla zachowania bezpieczeństwa informacji konieczności aktualizowania wiedzy i posiadania świadomości zagrożeń, a dyrektorzy z 7 sądów mówili o obowiązku uczestniczenia w szkoleniach. Rekomendowane jest przeprowadzanie przynajmniej raz w roku szkoleń zwiększających świadomość członków organizacji o zagrożeniach dotyczących bezpieczeństwa informacji, jak i o pozytywnych efektach przestrzegania procedur związanych z bezpieczeństwem informacji w zakresie dostosowanym do odbiorców.

Usprawnienie przepływu informacji o działaniach związanych z bezpieczeństwem informacji to czwarta rekomendacja, która może przybliżyć organizację do powstania kultury bezpieczeństwa informacji. Według dyrektora z sądu o najwyższym poziomie dojrzałości SZBI dostępność informacji o wdrożeniach i aktualizacjach rozwiązań, mających zapewnić bezpieczeństwo informacji oraz przekazywanie informacji o celowości ich zastosowania, sprzyja pozytywnym postawom wobec konieczności zachowania procedur. Z wypowiedzi dyrektorów wynika, że istotne jest również wdrożenie jasnych zasad zgłaszania incydentów, tak aby komunikaty o zaistniałym zagrożeniu docierały do osób odpowiedzialnych i była możliwa jak najszybsza reakcja na incydent. Rekomendowane jest informowanie w sposób indywidualny o wdrożeniach i aktualizacjach procedur systemu zarządzania bezpieczeństwem informacji z koniecznością potwierdzenia zapoznania się z regulacjami. Zalecane jest również wprowadzenie systemu zgłaszania incydentów.

Rekomendacja piąta dotyczy stwarzania warunków do wzbudzania lojalności w stosunku do organizacji i poczucia obowiązku wśród członków organizacji. Zalecenie to powiązane jest z cechami kultury klanowej. Typowymi cechami organizacji o profilu kultury klanowej są praca zespołowa, dążenie do zwiększenia zaangażowania ludzi i poczucia odpowiedzialności organizacji za jej członków. Lojalność członków wobec organizacji można promować, dbając o ich rozwój, w tym zdobywanie nowych umiejętności, przy jednoczesnym okazywaniu wobec nich szacunku i ich docenianiu. „Pracownik XXI w. może być wobec firmy lojalny, a jednocześnie dbać o realizację własnych celów. W czasie, w którym zatrudniony jest w danej firmie, pracuje uczciwie, z pełnym zaangażowaniem, identyfikuje się z nią. Kiedy firma pomaga zatrudnionym nabywać nowych umiejętności, otrzymuje ich zaangażowanie i przyciąga nowych, lojalnych pracowników”[439]. Lojalność i poczucie obowiązku wśród członków organizacji to postawy, które organizacja powinna promować przy pomocy najwyższego kierownictwa, aby działania członków organizacji były zgodne z regulacjami dotyczącymi bezpieczeństwa informacji.

Na podstawie przeprowadzonych badań, można uznać za istotne, aby kierownictwo dążyło do łagodzenia konfliktów wśród członków organizacji i motywowało do współpracy. Rekomendacja ta jest podyktowana wynikami badań własnych, z których można wnioskować, że w sądach, w których respondenci zaobserwowali spójność, wysoki stopień uczestnictwa i duże poczucie wspólnoty, poziom dojrzałości SZBI był wysoki. Łagodzenie konfliktów w organizacji daje możliwość współpracy pomiędzy jej członkami. Rekomendowane jest wdrożenie zachęt do zgłaszania propozycji dotyczących doskonalenia własnych działań i funkcjonowania całej organizacji. Proponuje się tworzenie zespołów roboczych składających się z przedstawicieli różnych jednostek organizacyjnych w celu opracowywania nowych lub aktualizacji istniejących procedur, również tych dotyczących bezpieczeństwa informacji.

Posiadanie przez członków organizacji wiedzy na temat typu rozwiązań organizacyjnych i technicznych, które sprzyjają zapewnieniu bezpieczeństwa informacji, jest istotnym czynnikiem wpływającym na bezpieczeństwo informacji. Dyrektor sądu, który uzyskał najwyższy stopień dojrzałości SZBI, podkreślał ważność przeprowadzonego zewnętrznego audytu, który umożliwił wybór właściwych

[439] I. Świątek-Barylska, *Lojalność pracowników współczesnych organizacji*. *Istota i elementy składowe*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2013, s. 217.

rozwiązań przy tworzeniu systemu zarządzania bezpieczeństwem informacji. Zaleca się, aby najwyższe kierownictwo zapewniło członkom organizacji, szczególnie tym, którzy są odpowiedzialni za utrzymanie systemu zarządzania bezpieczeństwem informacji, możliwość poszerzania wiedzy koniecznej do realizacji przydzielonych zadań. Oprócz dostępności szkoleń zaleca się stworzenie warunków dających okazję do dzielenia się wiedzą i doświadczeniem pomiędzy członkami organizacji, jak i z innymi organizacjami lub zewnętrznymi interesariuszami, którzy prowadzą profesjonalną działalność w obszarze bezpieczeństwa informacji, np.: audytorami, specjalistami przeprowadzającymi testy penetracyjne systemów, dostawcami rozwiązań technicznych, jednostkami certyfikacyjnymi czy krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego (ang. *Computer Security Incident Response Team*, skrót: CSIRT).

7. Zakończenie

Dysertacja została poświęcona tematyce dojrzałości zarządzania bezpieczeństwem informacji z uwzględnieniem kontekstu kultury organizacyjnej. Ważkość problemu wynika z rosnącego ryzyka utraty bezpieczeństwa przetwarzanych informacji w związku z transformacjami cyfrowymi zachodzącymi w organizacjach. Bezpieczeństwo informacji nie może być zapewniane jedynie przez wdrożenia rozwiązań technicznych, zmieniająca się, w związku z transformacją cyfrową, kultura organizacyjna powinna sprzyjać zachowaniu bezpieczeństwa informacji.

Głównym celem dysertacji było zdiagnozowanie dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych z uwzględnieniem kontekstu kultury organizacyjnej. Na początku postępowania badawczego, przeprowadzono przegląd literatury dotyczącej problemów związanych z oceną dojrzałości systemów zarządzania bezpieczeństwem informacji oraz przegląd literatury w zakresie perspektyw rozumienia i badania procesów kulturowych, zachodzących w organizacjach. Analiza literatury wykazała lukę badawczą w zakresie przeprowadzonych na cele powstania niniejszej dysertacji badań, co oznacza, że badania własne zaprezentowane i omówione na kartach niniejszej pracy stanowią pierwszą w Polsce eksplorację dotyczącą dojrzałości systemów zarządzania bezpieczeństwem informacji wojewódzkich sądów administracyjnych z uwzględnieniem kontekstu kultury organizacyjnej. Głównie deskryptywny i eksploracyjny charakter badania dał możliwość poznania procesów związanych z zarządzaniem bezpieczeństwem informacji oraz postaw i działań członków organizacji. Badanie przeprowadzone było z wykorzystaniem metod i technik ilościowych, jak i jakościowych, co pozwoliło na pogłębione zrozumienie problemów badawczych sformułowanych na wstępie dysertacji:

1. Jaki jest poziom dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych?
2. Jaki jest w ocenie pracowników dominujący profil kultury organizacyjnej w wojewódzkich sądach administracyjnych?
3. Czy istnieją cechy kultury organizacyjnej mające potencjalny związek z dojrzałością systemów zarządzania bezpieczeństwem informacji?

Odpowiedź na pierwsze pytanie badawcze uzyskane zostało na podstawie sondaży diagnostycznych, tj. wywiadów z dyrektorami i na podstawie badania

dokumentów zawierających polityki bezpieczeństwa poszczególnych sądów. Systemy zarządzania bezpieczeństwem informacji we wszystkich wojewódzkich sądach administracyjnych zostały ustanowione na podstawie obowiązujących przepisów krajowych. Zauważono różnice w zaangażowaniu najwyższego kierownictwa w utrzymanie tych systemów. Żaden z sądów nie poddał certyfikacji swojego SZBI. We wszystkich sądach zdefiniowane zostały role i obowiązki w procesach związanych z zarządzania bezpieczeństwem informacji. W podrozdziałach 4.2 i 4.4.3 zostały przedstawione wyniki dotyczące poziomów dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych. Dojrzałość SZBI oceniono następująco: pięć WSA osiągnęło pierwszy poziom dojrzałości, siedem poziom drugi, trzy poziom trzeci oraz jeden sąd poziom najwyższy, piąty. Do oceny dojrzałości SZBI wykorzystano utworzone narzędzie, które może posłużyć za wzór w badaniach innych organizacji (Podrozdział 3.6.2).

W celu odpowiedzi na drugie pytanie badawcze zastosowano metodę sondażu diagnostycznego oraz techniki badawcze w postaci wywiadu i ankiety. W badaniach zauważalny był subiektywizm osób biorących w nich udział, co wynikało z natury tych technik. Cechy kultury hierarchicznej były zdiagnozowane jako dominujące w piętnastu sądach na szesnaście badanych, w jednym sądzie dominowały cechy kultury rynkowej. W podrozdziale 4.3.1 przedstawione zostały szczegółowe wyniki badań z uwzględnieniem sześciu badanych wymiarów kultury organizacyjnej, tj.: „ogólna charakterystyka", „styl przywództwa", „styl zarządzania pracownikami", „co zapewnia spójność organizacji?", „na co kładzie się największy nacisk?" i „kryteria sukcesu w organizacji". W dwóch wymiarach: „styl przywództwa" i „styl zarządzania pracownikami" zauważone zostały rozbieżności w wynikach badanych sądów. W wymiarze „styl przywództwa" w 50% badanych sądów zauważane były przez respondentów jako dominujące cechy charakterystyczne dla kultury rynkowej. W jednym z sądów dominowały cechy kultury klanowej. W wymiarze „styl zarządzania pracownikami" w jednym z sądów dominował profil kultury rynkowej, w innym zaś obok cech kultury hierarchicznej porównywalnie istotne były cechy kultury klanowej.

Zauważone w badaniu rozbieżności w wymiarach kultury dotyczących przywództwa w organizacji i zarządzania pracownikami, jak i różnice w poziomach dojrzałości SZBI w badanych organizacjach, pozwoliły na wyodrębnienie cech kultury organizacyjnej mających potencjalny związek z dojrzałością SZBI – zatem odpowiedź na ostatnie pytanie problemu badawczego jest twierdząca. W wojewódzkim sądzie

administracyjnym, który uzyskał najwyższy, piąty poziom dojrzałości SZBI, w wymiarach „styl przywództwa" i „styl zarządzania pracownikami" respondenci wskazywali jako wyróżniające się cechy kultury klanowej obok cech kultury hierarchicznej. Dostrzeżona koincydencja pomiędzy cechami kultury a dojrzałością SZBI była podstawą sformułowania rekomendacji dotyczących rozwijania kultury bezpieczeństwa informacji w organizacji (Rozdział 6). Można przypuszczać, że rekomendacje okażą się przydatne nie tylko w sądownictwie administracyjnym, ale również w sądownictwie powszechnym lub szerzej w organizacjach sektora publicznego.

Podsumowując, należy stwierdzić, że – pomimo wskazanych ograniczeń badań – główny cel dysertacji został osiągnięty. Zdiagnozowana została dojrzałość systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych z uwzględnieniem kontekstu kultury organizacyjnej. W pracy zidentyfikowano znaczenie czynników kulturowych w zarządzaniu bezpieczeństwem informacji. Wyniki zaprezentowane w dysertacji pozwoliły poszerzyć wiedzę o zarządzaniu bezpieczeństwem informacji oraz o kulturze organizacyjnej w wybranej grupie organizacji sektora publicznego, co stanowi wkład do rozwoju nauk o zarządzaniu i jakości.

Ze względu na złożoność poruszanych w dysertacji problemów badawczych, temat związku kultury organizacyjnej i zarządzania bezpieczeństwem informacji nie został wyczerpany. Z uwagi na istotność dla dojrzałości SZBI procesów związanych z zarządzaniem ryzykiem dotyczącym bezpieczeństwa informacji, zauważono potrzebę dalszych badań w tym obszarze z uwzględnieniem kultury organizacyjnej. Szczegółowe zbadanie występujących procesów związanych z zarządzaniem ryzykiem dotyczącym bezpieczeństwa informacji oraz zbadanie zaangażowania osób odpowiedzialnych za bezpieczeństwo informacji i ochronę danych osobowych w te procesy może poszerzyć wiedzę na temat kultury bezpieczeństwa informacji w organizacji.

8. Bibliografia

Abulencia J., *Insider attacks: Human-factors attacks and mitigation,* „Computer Fraud and Security" 2021, (5).

Ackoff R.L., *From Data to Wisdom*, „Journal of Applied Systems Analysis" 1989, Vol. 16.

Ackoff R.L., *O systemie pojęć systemowych*, „Prakseologia" 1973, nr 2;

Adamiak B., Borkowski J., *Charakter kompetencji judykacyjnej sądów administracyjnych*, [w:] B. Adamiak, J. Borkowski, *Metodyka pracy sędziego w sprawach administracyjnych*, Wolters Kluwer 2020.

Adriaans P., Benthem J., *Introduction: Information is What Information Does*, [w:] Adriaans P., Benthem J., *Philosophy of Information*, Elsevier 2008.

Akter S., Uddin M.R., Sajib S., Lee W.J.T., Michael K., Hossain M.A., *Reconceptualizing Cybersecurity Awareness Capability in the Data-Driven Digital Economy,* „Annals of Operations Research" 2022.

Al Ghamdi S., Win K., Vlahu-Gjorgievska E., *Information security governance challenges and critical success factors: Systematic review*, „Computers and Security", 2020, Vol. 90.

Alhogail A., Mirza A., *Information security culture: a definition and a literature review*, [w:] Proceedings of IEEE World Congress On Computer Applications and Information Systems, 2014.

Ali R.F., Dominic P.D.D., Ali S.E.A., Rehman M., Sohail A, *Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance*, „Applied Sciences" 2021, Vol. 11 (8).

Amankwa E., Loock M., Kritzinger E., *Establishing Information Security Policy Compliance Culture in Organizations*, „Information & Computer Security" 2018, Vol. 26(4).

Amrozy K., *O czym mówimy, kiedy mówimy o kulturze policyjnej?* „Athenaeum. Polskie Studia Politologiczne", nr 57.

Andrukiewicz E., Kowalewski M., *Praktyczne podejście do wdrażania systemów zarządzania bezpieczeństwem informacji w małych i średnich przedsiębiorstwach*, „Studia Ekonomiczne" 2018, Vol. 355.

Aniszewska G., Gielnicka I., *Firma to ja, firma to my. Poradnik kultury organizacyjnej firmy*, Ośrodek Doradztwa i Doskonalenia Kadr, Gdańsk 1999.

Annarelli A., Nonino F., Palombi G., *Understanding the management of cyber resilient systems*, Computers & Industrial Engineering, 2020, Vol. 149.

Apanowicz J., Metodologia ogólna, Wydawnictwo Diecezji Pelplińskiej „BERNARDINUM", Gdańsk 2002.

Armstrong M., *Zarządzanie zasobami ludzkimi*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 1996.

Arsenijevic O., Trivan D., Milosevic M., *Storytelling as a Modern Tool of Construction of Information Security Corporate Culture*, „Industrial Organization" 2016, Vol. 62 (4), s. 105–114.

Ashenden D., *Information Security Management: A Human Challenge?* „Information Security Technical Report" 2008, 13 (4), s. 195–201.

Auksztol J., Chomuszko M., *Modelowanie organizacji procesowej*, Wydawnictwo Naukowe PWN, Warszawa 2012.

Austen A., Kulikowska-Pawlak M, *Analiza i interpretacja danych empirycznych w badaniach mieszanych*, [w:] *Metody badań mieszanych w naukach o zarządzaniu*, (red.) Ł. Sułkowski, R. Lenart-Gansiniec, Wydawnictwo Naukowe Akademii WSB, Dąbrowa Górnicza 2023.

Baiyere A., Salmela H., Tapanainen T., *Digital transformation and the new logics of business process management*, „European Journal of Information Systems" 2020, 29(3).

Balková M., Jambal T., *Evaluation of organizational culture in enterprises in the Czech Republic using OCAI*, „Frontiers in Psychology" 2023, 14:1297041.

Barnard Ch., *Funkcje kierownicze*, AE w Krakowie, Czytelnik, Kraków 1997.

Bate P., *Changing the culture of a hospital: from hierarchy to networked community*, „Public Administration" 2000, 78(3).

Bednarek M., *Kierunki rozwoju zarządzania we współczesnym przedsiębiorstwie*, [w:] *Kulturowa zmienność systemów zarządzania*, (red.) Ł. Sułkowski, M. Bednarek, A. Parkes, Difin, Warszawa 2016.

Bełz G., Skalik J., *Rozumienie systemu zarządzania. Próba definicji*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Kształtowanie i doskonalenie systemu zarządzania w przedsiębiorstwach" 2011, nr 178.

Berger D., Shashidhar N. and Varol C., *Using ITIL 4 in Security Management*, 8th International Symposium on Digital Forensics and Security (ISDFS), 2020.

Berrio A.A., *An Organizational Culture Assessment Using the Competing Values Framework: A Profile of Ohio State University Extension*, „Journal of Extension" 2003, 41(2).

Bielski M., *Organizacje: istota, struktury, procesy*, Wyd. III, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2001.

Bieńkowska J., Sikorski C., *Ewolucja zarządzania. Dyktat struktury, strategii i kultury*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2016.

Binder P., *Wywiady online w badaniach jakościowych okresu pandemii: inkluzywny potencjał, zagrożenie wykluczeniem i jakość gromadzonych danych*, „Kultura i Edukacja" 2022, Nr 3 (137).

Bing-You R.G., Varaklis K., *Organizing Graduate Medical Education Programs into Communities of Practice*, „Medical Education Online" 2016, nr 2

Bishop M., *Introduction to computer security*, Addison-Wesley, Boston 2005.

Bitkowska A., *The relationship between Business Process Management and Knowledge Management – selected aspects from a study of companies in Poland*, „Journal of Entrepreneurship, Management and Innovation" 2020, 16.

Bittencourt M., Gupta R., Makena P., Stander L., *Socio-political instability and growth dynamics*, „Economic Systems" 2022,Vol. 46(4).

Borbinha J., Proença D., *Information Security Management Systems – A Maturity Model Based on ISO/IEC 27001*, [w:] Abramowicz W., Paschke A., *Business Information Systems*, BIS 2018. Lecture Notes in Business Information Processing, vol. 320, Springer, Cham 2018.

Boufounou P., Argyrou M.D, *Changing the organizational culture to transform the economy: The case of Greece*, „Frontiers in Research Metrics and Analytics", 2022, 7:1050544.

Brajer-Marczak R., Gębczyńska A., *Process Maturity Models as Tools for Organisation Improvement and Development*, [w:] *Education Excellence and Innovation Management: A 2025 Vision to Sustain Economic Development during Global Challenges*, (red.) S. Soliman Khalid, International Business Information Management Association (IBIMA), 2020.

Brzozowski T., Rogala P., *Podejście procesowe według norm ISO serii 9000 − istota i ewolucja*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu" 2017, nr 470.

Buchelt B., Jonczyk J., *Powiązania kultury organizacyjnej i zarządzania zasobami ludzkimi w szpitalach publicznych*, „Zarządzanie Publiczne" 2017, 40.

Burdon M., Coles-Kemp L., *The Significance of Securing as a Critical Component of Information Security: An Australian Narrative*, „Computers & Security" 2019, Vol. 87.

Burrel G., Morgan G., *Sociological Paradigms and Organisational Analysis*, Heinemann, London 1979.

Caliskan A., Zhu Ch., *Organizational Culture Type in Turkish Universities using OCAI: Perceptions of Students*, „Journal of Education Culture and Society" 2019, No. 2.

Calvache C., Piattini M., Garcia F., Pino F., Baldassarre M., *A 360-degree process improvement approach based on multiple models*, „Revista Facultad de Ingenieria" 2015, Vol. 1(77).

Cameron K.S., Quinn R.E., *Kultura organizacyjna – diagnoza i zmiana. Model wartości konkurujących*, Oficyna Ekonomiczna, Kraków 2003.

Cancino V., Aliaga M., *Instrumento de evaluación de la cultura organizacional: revisión sistemática de su aplicación*, „Revista Venezolana de Gerencia" 2022, 27 No. 97.

Carroll A.B., *Corporate social responsibility: Evolution of a definitional construct*, „Business and Society" 1999, vol. 38, no. 3.

Chadegani A.A., Hadi Salehi M., Md Yunus M., Farhadi H., Fooladi M., Farhadi M., and Ale Ebrahim N., *A Comparison between Two Main Academic Literature Collections,* Asian Social Sciences, Vol. 9, No. 5, 2013.

Chang S.E., Lin C.-S., *Exploring organizational culture for information security management,* „Industrial Management and Data Systems" 2007, Vol. 107, No. 3.

Chmielewska-Muciek D., *Dyskusja nad pojęciem kultury organizacyjnej*, „Annales Universitatis Mariae Curie-Skłodowska. Sectio H, Oeconomia" 2009, Nr 43.

Chmura J., *Forming the Awareness of Employees in the Field of Information Security*, „Journal of Positive Management" 2017, nr 8(1).

Chmura J., The impact of positive organisational culture values on information security management in the company, „Journal of Positive Management" 2016, Vol. 7 (1).

Cieciora M., Pietrzak P., Dębski M., Kandefer K., Bołkunow W., *Differences in the Perception of Organizational Culture in Non-Public Universities in Poland by Academic and Administrative Staff – A Study Based on Cameron and Quinn's Model*, „Foundations of Management" 2021, Vol. 13.

Clinch J., „ITIL v3 and Information Security," Axelos Global Best Practices, May 2009.

Choo C.W., Detlor D., Turnbull D., *Web Work: Information Seeking and Knowledge Work on the World Wide Web*, Kluwer, Dordrecht 2000.

Cooper J., Fisher M., *Software Acquisition Capability Maturity Model (SA-CMM) Version 1.03*, CMU/SEI-2002-TR-010, Carnegie Mellon University, Software Engineering Institute, Pittsburgh 2002, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2002_005_001_14036.pdf (dostęp: 3.08.2023 r.).

Creswell J.W., Tashakkori A., *Differing perspectives on mixed methods research*, „Journal of Mixed Methods Research" 2007, 1(4).

Crosby P.B., *Quality is free: The Art of Making Quality Certain*, McGraw–Hill, New York 1979.

Čuček M., Mlaker Kač S., *Organizational culture in logistics sector and its relation to employee satisfaction*, „Journal of Contemporary Management Issues" 2020, Vol. 25, No. 2.

Culot G., Nassimbeni G., Podrecca M., Sartor M., *The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda,* „The TQM Journal 2021", Vol. 33.

Curtis B., Hefley B., Miller S., *People Capability Maturity Model, Version 2 Second Edition*, CMU/SEI-2009-TR-003, Carnegie Mellon University, Software Engineering Institute, Pittsburgh 2009, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2009_005_001_15095.pdf (dostęp: 3.08.2023 r.).

Czarniawska B., *Antropologia i teoria organizacji: wczoraj i dziś*, „Problemy Zarządzania: Antropologia Organizacji" 2011, 9/2 (32).

Czarniawska B., *Interviewes and organizational narratives* [w:] *Handbook of interviewing*, (red.) J.F. Gubrium, J. Holstein, Sage, Thousand Oaks 2002.

Czekaj J., Ziębicki B., *Pozytywna nauka o organizacji na tle ewolucji teorii i koncepcji zarządzani*a, „Organizacja i Kierowanie" 2013, nr 3(156).

Czekan w., *Metodyka systematycznego przeglądu literatury*, [w:] *Podstawy metodologii badań w naukach o zarządzaniu*, (red.) W. Czekan, Wyd. III, Wolters Kluwer, Warszawa 2015.

Czekon W., *Podstawy metodologii badań w naukach o zarządzaniu*, Wolters Kluwer, Warszawa 2015.

Czerska M., *Proces kształtowania kultury organizacji*, „Prace Naukowe Akademii Ekonomicznej We Wrocławiu. Zmiana warunkiem sukcesu: Integracja, globalizacja, regionalizacja – wyzwania dla przedsiębiorstw" 2002, 32/33 (963).

Da Veiga A., Martins N., *Defining and Identifying Dominant Information Security Cultures and Subcultures*, „Computers & Security" 2017, 70.

Da Veiga A., *An Approach to Information Security Culture Change Combining ADKAR and the ISCA Questionnaire to Aid Transition to the Desired Culture*, „Information & Computer Security" 2018, Vol. 26 (5).

da Veiga A., Astakhova L.V., Botha A., Herselman M., *Defining Organisational Information Security Culture—Perspectives from Academia and Industry*, „Computers & Security" 2020, Vol. 92.

Da Veiga A., Martins N., *Defining and Identifying Dominant Information Security Cultures and Subcultures*, „Computers & Security" 2017, Vol. *70*.

Davidow W.H., Malone M.S., *The Virtual Corporation: Structuring and Revitalizing the Corporation for the 21st Century*, Harper Collins, New York 1992.

de Bruin T., Rosemann M., *Towards a Business Process Management Maturity Model*, Proceedings of the 13th European Conference on Information Systems, 2005.

Deal T.E., Kennedy A.A., *Corporate cultures: the rites and rituals of corporate life*, Penguin, Harmondsworth 1982.

Dembowska M., *Słownik terminologiczny informacji naukowej*, Zakład Narodowy im. Ossolińskich, Wrocław–Warszawa–Kraków–Gdańsk 1979.

Denning P.J., *The IT Schools Movement*, „Communications of ACM" 2001, Vol. 44, No. 8.

Denzin N.K., *The research act: A theoretical introduction to sociological methods*, Praeger, New York 1978.

Deshapande R., Parasurman R., *Linking corporate to strategic planning*, „Organizacja i Kierowanie" 1987, nr 6.

Davis J., Mengersen K., Bennett S., Mazerolle L., *Viewing systematic reviews and meta-analysis in social research through different lenses*, „SpringerPlus" 2014, 3.

Dębski M., Cieciora M., Pietrzak P., Bołkunow W., *Organizational Culture in Public and Non-public Higher Education Institutions in Poland: A Study Based on Cameron and Quinn's Model*, „Human Systems Management" 2020, 39.

Dhillon G., Syed R., Pedron C., *Interpreting Information Security Culture: An Organizational Transformation Case Study*, „Computers & Security" 2016, Vol. 56.

Dhillon G., Torkzadeh G., *Value-Focused Assessment of Information System Security in Organizations*, „Information Systems Journal" 2006, Vol. 16 (3).

Drucker P.F., *Information, Communications, and Understanding*, Routledge 2017.

Drucker P.F., *Knowledge-Worker Productivity: THE BIGGEST CHALLENGE*, California Management Review, 1999, Vol. 41(2).

Duff A.S., *Castells versus Bell: A comparison of two grand theorists of the information age*, European Journal of Social Theory, 26(1), 2023.

Dumas M., La Rosa M., Mendling J., Reijers H.A., *Introduction to Business Process Management*, [w]: M. Dumas, M. La Rosa, J. Mendling, H.A. Reijers, Fundamentals of Business Process Management, Springer, Berlin, Heidelberg 2018.

Ernest Chang S,, Lin C., *Exploring Organizational Culture for Information Security Management*, „Industrial Management & Data Systems" 2007, 107 (3).

Fernandes P., Pereira R., Wiedenhöft G., *The Effect of Organizational Cultures on Relationships between IT Governance and Individual Behavior*, „Emerging Science Journal Open Access" 2023, Vol. 7, I. 5.

Flakiewicz W., *Pojęcie informacji w technologii multimedialnej*, SGH, Warszawa 2005.

Flores R.W., Ekstedt M., *Shaping Intention to Resist Social Engineering through Transformational Leadership*, Information Security Culture and Awareness, „Computers & Security" 2016, Vol. 59.

Flores W.R., Antonsen E., Ekstedt M., *Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture*, „Computers & Security" 2014, 43.

Fontana A., Frey, *Interviewing: The art of science*, [w:] *Collecting and interpretative qualitative materials*, (red.) B.K. Denzin, Y.S. Lincoln, Sage, London 1994.

Fosher K.B., Lane R., Tarzi E., Post K., Gauldin E.M., Tashev B., Edwards J., McLean J.D., *Translational Research in a Military Organization: The Marine Corps Organizational Culture Research Project*, „Annals of Anthropological Practice" 2020, 44(1).

Frączkiewicz-Wronka A, *Poszukiwanie istoty zarządzania publicznego,* [w:] *Zarządzanie publiczne – elementy teorii i praktyki*, Akademia Ekonomiczna w Katowicach, Katowice 2009.

Frączkiewicz-Wronka A., *Diagnozowanie kultury organizacyjnej w podmiocie leczniczym – studium szpitala publicznego*, [w:] *Instrumentarium zarządzania publicznego*, (red.) B. Kożuchowska, Ł. Sułkowski, Difin, Warszawa 2015.

Frączkiewicz-Wronka A., *Zarządzanie publiczne – elementy teorii i praktyki*, Wydawnictwo Akademii Ekonomicznej w Katowicach, Katowice 2009.

Frey R., Boyd M., Foster S., Robinson J., Gott M., *What's the Diagnosis? Organisational Culture and Palliative Care Delivery in Residential Aged Care in New Zealand,* „Health & Social Care in Community" 2016, 24.

Gaus N., *Organisational culture in higher education: mapping the way to understanding cultural research*, „Journal of Further and Higher Education", No. 43, 2017.

Ge X.Y., Yuan Y.Q., Lu L.L., *An information security maturity evaluation mode*, Procedia Engineering, 2011, No. 24.

Geertz C., *Interpretation of cultures. Selected essays*, Basic Books, New York 1973.

George D, Mallery P., *IBM SPSS statistics 23 step by step: A simple guide and reference*, Routledge, New York 2016.

Gioia D.A., Corley K.G., Hamilton A.L., *Seeking qualitative rigor in inductive research: Notes on the Gioia methodology*, „Organizational Research Methods" 2013, Vol. 16(1).

Goel S., Shawky H.A., *Estimating the market impact of security breach announcements on firm values*, „Information and Management" 2009, Vol. 46, No. 7.

Góra N., *Zintegrowane systemy zarządzania w ujęciu teoretyczno-praktycznym*, „Management and Quality" 2021, t. 3, nr 2.

Grajewski P., *Procesowe zarządzanie organizacją*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2012.

Grudzewski W.M., Hejduk J.K., *Zarządzanie wiedzą w przedsiębiorstwach*, Difin, Warszawa 2004.

Gutschmidt D., A. Vera, *Organizational culture, stress, and coping strategies in the police: An empirical investigation*, „Police Practice & Research" 2022, 23(5).

Haffer R., *Samoocena i pomiar wyników działalności w systemach zarządzania przedsiębiorstw: w poszukiwaniu doskonałości biznesowej*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2011.

Hammer M., Champy J., *Reengineering the Corporation: A Manifesto for Business Revolution*, Harper Collins Publisher, New York 1993.

Hammer M., Champy J., *Reengineering w przedsiębiorstwie*, Neumann Management Institute, Warszawa 1996.

Hampden-Turner Ch., Trompenaars A., *Siedem kultur kapitalizmu*, Dom Wydawniczy ABC, Warszawa 1998.

Hampden-Turner Ch., Trompenaars F., *Siedem wymiarów kultury*, Oficyna Ekonomiczna, Kraków 2002.

Handy C.B., *Understanding organizations*, Penguin, London 1999.

Haraty R.A., Naous M., *Modeling and validating the clinical information systems policy using alloy*, „Lecture Notes in Computer Science" 2013 (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7798 LNCS.

Harnesk D., Lindström J., Shaping Security, *Behaviour through Discipline and Agility: Implications for Information Security Management*, „Information Management & Computer Security" 2011, Vol. 19 (4).

Harrison R., *Understanding your organization's character*, Harvard Business Review, 1972.

Hassandoust F., Johnston A.C., *Peering through the Lens of High-reliability Theory: A Competencies Driven Security Culture Model of High-reliability Organisations*, „Information Systems Journal" 2023, Vol. 33(5).

Hassandoust F., Subasinghage M., Johnston A.C., *A Neo-Institutional Perspective on the Establishment of Information Security Knowledge Sharing Practices*, „Information & Management" 2022, Vol. 59 (1).

Hatch M.J., *The dynamics of organizational culture*, „Academy of Management Review" 1993, 18/4.

Hatch M.J., *Teoria organizacji*, Wydawnictwo Naukowe PWN, Warszawa 2002.

Hofstede G, Hofstede G.J., *Kultury i organizacje. Zaprogramowanie umysłu*, Wydanie II zmienione, PWE, Warszawa 2007.

Hofstede G., *Culture and organizations*, „International Studies of Management & Organization" 1980, nr 10(4).

Hofstede G., *Culture's Consequences. International Differences in Work-Related Values*, Sage, Beverly Hills–London–New Delhi 1984.

Hofstede G., Hofstede G.J., Minkov M., *Kultury i organizacje. Zaprogramowanie umysłu*, Wydanie III zmienione, PWE, Warszawa 2011.

Hofstede G., *Kultury i organizacje. Zaprogramowanie umysłu*, PWE, Warszawa 2000.

Hogail A.A., *Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study*, „IJSIA" 2015, Vol. 9 (7).

Hood C., *A Public Management for All Seasons?* „Public Administration" 1991, 69(1).

Hu Q., Dinev T., Hart P., Cooke D., *Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture: Managing Employee Compliance with Information Security Policies*, „Decision Sciences" 2012, Vol. 43 (4).

Humaidi N., Balakrishnan V., *Indirect Effect of Management Support on Users' Compliance Behaviour towards Information Security Policies*, „Health Information Management Journal" 2018, Vol. 47 (1), s. 17–27.

Humphrey W.S., *Characterizing the Software Process: A Maturity Framework*, Carnegie Mellon University/Software Engineering Institute, Pittsburgh 1987.

Humphrey W.S., W.L. Sweet, *A method for assessing the software engineering capability of contractors*, Carnegie Mellon University, Software Engineering Institute, Pittsburgh 1987.

Hys K., *Wybrane modele dojrzałości systemu zarządzania jakością w organizacji*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu: Sieci międzyorganizacyjne, procesy i projekty w erze paradoksów" 2016, 5(421).

Imgrund F., Fischer M., Janiesch C., Winkelmann A., *Approaching digitalization with business process management*, Proceedings of the MKWI, 2018.

ITIL Foundation, ITIL 4 edition. Norwich: TSO (The Stationery Office), 2019.

Jacques E., *The Changing Culture of a Factory*, Dryden Press, New York 1952.

Januszkiewicz K., *Od teorii naukowych do badania empirycznego — budowa narzędzi do badania zachowań ludzi w organizacji*, „Przegląd Organizacji" 2016, Nr 12 (923).

Jarosiewicz H., *Świadomość organizacji. O znaczeniu klimatu dla rozwoju osoby i sukcesu przedsiębiorstwa*, Uniwersytet Wrocławski, Instytut Psychologii, Wrocław 2022.

Jaworska E., *Społeczna odpowiedzialności przedsiębiorstw jako źródło szans i przewagi konkurencyjnej*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Instrumenty zarządzania kosztami i dokonaniami" 212, nr 252.

Jemielniak D., Latusek-Jurczak D., *Zasady zarządzania*, Wolters Kluwer SA, Warszawa 2014.

Jeszka A., *Problemy badawcze i hipotezy w naukach o zarządzaniu*, „Organization and Management" 2013, Nr 5.

Johnson R.B. Onwuegbuzie A.J, Turner L.A., *Toward a Definition of Mixed Methods Research*, „Journal of Mixed Methods Research" 2007, 1(2).

Jokiel G., *Podejście procesowe w zarządzaniu – geneza i kierunki rozwoju* koncepcji, „ Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Podejście procesowe w organizacjach, Wydawnictwo Uniwersytetu Ekonomicznego" 2009, nr 52.

Juchniewicz M., *Koncepcje doskonalenia organizacji – ewolucja, krytyka, perspektywy rozwoju,* „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu: Nowe kierunki w zarządzaniu przedsiębiorstwem. Procesy i projekty w zarządzaniu zmianami" 2017, 12(463).

Jung T., Scott T., Davies H., Bower P., Whalley D., Mcnally R., Mannion R., *Instruments for Exploring Organizational Culture: A Review of the Literature*, „Public Administration Review" 2009, Vol. 69.

Kacała J., Michaluk A., *Rozwój kadr a kultura organizacyjna w dobie profesjonalizacji sił zbrojnych RP*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Nauki o Zarządzaniu, 4. Zarządzanie w teorii" 2010, nr 137.

Kaczmarek A., *Wybrane modele dojrzałości zarządzania bezpieczeństwem informacji – analiza porównawcza*, [w:] *Współczesny człowiek wobec wyzwań: szans i zagrożeń w cyberprzestrzeni*, (red.) J. Grubicka, A. Kamińska-Nawrot, Akademia Pomorska w Słupsku, Słupsk 2021.

Kalinowski T.B., *Dojrzałość procesowa a wyniki organizacji*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2018.

Kalinowski T.B., *Modele oceny dojrzałości procesów*, „Acta Universitatis Lodziensis. Folia Oeconomica" 2011, nr 258.

Kalinowski T.B., *Process maturity vs. organisational results*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2017, (463).

Kam H.-J., Mattson T., Kim D. J., *The "Right" Recipes for Security Culture: A Competing Values Model Perspective*, „Information Technology & People" 2021, Vol. 34 (5).

Karlsson F, *Information security culture – state-of-the-art review between 2000 and 2013*, „Information & Computer Security" 2015, Vol. 23, No. 3.

Karlsson M,, Karlsson F., Åström J., Denk T., *The effect of perceived organizational culture on employees' information security compliance*, „Information & Computer Security" 2022, Vol. 30 (3).

Karlsson M., Denk T., Åström, *J. Perceptions of Organizational Culture and Value Conflicts in Information Security Management*, „Information & Computer Security" 2018, Vol. 26 (2).

Katz D., Kahn R.L., *Społeczna psychologia organizacji*, PWN, Warszawa 1979.

Kessler S. R.; Pindek S.; Kleinman, G.; Andel S. A.; Spector P. E., *Information Security Climate and the Assessment of Information Security Risk among Healthcare Employees*, „Health Information Management Journal" 2020, Vol. 26 (1).

Khan H.U., AlShare K.A., *Violators versus Non-Violators of Information Security Measures in Organizations—A Study of Distinguishing Factors*, „Journal of Organizational Computing and Electronic Commerce" 2019, Vol. 29 (1).

Kisielnicki J., Sroka H., *Systemy informacyjne biznesu*, Placet, Warszawa 2005.

Kluckhohn, F.,Strodtbeck *Variations in Value Orientations*, Peterson, Evanston 1961.

Knapp K. J., Marshall T. E., Kelly R. R., Nelson F. F., *Information Security: Management's Effect on Culture and Policy*, „Information Management & Computer Security" 2006, Vol. 14 (1)

Kohlbacher M., Gruenwald S., *Process orientation: Conceptualization and measurement*, „Business Process Management Journal" 2011, Vol. 17, No. 2.

Kohlegger M., Reijers H.A., The effects of process-oriented organizational design on firm performance, „Business Process Management Journal" 2013, Vol. 19(2).

Kolasińska-Morawska K., *Strategie badań mieszanych*, [w:] *Metody badań mieszanych w naukach o zarządzaniu*, (red.) Ł. Sułkowski, R. Lenart-Gansiniec, Wydawnictwo Naukowe Akademii WSB, Dąbrowa Górnicza 2023.

Kolmogorov A.N., *Three approaches to the quantitative definition of information*, „International Journal of Computer Mathematics" 1968, 2:1–4, s. 157–168.

A.N. Kolmogorov, *On Tables of Random Numbers*, „Theoretical Computer Science" (1998) [1963], 207 (2).

Kołodziej-Durnaś A., *Kultura organizacji – idea i instrumentalizacja*. *Socjologiczne studium krytyczne*, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2012.

Kostera M., *Antropologia organizacji. Metodologia badań terenowych*, Wydawnictwo Naukowe PWN, Warszawa 2003.

Kostera M., Glinka B., *Wstęp*, [w:] *Nowe kierunki w organizacji i zarządzaniu* (red.) M. Kostera, B. Glinka Wyd. II, Wolters Kluwer, Warszawa 2016.

Kostera M., Krzyworzeka P., Połeć M., *Antropologia organizacji. Jak prowadzić badania terenowe?* Wydawnictwo Naukowe PWN, Warszawa 2023.

Kostera M., *Postmodernizm w zarządzaniu*, Polskie Wydawnictwo Ekonomiczne, Warszawa 1996.

Kostera M., *Studium przypadku a edukacja zarządzania,* [w:] *O zarządzaniu historie niezwykłe: studia przypadków z zarządzania humanistycznego*, (red.) M. Kostera, Difin, Warszawa 2014.

Kotarbiński T., *Traktat o dobrej robocie*, Zakład Narodowy im. Ossolińskich, Wrocław-Warszawa 1958.

Kour R., Karim R., Thaduri A., *Cybersecurity for railways – A maturity model*, Proceedings of the Institution of Mechanical Engineers. Part F-Journal of Rail and Rapid Transit, Article Number: UNSP 0954409719881849, 2019.

Koźmiński A.K., Jemielniak D., Latusek D., *Współczesne spojrzenie na organizację*, E-mentor, nr 3, 2009.

Koźmiński A.K., Latusek-Jurczak D., *Rozwój teorii organizacji. Od systemu do sieci*, Poltex, Warszawa 2017.

Koźmiński A.K., Obłój K., Zarys teorii równowagi organizacyjnej, PWE, Warszawa 1989.

Koźmiński A.K., *Zarządzanie systemowe*, PWE, Warszawa 1971.

Kożuch A., Kożuch B., Sułkowski Ł., Bogacz-Wojtanowska E., Lewandowski M., Sienkiewicz-Małyjurek K., Szczudlińska-Kanoś A., Jung-Konstanty S., *Obszary zarządzania publicznego,* Instytut Spraw Publicznych UJ (Monografie i Studia Instytutu Spraw Publicznych Uniwersytetu Jagiellońskiego), Kraków 2016.

Kożuch B., Sienkiewicz-Małyjurek K., Sułkowski Ł., *Zarzadzanie publiczne oparte na wartościach*, Wydawnictwo Społecznej Akademii Nauk, Łódź 2021.

Kożuch B., *Zarządzanie publiczne w teorii i praktyce polskich organizacji*, Wydawnictwo Placet, Warszawa 2004.

Krippendorf K., *Content analysis. An introduction to its methodology*, Wyd. II, Sage, Thousand Oaks 2004.

Krukowski K., *Cechy kultury organizacyjnej na różnych poziomach dojrzałości procesowej wybranych urzędów miast*, Optimum. Economic Studies, nr 1(91), 2018

Krzakiewicz K, Cyfert S., *Podstawy zarządzania organizacjami*, Poznań University of Economics and Business, 2020.

Krzyworzeka P., *Kultura i organizacje,* [w:] Perspektywa antropologiczna. Nowe kierunki w organizacji i zarządzaniu, (red.) B. Glinka, M. Kostera, Wolters Kluwer 2016.

Krzyworzeka P., *Kultura organizacyjna – ślepa uliczka teorii organizacji*, „Master of Business Administration" 2012, Nr 1.

Krzyżanowski L., *Podstawy nauk o zarządzaniu*, Wydawnictwo Naukowe PWN, Warszawa 1994.

Kuper A., Kołbon I., *Kultura : Model Antropologiczny*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2005.

Lane J.E., *New public management: an introduction*, Routledge 2002.

Leavitt H.J., *Applied organizational change in industry: Structural and humanistic approaches,* Carnegie Institute of Technology, Graduate School of Industrial Administration, 1962.

Lehto M., Limnell J., *Cyber Security Capability and the Case of Finland,* Proceedings of the 15th European Conference on Cyber Warfare and Security (Eccws 2016), 2016.

Lenart-Gansiniec R., *Systematyczny przegląd literatury w naukach społecznych : przewodnik dla studentów, doktorantów i nie tylko*, Wydawnictwo Naukowe Scholar, Warszawa 2021.

Likert R., Likert J., *New Ways of Managing Conflict*, McGraw–Hill, New York 1976.

Likert R., *New Patterns of Management*, McGraw–Hill, New York 1961.

Lin, C. Wittmer J.L.S., Luo X.R., *Cultivating Proactive Information Security Behavior and Individual Creativity: The Role of Human Relations Culture and IT Use Governance*, „Information & Management" 2022, Vol. 59 (6).

Linneberg M.S., Korsgaard S., *Coding qualitative data: A synthesis guiding the novice*, „Qualitative Research Journal", Vol. 19, No. 3, 2019.

Ližbetinová L., Lorincová S., Caha Z., *The Application of the Organizational Culture Assessment Instrument (OCAI) to Logistics Enterprises*, „NAŠE MORE: znanstveni časopis za more i pomorstvo" 2016, 63(3).

Lundgren B., Möller N., *Defining Information Security*, „Sci Eng Ethics" 2019, Vol. 25.

Maier A., Moultrie J., Clarkson P., *Assessing Organizational Capabilities: Reviewing and Guiding the Development of Maturity Grids*, „IEEE Transactions on Engineering Management" 2012, Vol. 59.

Marek A., *Model wartości konkurujących w badaniu kultury organizacji samorządowych (The model of competing values in the study of the culture of local government organizations)*, „Roczniki Ekonomii i Zarządzania" 2014, 6(42).

Matejun M., *Metody, techniki i narzędzia gromadzenia danych w badaniach mieszanych*, [w:] *Metody badań mieszanych w naukach o zarządzaniu*, (red.) Ł. Sułkowski, R. Lenart-Gansiniec, Wydawnictwo Naukowe Akademii WSB, Dąbrowa Górnicza 2023.

Mazur B., *Kultura organizacyjna w perspektywie poznawczej. Próba operacjonalizacji*, [w:] *Metody zarządzania kulturą organizacyjną*, (red.) Ł. Sułkowski, C. Sikorski, Wydawnictwo Difin, Warszawa 2014.

Mazur B., *Kultura organizacyjna w zróżnicowanym wyznaniowo otoczeniu,* Oficyna Wydawnicza Politechniki Białostockiej, Białystok 2012.

Megasyah, Y., Arifnur, A., *Academic information system security audits using Cobit 5 framework domains APO12, APO13 and DSS05*, „Journal of Applied Engineering and Technological Science" 2020, Vol 1(2).

Miller D., *Paradigm prison, or in praise of aheoretic research*, „Strategic Organizations" 2007, nr 5.

Minn H., Zeng M., Bhargava V., *Towards a definition of the Internet of Things (IoT)*, IEEE Internet Initiative 2015.

Mirtsch M., *Adoption of the information security management system standard ISO/IEC 27001: a study among German organizations*, „International Journal for Quality Research" 2023, 17(3).

Mirtsch M., Blind K., Koch C., Dudek G., *Information security management in ICT and non-ICT sector companies: A preventive innovation perspective*, „Computers & Security" 2021, Vol. 109.

Mitroff I.I., *Stakeholders of organizational mind*, Jossey-Bass, San Francisco 1983.

Młodzik L., *Kultura organizacyjna w instytucji publicznej*, Wydawnictwo Stowarzyszenia Maximus Primus, Zielona Góra 2014.

Mohamed N, Kaur A/P Gian Singh J., *A Conceptual Framework for Information Technology Governance Effectiveness in Private Organizations*, „Information Management & Computer Security" 2012, Vol. 20, nr 2.

Molina-Azorín J.F., López-Gamero M.D., *Mixed methods studies in environmental management research: Prevalence, purposes and designs*, „Business Strategy and the Environment" 2016, 25(2).

Morgan G., *Obrazy organizacji*, PWN, Warszawa 1997.

Muraszkiewicz M., *Społeczeństwo informacyjne i praca*, [w:] *Społeczeństwo informacyjne i jego technologie*, (red.) B. Sosińska-Kalata, K. Materska, W. Gliński, Wydawnictwo SBP, Warszawa 2004.

Murphey M.G., *The Development of Peirce's Philosophy*, Harvard University Press: Cambridge, MA, USA, 1961.

Myszewski J.M., *Zarządzanie zmiennością. Systemowe spojrzenie na metody statystyczne w zarządzaniu jakością*, Orgmasz, Warszawa 1998.

Niekerk J.F. van, Solms R. von, Information Security Culture: A Management Perspective, „Computers & Security" 2010, Vol. 29 (4).

Niemczyk J., Metodologia nauk o zarządzaniu, [w:] Podstawy metodologii badań w naukach o zarządzaniu, (red.) W. Czakon, Wolters Kluwer, Warszawa 2015.

Niemiec A., *Możliwość zastosowania analizy istotności-osiągnięć w identyfikacji i ewaluacji zestawu kluczowych mierników dokonań (KPIs)*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego, nr 873. Finanse, Rynki Finansowe, Ubezpieczenia" 2015, 77.

Nonaka I., Takeuchi H., *The Knowledge-Creating Company*, Oxford University Press, Oxford, UK 1995.

Nowosielski S., *Podejście procesowe w organizacjach*, Wydawnictwo Uniwersytetu Ekonomicznego, Wrocław 2009.

Obenchain A.M., Johnson W.C., Dion P.A., *Institutional Types, Organizational Cultures, and Innovation in Christian Colleges and Universities*, „Christian Higher Education" 2004, 3:1.

Omerzel D., Biloslavo R., Trnavcevic A., *Knowledge management and organisational culture in higher education institutions*, „Journal for East European Management Studies" 2011, Vol. 16.

Pallant J., *SPSS Survival Manual: A step by step guide to data analysis using SPSS*, Open University Press, Edycja 4, listopad 2010.

Pasmore W.,Winby S., Mohrman S.A., Vanasse R., *Reflections: Sociotechnical Systems Design and Organization Change*, „Journal of ChangeManagement" 2019, 19/2.

Patapas A., Labenskyte G., *Research of organisational culture and values of state tax inspectorate of N county*, "Public Policy and Administration" 2011, Volume 10, Issue 4.

Paul S.P., Shruti *A.*, *A Systematic Analysis of Research Trends on Network Control System in Wireless Sensor Network*, 2022, 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Advanced Computing and Communication Systems (ICACCS), 2022 8th International Conference on 1 (March).

Paulk M.C., Curtis B., Chrissis M.B., Weber C.V., *Capability Maturity Model for Software, version 1.1. CMU/SEI-93-TR-24*, Pittsburgh: Carnegie Mellon University, Software Engineering Institute, Pittsburgh 1993.

Paulk M.C., Curtis B., Chrissis M.B., Averill E.L., Bamberger J., Kasse T.C., Konrad M.D., Perdue J.R., Weber C.V., Withey J.V., *Capability Maturity Model for Software*. CMU/SEI-91-TR-24, Carnegie Mellon University, Software Engineering Institute, Pittsburgh 1991.

Pawluczuk A., Ryciuk U., *Variables Shaping the Culture in Organizational Learning in Municipalities*, International Journal of Contemporary Management, Vol. 14, No. 2, 2015.

Penc J., *Strategiczny system zarządzania*, Placet, Warszawa 2001.

Pérez-González D., Preciado S.T., Solana-Gonzalez P., *Organizational Practices as Antecedents of the Information Security Management Performance: An Empirical Investigation*, „Information Technology & People" 2019, Vol. 32 (5).

Perrow C., *A Society of Organizations*, „Theory and Society" 1991, vol. 20, nr 6.

Peters T., *Management systems: The language of organizational character and competence*, „Organizational Dynamics" 1980, Vol. 9, No. 1.

Peters T.J., *Business Policy in Action,* „Management decision" 1993, Vol. 31 No. 6.

Pinheiro M.G., Misaghi M., *Proposal of a Framework of Lean Governance and Management of Enterprise IT*, Proceedings of the 16th International Conference on Information Integration and Web-Based Applications & Services – IiWAS '14, 2014.

Piotrowski W., *Organizacje i zarządzanie – kierunki, koncepcje, punkty widzenia*, [w:] *Zarządzanie: Teoria i praktyka*, (red.) A. Koźmiński, W. Piotrowski, Warszawa 2002.

Plecka D., Młodzik L., *Kulturowe uwarunkowania zarządzania wiedzą w organizacjach publicznych*, „Studia Iuridica" 2022, vol. 92.

Podgórniak-Krzykacz A., *The relationship between the professional, social, and political experience and leadership style of mayors and organisational culture in local government. Empirical evidence from Poland,* „PLoS ONE" 2021, 16(12).

Podrecca M., Culot G., Nassimbeni G., Sartor M., *Information security and value creation: The performance implications of ISO/IEC 27001,* „Computers in Industry" 2022, 142.

Pollini A., Tiziana C.C., Tedeschi A., Ruscio D., Save L., Chiarugi F., Guerri D., *Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach, Cognition,* „Technology & Work" 2022, 24, nr 2.

Qodarsih N., Yudhoatmojo S.B. and Hidayanto A.N., *Master Data Management Maturity Assessment: A Case Study in the Supreme Court of the Republic of Indonesia,* 2018 6th International Conference on Cyber and IT Service Management (CITSM), Parapat, Indonesia, 2018.

Quinn R. Spreitzer G., *The Psychometric of the Competing Values Culture Instrument and an Analysis of the Impact of Organizational Culture on Quality of Life*, [w:] *Research in Organizational Change and Development*, (red.) W.R. Woodman, W.A. Pasmore, Vol. 5 1991, JAI Press, Greenwich.

Rakowska A.A., *Human-Robot Interactions in the Workplace – Key Challenges and Concerns*, „Annales Universitatis Mariae Curie-Skłodowska, sectio H – Oeconomia" 2022, 56, 1.

Rea-Guaman A.M., San Feliu T., Calvo-Manzano J.A., Sanchez-Garcia I.D., *Comparative Study of Cybersecurity Capability Maturity Models,* Conference: International Conference on Software Process Improvement and Capability Determination, September 2017.

Reijers H.A., *Business Process Management: The evolution of a discipline,* „Computers in Industry" 2021, Vol. 126.

Rosemann M., de Bruin T., Hueffner T., *A Model for Business Process Management Maturity*, ACIS 2004 Proceedings, 6.

Sajdera J., *Application of the "textual laboratory" tools of the MaxQda computer program in scientific research – comparative analysis of Polish and foreign research reports,* „E-mentor" 2023, Nr 1.

Saldana J., *The Coding Manual for Qualitative Researchers,* Thousand Oaks 2015, Sage Publications.

Schein E.H., *Culture: The missing concept in organization studies*, „Administrative Science Quarterly 1996", nr 41(2).

Schein E.H., *Organizational Culture and Leadership*, Jossey-Bass Publisher, San Francisco– Washington–London 1985.

Schein E.H., *Organizational culture and leadership, Edycja 3. Jossey-Bass, 2004.*

Schmitz Ch, Schmid M., Harborth D., Pape S., *Maturity Level Assessments of Information Security Controls: An Empirical Analysis of Practitioners Assessment Capabilities*, „Computers & Security" 2021, 108.

Shah S.N., *Understanding medical practice cybersecurity risks: Mitigations for the digital health era*, [w:] Risk Management, Liability Insurance, and Asset Protection Strategies for Doctors and Advisors: Best Practices from Leading Consultants and Certified Medical Planners, CRC Press 2015.

Shannon C., *A Mathematical Theory of Communication*, „Bell System Technical Journal" 1948, 27.

Sharma S., Aparicio E., *Organizational and Team Culture as Antecedents of Protection Motivation among IT Employees*, „Computers & Security" 2022, 120.

Shetreet S., *Creating A Culture of Judicial Independence: The Practical Challenge and the Conceptual and Constitutional Infrastructure*, [w:] *The culture of judicial independence: Conceptual foundations and practical challenges*, S. Shetreet, C. Forsyth (red.), Martinus Nijhoff, Boston 2011.

Siemiński M., Krukowski K., Szamrowski P., *Kształtowanie kultury organizacyjnej w administracji publicznej na przykładzie urzędów miast*, Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego, Olsztyn 2014.

Sikorski C., *From Reducing Uncertainty to Dealing with Uncertainty. Change of Function of Organizational Culture*, „Edukacja Ekonomistów i Menedżerów" 2017, Tom 46, Nr 4.

Sikorski C., *Kształtowanie kultury organizacyjnej. Filozofia, strategie, metody*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2009.

Sikorski C., *Nauka o zarządzaniu*, Wydawnictwo AHE, Łódź 2009.

Sikorski Cz, *Kultura organizacyjna*, Wydawnictwo C.H. Beck, Warszawa 2002.

Simonet D., *The new public management theory and the reform of European health care systems: An international comparative perspective*, „International Journal of Public Administration" 2011, 34(12).

Singh A.N., Gupta M.P., *Information Security Management Practices: Case Studies from India*, „Global Business Review" 2019, Vol. 20 (1).

Siponen M., *A conceptual foundation for organizational information security awareness*, „Information Management & Computer Security" 2000, nr 8(1).

Sitko-Lutek A., *Aspekty złożoności kultury organizacyjnej*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2018.

Sitko-Lutek A., op. cit., s. 83; B. Heritage, C. Pollock, L. Roberts, *Validation of the Organizational Culture Assessment Instrument*, „PLoS ONE" 2014, 9(3).

Sjöstrand S.E., *Företagsledning*, [w:] *Organisationsteori pa svenska*, (red.) B. Czarniawska, Liber, Malmö 1998

Skalik J., Barabasz A., Bełz G., *Systemowe uwarunkowania rozwoju metod zarządzania. Przykład modelu Triady*, „Acta Universitatis Lodziensis. Folia Oeconomica" 2010, 234.

Smagowicz J., Kosieradzka A., *Analiza porównawcza modeli dojrzałości organizacji*, [w:] *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego*, (red.), M. Ćwiklicki, M. Jabłoński, S. Mazur Stanisław, Fundacja Gospodarki i Administracji Publicznej, Kraków 2016.

Smircich L., *Concepts of Culture and Organizational Analysis,* „Administrative Science Quarterly" 1983, Vol. 28(3).

Smircich L., *Studing Organisations as Cultures,* [w:] G. Morgan, *Beyond Method: Strategies for Social Research*, Beverly Hills London ñ New Delhi 1983; C. Geertz, *The Interpretation of Culture*, Basic Book, London 1973.

Snyder H., *Literature review as a research methodology: An overview and guidelines*, „Journal of Business Research" 2019, Vol. 104.

Sommestad T., *Work-Related Groups and Information Security Policy Compliance*, „Information & Computer Security" 2018, Vol. 26 (5).

Sompór-Świderska J, *Diagnoza kultury organizacyjnej uniwersytetu: elastyczne podejście do kierunków zmian i nowych wyzwań*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu nr 249,Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2012.

Son J.-Y., Kim S.S., *Internet users' information privacy-protective responses: A taxonomy and a nomological model*, „MIS Quarterly" 2009, Vol. 32, No. 3.

Soomro Z.A., Shah M.H., Ahmed J., *Information Security Management Needs More Holistic Approach: A Literature Review*, „International Journal of Information Management" 2016, 36 (2).

Sousa M., Raposo M.J., Mendonça J., Corchuelo B., *Exploring organisational culture in higher educational institutions: a comparative study*, „International Journal of Management in Education" 2022, Volume 16, Issue 1.

Spruit M., Roeling M., *ISFAM: The information security focus area maturity model*, [w] Proceedings of the European Conference on Information Systems (ECIS) 2014,Tel Aviv, Izrael 2014.

Spruit M., Slot G., *ISFAM 2.0: Revisiting the Information Security Assessment Model*, [w] *Security Risks: Assessment, Management and Current Challenges*, Springer: Cham, Szwajcaria, 2017.

Stabryła A., *Analiza systemowa procesu zarządzania*, PAN, Zakład Narodowy im. Ossolińskich, Wrocław 1984.

Stachowiak H., *Allgemeine Modelltheorie,* Springer–Verlag, Wien New York 1973.

Stefanowicz B., *Informacja,* Oficyna Wydawnicza SGH, Warszawa 2004.

Steuperaert D., *COBIT 2019: A Significant Update,* „EDPACS" 2019, 59(1).

Stoll M., *An Information Security Model for Implementing the New ISO 27001*, Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications, edited by Information Resources Management Association, IGI Global, 2019.

Strengers J., Mutsaers L., van Rossum L,, Graamans E., *The organizational culture of scale-ups and performance*, „Journal of Organizational Change Management" 2022, Vol. 35, No. 8.

Sułkowski Ł, Lenart-Gansiniec R., *Metody badań mieszanych w naukach o zarządzaniu*, (red.) Ł. Sułkowski, R. Lenart-Gansiniec, Wydawnictwo Naukowe Akademii WSB, Dąbrowa Górnicza 2023.

Sułkowski Ł., *Functionalistic models of organizational culture,* „Przedsiębiorczość i Zarządzanie" 2014, Wydawnictwo SAN, tom XV, zeszyt 10, część II.

Sułkowski Ł., *Funkcjonalistyczna wizja kultury organizacyjnej w zarządzaniu – dominujący paradygmat i jego krytyka*, „Problemy Zarządzania" 2013, vol. 11, nr 4 (44).

Sułkowski Ł., *Interpretatywne koncepcje zarządzania – sensemaking, enactment oraz management of meaning,* „Przegląd Organizacji" 2012, Nr 12 (875).

Sułkowski Ł., *Kultura organizacji publicznej* [w:] *Instrumentarium zarządzania publicznego*, (red.) B. Kożuchowska, Ł. Sułkowski, Difin, Warszawa 2015.

Sułkowski Ł., *Kultura organizacyjna od podstaw,* Społeczna Akademia Nauk, Łódź 2020.

Sułkowski Ł., *Kulturowa zmienność organizacji*, PWE, Warszawa 2002.

Sułkowski Ł., *Organizacja jako przedmiot badań nauk o zarządzaniu,* Przedsiębiorczość i Zarządzanie 2012, tom XIII, zeszyt 2, Wydawnictwo SAN, Łódź 2012.

Sułkowski Ł., *Paradygmaty nauk o zarządzaniu*, „Współczesne Zarządzanie" 2013, nr 2.

Sułkowski Ł., *Wieloznaczność kultury organizacyjnej*, „Przedsiębiorczość i Zarządzanie" 2012, Wydawnictwo SAN, TOM XIII, Zeszyt 12.

Sułkowski Ł., *Zmiana kultury organizacyjnej – paradygmaty, modele i metody zarządzania*, [w:] *Metody zarządzania kulturą organizacyjną*, (red.) Ł. Sułkowski, Cz. Sikorski, Wydawnictwo Difin, Warszawa 2014.

Susanto H., Nabil Almunawar M., Tuan Y., *Information Security Management System Standards: A Comparative Study of the Big Five*, „International Journal of Engineering and Computer Science" 2011, Vol. 11.

Szeptuch A., *Pomiar kultury organizacyjnej w organizacjach ochrony zdrowia,* „e-Mentor" 2016, [s. l.], vol. 65, 3.

Szmit M., Szmit A., *O normatywnych definicjach cyberbezpieczeństwa*, [w:] *Bezpieczeństwo Polski w drugiej dekadzie XXI wieku,* (red.) K. Załęski, P. Polko, Akademia WSB, Dąbrowa Górnicza 2019.

Szybiński L., *Projektowanie organizacji i systemu zarządzania, cz. I*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 1984.

Śliwa M., Kostera M., *Zarządzanie w XXI wieku. Jakość, twórczość, kultura*, Wolters Kluwer, Warszawa 2012.

Świątek-Barylska, *Lojalność pracowników współczesnych organizacji*, Istota i elementy składowe, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2013.

Tang M., Li T., Zhang M., *The impacts of organizational culture on information security culture: A case study*, „Information Technology and Management" 2016, Vol. 17(2).

Tarhan A., Turetken O., Reijers H.A., *Business process maturity models: A systematic literature review*, „Information and Software Technology" 2016, Vol. 75.

Tavakol M., Dennick R., *Making Sense of Cronbach's Alpha*, „International Journal of Medical Education" 2011, Vol. 2.

Thakare S.V., Gore D.V., *Comparative study of CIA and revised-CIA algorithm*, Proceedings – 2014, 4th International Conference on Communication Systems and Network Technologies, CSNT 2014, art. no. 6821492.

Thomson K., Niekerk J. van, *Combating Information Security Apathy by Encouraging Prosocial Organisational Behaviour*, „Information Management & Computer Security" 2012, 20 (1).

Tiller J.S., Fish B.D., *Packet sniffers and network monitors*, [w:] *Information security management handbook* 5th ed. (red.) H.F. Tipton, M. Krause, Boca Raton, Auerbach 2004.

Toffler A., *Trzecia fala*, Książka i Wiedza, Warszawa 1986.

Tolah A., Furnell S.M., Papadaki M., *An Empirical Analysis of the Information Security Culture Key Factors Framework*, „Computers & Security" 2021, Vol. 108.

Trzcieniecki J., *Projektowanie systemów zarządzania*, PWN, Warszawa 1980.

Uchendu B., Nurse J. R. C., Bada M., Furnell S., *Developing a Cyber Security Culture: Current Practices and Future Needs*, „Computers & Security" 2021, Vol. 109.

van der Spek R., Spijkervet A., *Knowledge Management: Dealing Intelligently with Knowledge*, CIBIT, Utrecht 1997.

Nguyen V.H., Nguyen T.H.T., Nguyen L.T.A., Nguyen T.H.A., Nguyen T.P., Nguyen T.C., Pham D.M., *The validation of organisational culture assessment instrument in healthcare setting: results from a cross-sectional study in Vietnam*, „BMC Public Health" 2020, 20, 316.

van Looy A., Backer M., Poels G., *Defining business process maturity*. *A journey towards excellence,* „Total Quality Management" 2011, Vol. 22

van Looy A., *Business Process Maturity – A Comparative Study on a Sample of Business Process Maturity Models*, Springer Briefs in Business Process Management, 2014.

van Steenbergen M., Bos R., Brinkkemper S., van de Weerd I., Bekkers W., *The Design of Focus Area Maturity Models*, Global Perspectives on Design Science Research, 5th International Conference, DESRIST 2010, St. Gallen, Switzerland, June 4–5, 2010, Proceedings, 6105.

van Wessela R., Yangb X., de Vriesa H.J., *Implementing international standards for Information Security Management in China and Europe: A comparative multi-case study*, „Technology Analysis & Strategic Management" 2011, Vol. 23/8.

Vasyakin B., Ivleva M., Pozharskaya Y.L., Shcherbakova O.I., A s*tudy of the Organizational Culture at a Higher Education Institution (Case Study: Plekhanov Russian University of Economics),* „International Journal of Environmental and Science Education" 2016, 11.

von Bertalanffy L., *General System Theory*, George Brazziler, New York 1968.

von Bertallanfy L., *Ogólna teoria systemów*. *Podstawy, rozwój, zastosowania*, PWE, Warszawa 1984.

von Solms R., van Niekerk J., *From information security to cyber security*, „Computers & Security" 2013, 38(0).

Vroom C., von Solms R., *Towards information security behavioural compliance*, „Computers and Security", 2004, Vol. 23, No. 3.

Waterman R., Peters T., Phillips J., *Structure is not organization*, Business Horizons, 1980.

Weber C., Curtis B., Gardiner T., *Business Process Maturity Model (BPMM)* Version 1.0, 2008.

Weber M., *The Theory of Social and Economic Organization*, The Free Press, New York 1965.

Weick K.E., *The Social Psychology of Organizing*, Random House 1979.

Wheatley M.J, *Leadership and the New Science. Discovering Order in a Chaotic World*, Berret-Koehler Publishers, San Francisco 1999.

Whorton J.W., Whorton J.*A., A perspective on the challenge of public management: Environmental paradox and organizational culture*, „Academy of Management Review" 1981, nr 6.3.

Widharto P., Suhatman Z., Aji R. F., *Measurement of information technology governance capability level: a case study of PT Bank BBS*, „TELKOMNIKA Telecommunication Computing Electronics and Control" 2022, Vol. 20, No. 2

Wiener N., *Cybernetics or Control and Communication in the Animal and the Machine (1948)*, MIT Press, Wyd. II, Massachusetts 1961.

Willmott H., *Strength is ignorance; slavery is freedom: Managing culture in modern organizations*, „Journal of Management Studies" 1993, Nr 30/4.

Wilson K.S., *Conflicts among the pillars of information assurance*, „IT Professional" 2013, 15 (4).

Witkowska D., *Wybrane metody ilościowe w finansach*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2023.

Wolniak R., *The level of maturity of quality management systems in Poland-Results of empirical research*, Sustainability (Switzerland), 2019, 11(15).

Wright S., *The politization of „culture"*, „Anthropology Today" 1998, Vol. 14(1).

Wudarzewski G., *Validation of Cameron and Quinn's Organizational Culture Assessment Instrument (OCAI) in Polish conditions*, „Central and Eastern European Journal of Management and Economics" 2018, Vol. 6, No. 1.

Yiğit Özkan B., Lingen S., Spruit M., *The Cybersecurity Focus Area Maturity (CYSFAM) Model*, „Journal of Cybersecurity and Privacy" 2021, Vol. 1.

Yiğit Özkan B., Spruit M., Wondolleck R., Burriel Coll V., *Modelling adaptive information security for SMEs in a cluster*, „Journal of Intellectual Capital" 2019, Vol. 21, No. 2.

Zbiegień-Maciąg L., *Kultura w organizacji: Identyfikacja kultur znanych firm*, PWN, Warszawa 1999.

Zieleniewski J., *Organizacja i zarządzanie*, PWE, Warszawa 1979.

Zioło M., Niedzielski P., Kuzionko-Ochrymiuk E., Marcinkiewicz J., Łobacz K., Dyl K., Szanter R., *E-Government Development in European Countries: Socio-Economic and Environmental Aspects*, „Energies" 2022, 15, 8870.

Załącznik 1. Kwestionariusz wywiadu

Szanowna Pani Dyrektor / Szanowny Panie Dyrektorze

Prowadzę badania w ramach pracy naukowej poświęconej wpływowi kultury organizacyjnej na zarządzanie bezpieczeństwem informacji. Zwracam się do Pani/Pana z prośbą o udział w wywiadzie. Zapewniam o anonimowości badań – ich wyniki zostaną wykorzystane wyłączenie do celów naukowych.

Pytanie nr 1

Kto w sądzie z najwyższego kierownictwa jest odpowiedzialny za **system zarządzania bezpieczeństwem informacji** (skrót: **SZBI)**?

Pytanie nr 2

Na podstawie zaleceń jakiego dokumentu został opracowany system zarządzania bezpieczeństwem informacji?

Pytanie nr 3

W jaki sposób informuje się pracowników sądu o ustanowieniu SZBI? W jaki sposób informuje się pracowników sądu o zmianach SZBI?

Pytanie nr 4

Jak często przeprowadzane są przeglądy SZBI? Kto jest odpowiedzialny za te przeglądy?

Pytanie nr 5

W jaki sposób kierownictwo sądu angażuje się w utrzymanie SZBI?

Pytanie nr 6

Jak zadziałał system zarządzania bezpieczeństwa informacji w trakcie ostatniego zapamiętanego przez Panią/Pana incydentu związanego z bezpieczeństwem informacji? Czy zostały wprowadzone zmiany w SZBI po zaistniałym incydencie?

Pytanie nr 7

Czym dla Pani/Pana jest kultura organizacyjna?

Pytanie nr 8

Kto Pani/Pana zdaniem ma największy wpływ na kształtowanie się kultury organizacyjnej w sądzie?

Pytanie nr 9

Czy Pani/Pana zdaniem można mówić o wpływie kultury organizacyjnej na zarządzania bezpieczeństwem informacji w sądzie?

Pytanie nr 10

Czy Pani/Pan uważa, że w sądzie można mówić o kulturze bezpieczeństwa informacji i danych osobowych? Jakie postawy, zachowania współpracowników w codziennej praktyce o niej świadczą?

Dziękuję za poświęcony czas i udzielone odpowiedzi.

Załącznik 2. Badanie dokumentów dotyczących systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych

1. Czy ustanowiono udokumentowany System Zarządzania Bezpieczeństwem Informacji w Sądzie (SZBI)?
2. Z ilu stron składa się dokument opisujący SZBI?

   ……
3. Jaka jest struktura dokumentu opisującego SZBI (z ilu i jakich rozdziałów/załączników się składa)?

   ……..
4. Czy w dokumencie ustanawiającym SZBI określono, jakim informacjom należy zapewnić bezpieczeństwo?
5. Czy w dokumencie ustanawiającym SZBI uwzględniono zewnętrzne przepisy prawne?
6. Czy w dokumencie ustanawiającym SZBI uwzględniono wewnętrzne regulacje?
7. Czy w dokumencie ustanawiającym SZBI wskazano techniki wykorzystywane do zapewnienia bezpieczeństwa informacji?
8. Czy w dokumencie ustanawiającym SZBI określono interesariuszy SZBI?
9. Czy w dokumencie ustanawiającym SZBI określono zasady wymiany informacji między sądem a innymi organizacjami?
10. Czy w SZBI istnieją zapisy o zasadach przydzielania i odbioru uprawnień do systemów informatycznych?
11. Czy w SZBI istnieją zapisy o zasadach „pracy zdalnej”?
12. Czy SZBI zawiera dodatkowe regulacje dotyczące bezpieczeństwa danych osobowych przetwarzanych w sądzie?

13. Czy SZBI zawiera procedury zgłaszania incydentów dotyczących bezpieczeństwa informacji i prywatności?
14. Czy SZBI zawiera plan ciągłości działania?
15. Czy SZBI zawiera procedury odzyskiwania kluczowych systemów?
16. Czy zintegrowano planowanie, projektowanie, wdrażanie i monitorowanie procedur bezpieczeństwa informacji i prywatności wymienione w pytaniach 13, 14, 15?
17. Czy kierownictwo wskazało w sposób udokumentowany osobę (lub osoby) do wdrożenia, monitorowania zmian w regulacjach wewnętrznych i przepisach prawa dotyczących SZBI i aktualizowania SZBI?
18. Czy istnieje w sądzie dokumentacja potwierdzająca dokonywanie przeglądów dokumentacji SZBI?
19. Jak często przeprowadzane są przeglądy dokumentacji SZBI?

……

20. Czy zdefiniowane są role i obowiązki dotyczące zarządzania bezpieczeństwem informacji w sądzie?
21. Czy informacje o procesach zawarte w SZBI zawierają wskazanie ról z podziałem na osoby odpowiedzialne za wykonanie procesu (R) oraz osoby sprawujące nadzór nad tym procesem (A)?
22. Czy w SZBI wskazano częstotliwość uczestnictwa w obowiązkowych szkoleniach uświadamiających zagrożenia związane z bezpieczeństwem informacji?
23. Czy sformułowano plan postępowania z ryzykiem w zakresie bezpieczeństwa informacji dostosowany do celów i struktury organizacyjnej sądu?
24. Czy utrzymuje się plan postępowania z ryzykiem w zakresie bezpieczeństwa informacji dostosowany do celów i struktury organizacyjnej sądu?

25. Czy zapewnia się/uzasadnia się, że plan (postępowania z ryzykiem w zakresie bezpieczeństwa informacji) określa odpowiednie praktyki zarządzania i rozwiązania w zakresie bezpieczeństwa, biorąc pod uwagę zasoby, odpowiedzialność i priorytety, w zakresie zarządzania zidentyfikowanym ryzykiem bezpieczeństwa informacji?

26. Czy istnieje udokumentowany sposób zarządzania ryzykiem związanym z bezpieczeństwem informacji?

27. Czy zarządzanie ryzykiem związanym z bezpieczeństwem informacji jest składową zarządzania ryzykiem działalności sądu?

28. Czy określono sposób pomiaru skuteczności praktyk dotyczących zarządzania bezpieczeństwem informacji?

29. Jakie mierniki zastosowano do pomiaru skuteczności praktyk dotyczących zarządzania bezpieczeństwem informacji?

    …….

    …….

30. Czy istnieją dokumenty potwierdzające przeglądy skuteczności SZBI w zaplanowanych odstępach czasu?

31. Czy istnieją dokumenty potwierdzające audyty SZBI w zaplanowanych odstępach czasu?

32. Czy istnieją dokumenty potwierdzające regularne przeglądy SZBI przez kierownictwo sądu, aby zapewnić, że zakres SZBI pozostaje odpowiedni oraz aby zidentyfikować możliwe usprawnienia w ustanowionych procesach SZBI?

33. Czy istnieją udokumentowane informacje o wkładzie kierownictwa sądu w utrzymanie SZBI?

Załącznik 3. Kwestionariusz ankiety

Webankieta

Ankieta

Blok opisowy

Szanowna Pani/ Szanowny Panie
Aktualnie prowadzę badania do pracy naukowej poświęconej wpływowi kultury organizacyjnej na zarządzanie bezpieczeństwem informacji. Zwracam się do Pani/Pana z prośbą o wypełnienie ankiety. Zapewniam o anonimowości badań, ich wyniki zostaną wykorzystane tylko i wyłączenie do celów naukowych. Badanie składa się z 2 części, wypełnienie ankiety zajmuje około 15 minut.
Z poważaniem
Aneta Kaczmarek

Blok opisowy

Część 1
Kwestionariusz do oceny kultury organizacyjnej
Na każde z sześciu pytań podano cztery odpowiedzi, między które należy rozdzielić 100 punktów. Najwięcej punktów proszę przypisać odpowiedzi, która jest najbliższa sytuacji panującej w Państwa Organizacji/Sądzie.

W pytaniach z opisem „**Stan obecny**" proszę rozdzielić 100 punktów między cztery odpowiedzi w zależności od tego, w jakim stopniu dana odpowiedź odzwierciedla obecną sytuację w Państwa Sądzie.
W pytaniach z opisem „**Stan pożądany**" proszę rozdzielić 100 punktów między cztery odpowiedzi, zgodne z Pani/Pana wizją pożądanej sytuacji w Państwa Sądzie, by był przykładem sprawnego funkcjonowania.

1a. Jaka jest ogólna charakterystyka organizacji?

Stan obecny
Każdej odpowiedzi można przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musi się równać 100.

Organizacja jest miejscem osobistego spotkania. Przypomina wielką rodzinę. Ludzie mocno się angażują.

Dominującymi cechami organizacji są energia i przedsiębiorczość. Ludzie chętnie podejmują ryzyko.

W organizacji liczą się przede wszystkim wyniki. Główną troską jest jak najlepsze wykonywanie zadań. Pracownicy są bardzo ambitni i nastawieni na osiągnięcia.

W organizacji obowiązuje ścisła hierarchia i kontrola. Tym, co robią ludzie, zazwyczaj rządzą formalne procedury.

1b. Jaka jest ogólna charakterystyka organizacji?

Stan pożądany

Każdej odpowiedzi można przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musi się równać 100.

Organizacja jest miejscem osobistego spotkania. Przypomina wielką rodzinę. Ludzie mocno się angażują.

Dominującymi cechami organizacji są energia i przedsiębiorczość. Ludzie chętnie podejmują ryzyko.

W organizacji liczą się przede wszystkim wyniki. Główną troską jest jak najlepsze wykonywanie zadań. Pracownicy są bardzo ambitni i nastawieni na osiągnięcia.

W organizacji obowiązuje ścisła hierarchia i kontrola. Tym, co robią ludzie, zazwyczaj rządzą formalne procedury.

2a. Jaki jest styl przywództwa w organizacji?

Stan obecny

Każdej odpowiedzi można przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musi się równać 100.

Przywództwo w organizacji powszechnie utożsamia się ze służeniem radą i pomocą oraz roztaczaniem opieki.

Przywództwo w organizacji powszechnie utożsamia się z przedsiębiorczością, nowatorstwem i podejmowaniem ryzyka.

Przywództwo w organizacji powszechnie utożsamia się ze stanowczością, ekspansywnością, orientacją na wyniki.

Przywództwo w organizacji powszechnie utożsamia się z koordynowaniem, sprawnym organizowaniem, stwarzaniem harmonijnych warunków do osiągania dobrych wyników.

2b. Jaki jest styl przywództwa w organizacji?

Stan pożądany

Każdej odpowiedzi można przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musi się równać 100.

Przywództwo w organizacji powszechnie utożsamia się ze służeniem radą i pomocą oraz roztaczaniem opieki.

Przywództwo w organizacji powszechnie utożsamia się z przedsiębiorczością, nowatorstwem i podejmowaniem ryzyka.

Przywództwo w organizacji powszechnie utożsamia się ze stanowczością, ekspansywnością, orientacją na wyniki.

Przywództwo w organizacji powszechnie utożsamia się z koordynowaniem, sprawnym organizowaniem, stwarzaniem harmonijnych warunków do osiągania dobrych wyników.

3a. Jaki jest styl zarządzania pracownikami?

Stan obecny

Każdej odpowiedzi można przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musi się równać 100.

W organizacji preferuje się pracę zespołową, dąży do powszechnej zgody i uczestnictwa.

W organizacji preferuje się samodzielne podejmowanie ryzyka, innowacyjność, swobodę i oryginalność.

W organizacji preferuje się ostrą rywalizację, stawiane są wysokie wymagania i liczą się przede wszystkim osiągnięcia.

W organizacji preferuje się bezpieczeństwo zatrudnienia, podporządkowanie, przewidywalność i niezmienność stosunków.

3b. Jaki jest styl zarządzania pracownikami?

Stan pożądany

Każdej odpowiedzi można przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musi się równać 100.

W organizacji preferuje się pracę zespołową, dąży do powszechnej zgody i uczestnictwa.

W organizacji preferuje się samodzielne podejmowanie ryzyka, innowacyjność, swobodę i oryginalność.

W organizacji preferuje się ostrą rywalizację, stawiane są wysokie wymagania i liczą się przede wszystkim osiągnięcia.

W organizacji preferuje się bezpieczeństwo zatrudnienia, podporządkowanie, przewidywalność i niezmienność stosunków.

4a. Co zapewnia spójność organizacji?

Stan obecny

Każdej odpowiedzi można przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musi się równać 100.

Spójność organizacji jest zapewniona przez lojalność i wzajemne zaufanie. Wysoko ceni się zaangażowanie w sprawy organizacji.

Spójność organizacji jest zapewniona przez zaangażowanie w innowacje i rozwój. Kładzie się nacisk na szukanie nowych dróg.

Spójność organizacji jest zapewniona przez nacisk na wyniki i osiąganie celów. Powszechnymi motywami działania są ekspansywność i chęć zwyciężania.

Spójność organizacji jest zapewniona przez formalne zasady i regulaminy. Najważniejsze jest sprawne funkcjonowanie.

4b. Co zapewnia spójność organizacji?

Stan pożądany

Każdej odpowiedzi można przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musi się równać 100.

Spójność organizacji jest zapewniona przez lojalność i wzajemne zaufanie. Wysoko ceni się zaangażowanie w sprawy organizacji.

Spójność organizacji jest zapewniona przez zaangażowanie w innowacje i rozwój. Kładzie się nacisk na szukanie nowych dróg.

Spójność organizacji jest zapewniona przez nacisk na wyniki i osiąganie celów. Powszechnymi motywami działania są ekspansywność i chęć zwyciężania.

Spójność organizacji jest zapewniona przez formalne zasady i regulaminy. Najważniejsze jest sprawne funkcjonowanie.

5a. Na co kładzie się największy nacisk?

Stan obecny

Każdej odpowiedzi można przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musi się równać 100.

W organizacji kładzie się nacisk na rozwój osobisty. Obserwuje się duże zaufanie, otwartość i współuczestnictwo.

W organizacji kładzie się nacisk na zdobywanie nowych zasobów i podejmowanie nowych wyzwań. Ceni się szukanie nowatorskich rozwiązań i możliwości.

W organizacji kładzie się nacisk na działania konkurencyjne i wyniki. Liczy się osiąganie ambitnych celów i zwyciężanie na rynku.

W organizacji kładzie się nacisk na trwałość i niezmienność. Ważne są sprawność, kontrola i praca bez zakłóceń.

5b. Na co kładzie się największy nacisk?

Stan pożądany

Każdej odpowiedzi można przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musi się równać 100.

W organizacji kładzie się nacisk na rozwój osobisty. Obserwuje się duże zaufanie, otwartość i współuczestnictwo.

W organizacji kładzie się nacisk na zdobywanie nowych zasobów i podejmowanie nowych wyzwań. Ceni się szukanie nowatorskich rozwiązań i możliwości.

W organizacji kładzie się nacisk na działania konkurencyjne i wyniki. Liczy się osiąganie ambitnych celów i zwyciężanie na rynku.

W organizacji kładzie się nacisk na trwałość i niezmienność. Ważne są sprawność, kontrola i praca bez zakłóceń.

6a. Jakie są kryteria sukcesu w organizacji?

Stan obecny

Każdej odpowiedzi można przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musi się równać 100.

Za miarę sukcesu uważa się rozwój zasobów ludzkich, pracę zespołową, zaangażowanie pracowników i troskę o ludzi.

Za miarę sukcesu uważa się wprowadzanie najbardziej oryginalnych i nowatorskich rozwiązań oraz osiągnięcie pozycji lidera w dziedzinie innowacyjności.

Za miarę sukcesu uważa się wygraną wśród podobnych organizacji i pokonywanie konkurentów. Najważniejsze jest osiągnięcie pozycji lidera wśród podobnych organizacji.

Za miarę sukcesu uważa się sprawność działania. Najważniejsze są: pewność realizacji zadań, terminowość, niskie koszty realizacji zadań.

6b. Jakie są kryteria sukcesu w organizacji?

Stan pożądany

Każdej odpowiedzi można przyporządkować od 0 do 100 punktów, suma wszystkich odpowiedzi musi się równać 100.

Za miarę sukcesu uważa się rozwój zasobów ludzkich, pracę zespołową, zaangażowanie pracowników i troskę o ludzi.

Za miarę sukcesu uważa się wprowadzanie najbardziej oryginalnych i nowatorskich rozwiązań oraz osiągnięcie pozycji lidera w dziedzinie innowacyjności.

Za miarę sukcesu uważa się wygraną wśród podobnych organizacji i pokonywanie konkurentów. Najważniejsze jest osiągnięcie pozycji lidera wśród podobnych organizacji.

Za miarę sukcesu uważa się sprawność działania. Najważniejsze są: pewność realizacji zadań, terminowość, niskie koszty realizacji zadań.

Blok opisowy

Część 2

Kwestionariusz ankiety dotyczący przepisów regulujących bezpieczeństwo informacji przetwarzanych w Sądzie

1. W jaki sposób po raz pierwszy zapoznała się Pani/zapoznał się Pan z obowiązującymi przepisami dotyczącymi bezpieczeństwa przetwarzanych informacji w Sądzie?

Można udzielić jednej odpowiedzi.

- ◯ W pierwszym dniu pracy, indywidualne szkolenie przeprowadził upoważniony pracownik.
- ◯ W pierwszym dniu pracy został mi udostępniony dokument zawierający regulacje dotyczące bezpieczeństwa przetwarzanych informacji.
- ◯ Na grupowym szkoleniu w Sądzie, w związku z wprowadzeniem lub zmianą regulacji dotyczących bezpieczeństwa przetwarzanych informacji.
- ◯ Wdrażane lub zmieniane regulacje dotyczące bezpieczeństwa przetwarzanych informacji zostały mi udostępnione w formie dokumentu.
- ◯ Nie zapoznałam/zapoznałem się jeszcze z regulacjami.

2. Osoba na jakim stanowisku po raz pierwszy przedstawiła Pani/Panu obowiązujące przepisy dotyczące bezpieczeństwa przetwarzanych informacji w Sądzie?

Można udzielić jednej odpowiedzi.

- ◯ Bezpośredni przełożony
- ◯ Inspektor Ochrony Danych
- ◯ Informatyk/Administrator Systemu Informatycznego
- ◯ Pracownik Oddziału Spraw Ogólnych i Osobowych
- ◯ Inny pracownik

3. Czy uczestniczyła Pani/uczestniczył Pan w Sądzie w szkoleniu uświadamiającym o zagrożeniach związanych z bezpieczeństwem informacji oraz danych osobowych?

Można udzielić jednej odpowiedzi.

- ◯ Tak. Szkolenie odbyło się raz.
- ◯ Tak. Szkolenia odbywają się regularnie.
- ◯ Nie. Ale wiem, że takie szkolenie odbyło się raz.
- ◯ Nie. Ale wiem, że takie szkolenia odbywają się regularnie.
- ◯ Nie. Nie wiem, czy takie szkolenie kiedykolwiek się odbyło.

4. Proszę ustosunkować się do poniższych stwierdzeń dotyczących bezpieczeństwa informacji w Sądzie.

Można udzielić jednej odpowiedzi w wierszu.

	tak	raczej tak	nie mam zdania	raczej nie	nie
Poziom zarządzania bezpieczeństwem informacji w Sądzie jest wysoki.	◯	◯	◯	◯	◯
W trakcie wykonywania obowiązków służbowych przestrzeganie przepisów dotyczących bezpieczeństwa informacji **nie jest** dla mnie uciążliwe.	◯	◯	◯	◯	◯
W Sądzie są bezwzględnie przestrzegane przepisy dotyczące bezpieczeństwa informacji.	◯	◯	◯	◯	◯

Jestem:

Można udzielić jednej odpowiedzi.

- ◯ Sędzią lub Asesorem Sądowym
- ◯ Referendarzem Sądowym lub Asystentem Sędziego
- ◯ Kierownikiem lub Pracownikiem Sekretariatu Wydziału
- ◯ Innym Pracownikiem Sądu

Pracuję w Wojewódzkim Sądzie Administracyjnym w/we:

Można udzielić jednej odpowiedzi.

- ◯ Białymstoku
- ◯ Bydgoszczy
- ◯ Gdańsku
- ◯ Gliwicach
- ◯ Gorzowie Wielkopolskim
- ◯ Kielcach
- ◯ Krakowie
- ◯ Lublinie
- ◯ Łodzi
- ◯ Olsztynie
- ◯ Opolu
- ◯ Poznaniu
- ◯ Rzeszowie
- ◯ Szczecinie
- ◯ Warszawie
- ◯ Wrocławiu

Załącznik 4. Zestawienie danych dotyczących liczby ważnych certyfikatów ISO/IEC 27001:2013 w roku 2022 w porównaniu z danymi z roku 2020 w poszczególnych krajach

Zestawienie danych dotyczących liczby ważnych certyfikatów ISO/IEC 27001:2013 w roku 2022 do danych z roku 2020 w poszczególnych krajach (ważny certyfikat to taki, który został wydany przez organ certyfikacyjny akredytowany przez członków IAF MLA w roku przeglądu lub w ciągu dwóch poprzedzających go lat, który jest nadal ważny na dzień 31 grudnia roku przeglądu). Opracowanie własne na podstawie danych zawartych na stronie internetowej https://www.iso.org/the-iso-survey.html

Lp.	Państwo	Liczba certyfikatów 2020 r.	Liczba certyfikatów 2022 r.	Zmiana
1	Afryka Południowa	77	105	36%
2	Albania	33	49	48%
3	Arabia Saudyjska	93	135	45%
4	Argentyna	57	100	75%
5	Armenia	17	10	–41%
6	Australia	562	702	25%
7	Austria	188	64	–66%
8	Azerbejdżan	3	9	200%
9	Bahrajn	53	33	–38%
10	Bangladesz	43	33	–23%
11	Belgia	141	220	56%
12	Belize	1	1	0%
13	Bhutan	6	3	–50%
14	Białoruś	33	46	39%
15	Birma	2	2	0%
16	Boliwia (państwo wielonarodowe)	4	5	25%
17	Bośnia i Hercegowina	51	52	2%
18	Botswana	1	1	0%
19	Brazylia	148	196	32%
20	Bułgaria	372	508	37%

Lp.	Państwo	Liczba certyfikatów 2020 r.	Liczba certyfikatów 2022 r.	Zmiana
21	Chile	89	33	–63%
22	Chiny	12403	25089	102%
23	Chorwacja	302	289	–4%
24	Cypr	42	57	36%
25	Czarnogóra	9	2	–78%
26	Czechy	394	694	76%
27	Dania	81	137	69%
28	Dominikana	6	4	–33%
29	Egipt	18	23	28%
30	Ekwador	13	14	8%
31	Estonia	17	30	76%
32	Etiopia	0	1	
33	Federacja Rosyjska	90	29	–68%
34	Fidżi	0	1	
35	Filipiny	110	117	6%
36	Finlandia	102	138	35%
37	Francja	392	782	99%
38	Gambia	1	1	0%
39	Ghana	42	58	38%
40	Gibraltar	1	1	0%
41	Grecja	454	404	–11%
42	Gruzja	3	2	–33%
43	Gwatemala	13	17	31%
44	Hiszpania	997	991	–1%
45	Holandia	1326	1688	27%
46	Honduras	6	5	–17%
47	Hongkong	186	235	26%
48	Indie	2226	2950	33%
49	Indonezja	542	816	51%
50	Irlandia	89	408	358%
51	Islandia	52	53	2%
52	Izrael	837	1464	75%

Lp.	Państwo	Liczba certyfikatów 2020 r.	Liczba certyfikatów 2022 r.	Zmiana
53	Japonia	5645	6831	21%
54	Jordania	24	29	21%
55	Kambodża	3	5	67%
56	Kanada	200	234	17%
57	Katar	58	80	38%
58	Kazachstan	16	20	25%
59	Kenia	14	26	86%
60	Kolumbia	238	294	24%
61	Kongo (Demokratyczna Republika Konga)	0	2	
62	Korea (Republika)	438	449	3%
63	Kostaryka	5	4	–20%
64	Kuwejt	44	39	–11%
65	Laotańska Republika Ludowo-Demokratyczna	2	4	100%
66	Liban	13	15	15%
67	Libia	0	2	
68	Liechtenstein	1	1	0%
69	Litwa	88	57	–35%
70	Luksemburg	17	48	182%
71	Łotwa	48	71	48%
72	Macedonia	52	48	–8%
73	Makau	21	11	–48%
74	Malezja	290	320	10%
75	Mali	1	1	0%
76	Malta	32	36	13%
77	Maroko	34	40	18%
78	Mauritius	19	23	21%
79	Meksyk	258	319	24%
80	Mołdawia (Republika)	11	3	–73%
81	Monako	1	6	500%
82	Mongolia	5	7	40%
83	Mozambik	0	2	
84	Nepal	5	16	220%

Lp.	Państwo	Liczba certyfikatów 2020 r.	Liczba certyfikatów 2022 r.	Zmiana
85	Niemcy	1281	1515	18%
86	Nigeria	62	104	68%
87	Norwegia	120	164	37%
88	Nowa Zelandia	66	84	27%
89	Oman	23	28	22%
90	Pakistan	35	98	180%
91	Panama	3	5	67%
92	Papua-Nowa Gwinea	1	2	100%
93	Peru	85	50	–41%
94	Polska	710	777	9%
95	Portugalia	90	94	4%
96	Republika Zielonego Przylądka	1	1	0%
97	Rumunia	729	819	12%
98	Rwanda	4	4	0%
99	Saint Vincent i Grenadyny	1	1	0%
100	Salwador	4	4	0%
101	San Marino	4	3	–25%
102	Senegal	2	3	50%
103	Serbia	351	435	24%
104	Singapur	222	274	23%
105	Słowacja	142	273	92%
106	Słowenia	131	45	–66%
107	Sri Lanka	68	81	19%
108	Sudan	3	2	–33%
109	Surinam	2	3	50%
110	Szwajcaria	274	364	33%
111	Szwecja	146	192	32%
112	Tajlandia	354	466	32%
113	Tajwan	895	1372	53%
114	Tanzania, Zjednoczona Republika	3	3	0%
115	Togo	2	1	–50%
116	Trynidad i Tobago	0	1	

Lp.	Państwo	Liczba certyfikatów 2020 r.	Liczba certyfikatów 2022 r.	Zmiana
117	Tunezja	27	14	–48%
118	Turcja	881	603	–32%
119	Turkmenistan	0	1	
120	Ukraina	59	84	42%
121	Urugwaj	13	56	331%
122	USA	1058	1784	69%
123	Węgry	560	673	20%
124	Wietnam	348	291	–16%
125	Wlk. Brytania i Irlandia Płn.	3327	6054	82%
126	Włochy	1827	2408	32%
127	Wybrzeże Kości Słoniowej	1	2	100%
128	Wyspy Salomona	1	1	0%
129	Zambia	4	4	0%
130	Zjednoczone Emiraty Arabskie	235	233	–1%
RAZEM		**44466**	**67326**	**51**

Załącznik 5. Standardy systemów zarządzania Międzynarodowej Organizacji Normalizacyjnej – ISO

1) Standardy systemów zarządzania, które mają zastosowanie we wszystkich sektorach gospodarki, różnych typach i rozmiarach organizacji oraz różnorodnych warunkach geograficznych, kulturowych i społecznych. Wiele z nich posiada tę samą strukturę i zawiera te same terminy, definicje i wymagania:
   - ISO 9001:2015 – Systemy zarządzania jakością — Wymagania .
   - ISO/IEC 27001:2022 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności — Systemy zarządzania bezpieczeństwem informacji — Wymagania.
   - ISO 14001:2015 – Systemy zarządzania środowiskowego — Wymagania wraz z wytycznymi dotyczącymi stosowania.
2) Standardy systemów zarządzania dotyczące stosowania ogólnej normy zarządzania w określonym sektorze gospodarczym:
   - ISO 13485:2016 – Wyroby medyczne — Systemy zarządzania jakością — Wymagania do celów regulacyjnych.
   - ISO 22163:2023 – Zastosowania kolejowe – System zarządzania jakością w kolejnictwie – ISO 9001:2015 i szczegółowe wymagania dotyczące stosowania w sektorze kolejowym.
   - ISO 29001:2020 – Przemysł naftowy, petrochemiczny i gazowniczy — Sektorowe systemy zarządzania jakością — Wymagania dotyczące organizacji dostarczających produkty i usługi.
3) Standardy związane z systemem zarządzania i wytyczne dotyczące wdrażania dalszych wytycznych i/lub wymagań dotyczących:
   - ISO 45003:2021 – Zarządzanie bezpieczeństwem i higieną pracy — Bezpieczeństwo psychiczne i higiena pracy — Wytyczne dotyczące zarządzania ryzykiem psychospołecznym.
   - ISO 14004:2016 – Systemy zarządzania środowiskowego — Ogólne wytyczne dotyczące wdrażania.
   - ISO 19011:2018 – Wytyczne dotyczące audytowania systemów zarządzania.
4) Standardy zarządzania, które mogą wspierać wdrażanie określonych aspektów systemu zarządzania organizacją:
   - ISO 26000:2010 – Wytyczne dotyczące odpowiedzialności społecznej.
   - ISO 31000:2018 – Zarządzanie ryzykiem – Wytyczne.

Załącznik 6. Narzędzie do oceny dojrzałości systemów zarządzania bezpieczeństwem informacji

Minimalna liczba punktów wymagana do osiągnięcia poziomu	Lp.	Pytanie	Odpowiedź: Tak – 1 pkt Nie – 0 pkt
Poziom 2.			
16 pkt	1.	Czy ustanowiono udokumentowany system zarządzania bezpieczeństwem informacji (SZBI) w organizacji?	
	2.	Czy w dokumencie ustanawiającym SZBI określono, jakim informacjom należy zapewnić bezpieczeństwo?	
	3.	Czy w dokumencie ustanawiającym SZBI uwzględniono zewnętrzne przepisy prawne?	
	4.	Czy w dokumencie ustanawiającym SZBI uwzględniono wewnętrzne regulacje?	
	5.	Czy w dokumencie ustanawiającym SZBI wskazano techniki wykorzystywane do zapewnienia bezpieczeństwa informacji?	
	6.	Czy w dokumencie ustanawiającym SZBI określono interesariuszy SZBI?	
	7.	Czy w dokumencie ustanawiającym SZBI określono zasady wymiany informacji między innymi organizacjami?	
	8.	Czy w SZBI istnieją zapisy o zasadach przydzielania i odbioru uprawnień do systemów informatycznych?	
	9.	Czy w SZBI istnieją zapisy o zasadach „pracy zdalnej”?	
	10.	Czy SZBI zawiera dodatkowe regulacje dotyczące bezpieczeństwa danych osobowych przetwarzanych w organizacji?	
	11.	Czy SZBI zawiera procedury zgłaszania incydentów dotyczących bezpieczeństwa informacji i prywatności?	
	12.	Czy SZBI zawiera plan ciągłości działania?	
	13.	Czy SZBI zawiera procedury odzyskiwania kluczowych systemów informatycznych?	

	14.	Czy kierownictwo wskazało w sposób udokumentowany osobę (lub osoby) do wdrożenia, monitorowania zmian w regulacjach wewnętrznych i przepisach prawa dotyczących SZBI i aktualizowania SZBI?	
	15.	Czy zdefiniowane są role i obowiązki dotyczące zarządzania bezpieczeństwem informacji w organizacji?	
	16.	Czy informacje o procesach zawarte w SZBI zawierają wskazanie ról z podziałem na osoby odpowiedzialne za wykonanie procesu (R) oraz osoby sprawujące nadzór nad tym procesem (A)?	
	17.	Czy informuje się członków organizacji o ustanowieniu SZBI i o zmianach SZBI?	
Poziom 3.			
16 pkt* + 7 pkt = **23 pkt**	1.	Czy zintegrowano planowanie, projektowanie, wdrażanie i monitorowanie procedur bezpieczeństwa informacji i prywatności wymienione w pytaniach 11, 12, 13 dla poziomu drugiego?	
	2.	Czy w SZBI wskazano częstotliwość uczestnictwa w obowiązkowych szkoleniach uświadamiających zagrożenia związane z bezpieczeństwem informacji?	
	3.	Czy sformułowano plan postępowania z ryzykiem w zakresie bezpieczeństwa informacji dostosowany do celów i struktury organizacyjnej organizacji?	
	4.	Czy utrzymuje się plan postępowania z ryzykiem w zakresie bezpieczeństwa informacji dostosowany do celów i struktury organizacyjnej?	
	5.	Czy zapewnia się/uzasadnia się, że plan (postępowania z ryzykiem w zakresie bezpieczeństwa informacji) określa odpowiednie praktyki zarządzania i rozwiązania w zakresie bezpieczeństwa, biorąc pod uwagę zasoby, odpowiedzialność i priorytety, w zakresie zarządzania zidentyfikowanym ryzykiem bezpieczeństwa informacji?	
	6.	Czy istnieje udokumentowany sposób zarządzania ryzykiem związanym z bezpieczeństwem informacji?	
	7.	Czy zarządzanie ryzykiem związanym z bezpieczeństwem informacji jest składową zarządzania ryzykiem działalności organizacji?	
	8.	Czy określono sposób pomiaru skuteczności praktyk dotyczących zarządzania bezpieczeństwem informacji?	
Poziom 4.			
	1.	Czy istnieje w organizacji dokumentacja potwierdzająca dokonywanie przeglądów dokumentacji SZBI?	

23 pkt + 4 pkt = **27 pkt**	2.	Czy istnieją dokumenty potwierdzające przeglądy skuteczności SZBI w zaplanowanych odstępach czasu?	
	3.	Czy istnieją dokumenty potwierdzające audyty SZBI w zaplanowanych odstępach czasu?	
	4.	Czy istnieją dokumenty potwierdzające regularne przeglądy SZBI przez kierownictwo organizacji, aby zapewnić, że zakres SZBI pozostaje odpowiedni oraz aby zidentyfikować możliwe usprawnienia w ustanowionych procesach SZBI?	
Poziom 5.			
27 pkt + 3 pkt = **30 pkt**	1.	Czy istnieją udokumentowane informacje o wkładzie kierownictwa w utrzymanie SZBI?	
	2.	Czy istnieją udokumentowane informacje o zaangażowania najwyższego kierownictwa w optymalizację SZBI?	
	3.	Czy można mówić o kulturze bezpieczeństwa informacji i danych osobowych?	

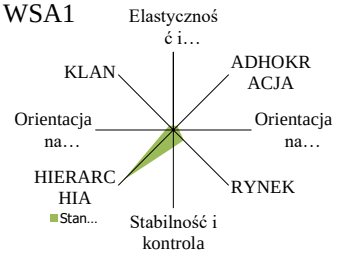
[*] *Osiągnięte punkty w poprzednich poziomach dojrzałości systemu zarządzania bezpieczeństwem informacji.*

Załącznik 7. Wymiary kultury organizacyjnej poszczególnych wojewódzkich sądów administracyjnych – kwestionariusz OCAI

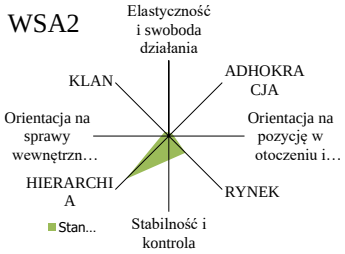
LP	WSA	1. Charakterystyka organizacji				2. Przywództwo w organizacji				3. Zarządzanie pracownikami				4. Co zapewnia spójność w organizacji?				5. Na co kładzie się nacisk?				6. Kryteria sukcesu				Profil kultury organizacyjnej – ogółem			
		Klan	Adhokracja	Rynek	Hierarchia	Klan	Adhokracja	Rynek	Hierarchia	Klan	Adhokracja	Rynek	Hierarchia	Klan	Adhokracja	Rynek	Hierarchia	Klan	Adhokracja	Rynek	Hierarchia	Klan	Adhokracja	Rynek	Hierarchia	Klan	Adhokracja	Rynek	Hierarchia
1	WSA1	6	6	15	73	6	6	63	25	11	1	20	68	6	3	19	73	9	3	6	81	8	1	5	86	**8**	**3**	**21**	**68**
2	WSA2	6	4	25	64	5	5	65	25	10	6	31	53	10	3	18	68	6	5	27	63	7	3	15	75	**7**	**4**	**30**	**58**
3	WSA3	19	4	21	56	11	4	33	53	15	8	13	63	26	0	2	72	4	14	3	80	14	4	1	82	**15**	**6**	**12**	**68**
4	WSA4	11	8	31	51	10	8	69	13	9	19	25	47	11	7	23	59	9	8	21	62	9	7	23	61	**10**	**10**	**32**	**49**
5	WSA5	4	28	20	49	5	3	80	13	5	5	88	3	3	3	63	33	3	5	55	38	3	3	65	30	**4**	**8**	**62**	**27**
6	WSA6	14	11	26	50	13	8	38	41	21	13	10	56	18	4	13	65	15	2	4	79	16	2	4	78	**16**	**7**	**16**	**61**
7	WSA7	21	11	23	45	48	8	15	30	43	3	8	48	33	5	13	50	29	1	13	58	18	18	8	58	**32**	**8**	**13**	**48**
8	WSA8	9	11	21	59	15	7	35	44	20	9	12	60	14	4	10	72	9	4	8	78	9	3	12	76	**13**	**6**	**16**	**65**
9	WSA9	17	13	21	49	15	13	31	41	23	17	17	43	22	14	6	58	24	14	7	55	24	10	26	40	**21**	**13**	**18**	**48**
10	WSA10	8	7	22	62	13	9	39	39	22	15	17	46	18	8	21	53	9	9	21	61	11	7	23	58	**14**	**9**	**24**	**53**
11	WSA11	4	5	49	42	16	10	36	38	19	21	11	48	24	7	15	54	17	6	4	73	21	9	17	53	**17**	**10**	**22**	**51**
12	WSA12	6	6	24	64	15	8	38	39	23	13	14	50	16	16	19	50	12	11	7	71	12	8	19	62	**14**	**10**	**20**	**56**
13	WSA13	9	8	15	68	11	12	54	23	14	9	18	59	12	9	14	65	9	9	12	71	9	9	15	67	**11**	**9**	**21**	**59**
14	WSA14	17	11	12	60	24	15	44	17	23	9	4	64	22	10	13	54	20	6	4	69	24	5	15	57	**22**	**10**	**15**	**53**
15	WSA15	7	6	18	70	7	4	46	43	14	6	13	68	14	3	17	66	8	10	13	69	8	3	8	81	**10**	**5**	**19**	**66**
16	WSA16	9	25	12	55	11	21	52	17	18	3	24	54	18	9	20	53	16	8	8	69	16	12	3	70	**15**	**13**	**20**	**53**

Załącznik 8. Wymiar kultury organizacyjnej „Charakterystyka organizacji”

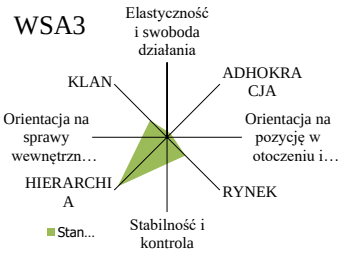
WSA1



WSA2

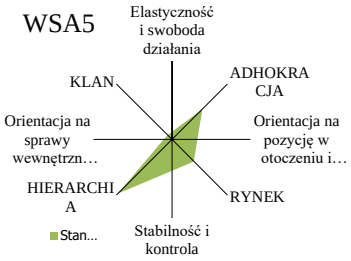


WSA3

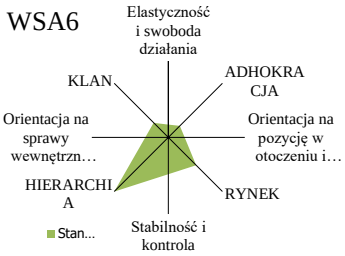


WSA4

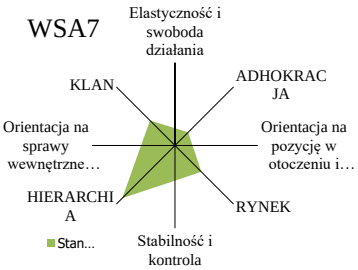
WSA5



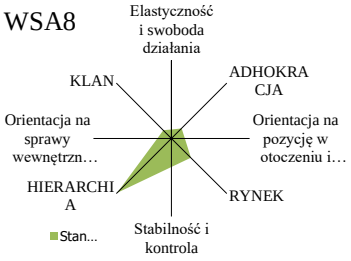
WSA6



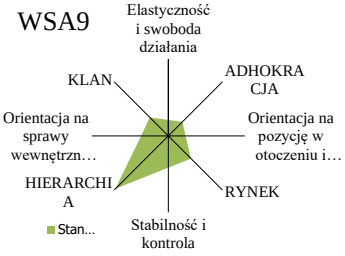
WSA7



WSA8

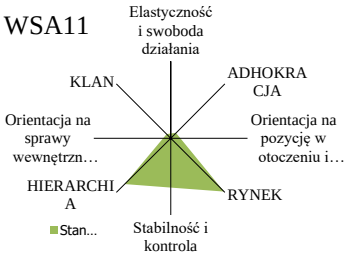


WSA9



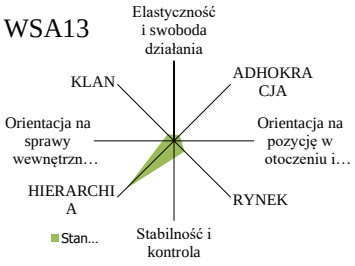
WSA10

WSA11

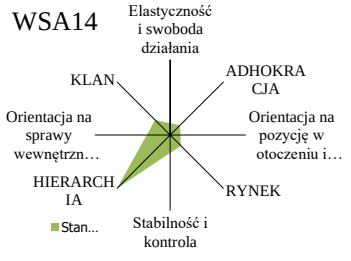


WSA12

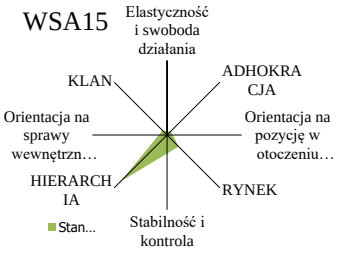
WSA13



WSA14



WSA15



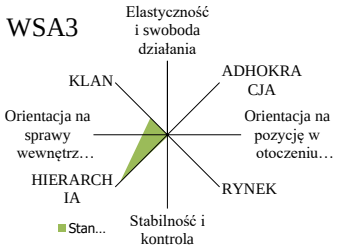

WSA16
Elastyczność i swoboda działania
ADHOKRACJA
Orientacja na pozycję w otoczeniu i…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy wewnętrzne…
KLAN
Stan...

Załącznik 9. Wymiar kultury organizacyjnej „Co zapewnia spójność?”

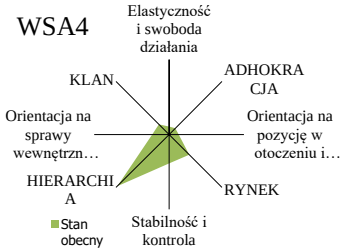
WSA1

WSA2

WSA3



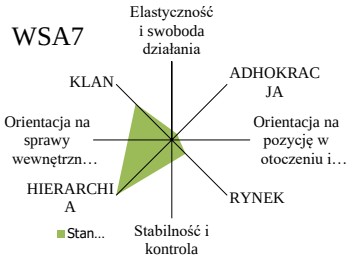
WSA4



WSA5

WSA6

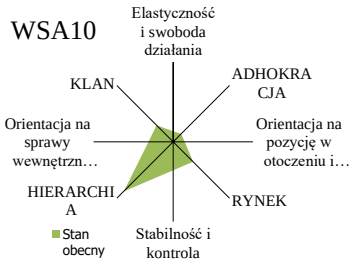
WSA7



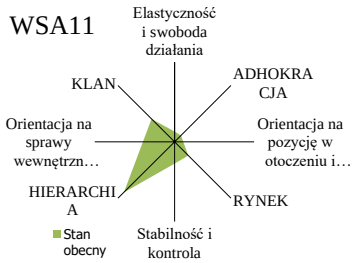
WSA8

WSA9

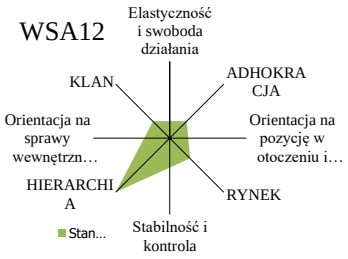
WSA10



WSA11



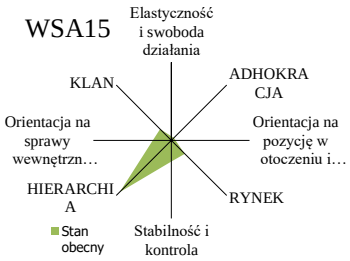
WSA12

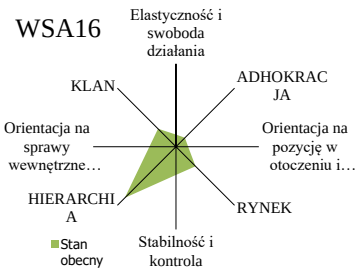


WSA13

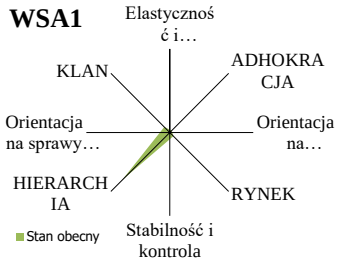
WSA14

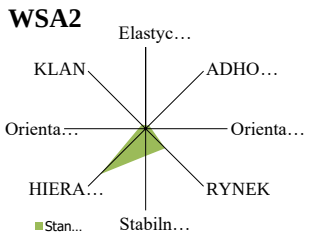
WSA15

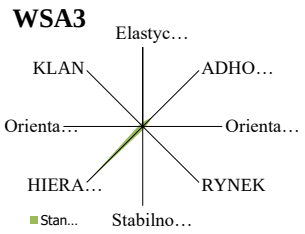


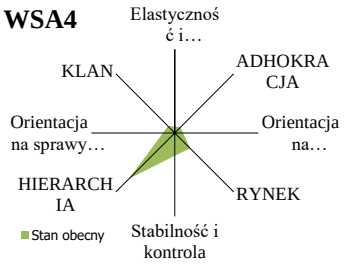

WSA16
Elastyczność i swoboda działania
ADHOKRACJA
Orientacja na pozycję w otoczeniu i…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy wewnętrzne…
KLAN
Stan obecny

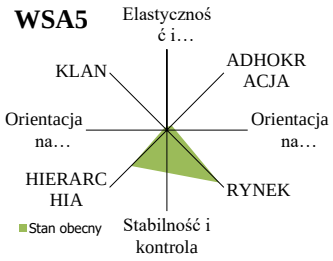
Załącznik 10. Wymiar kultury organizacyjnej „Na co kładzie się nacisk?”

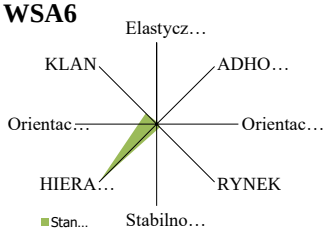


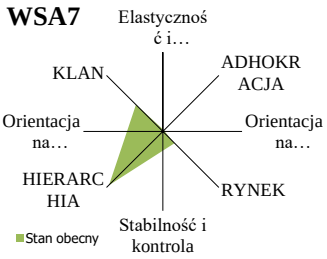


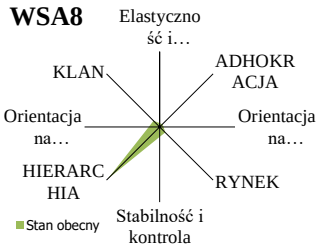


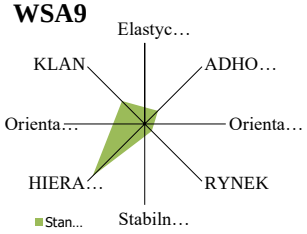


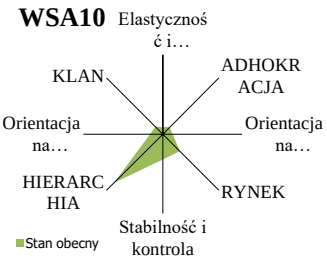


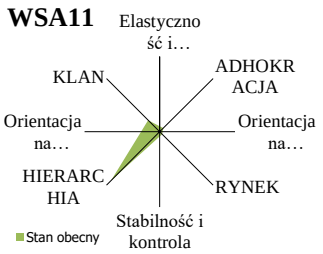


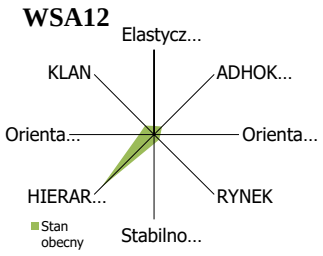




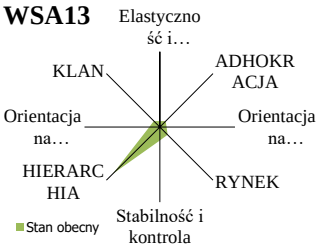




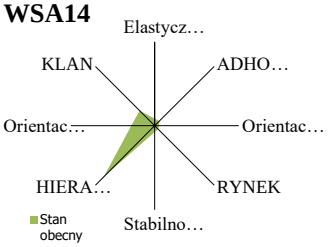




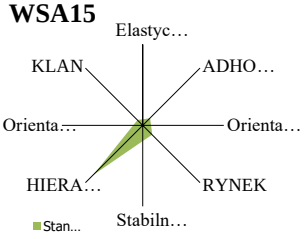
WSA13



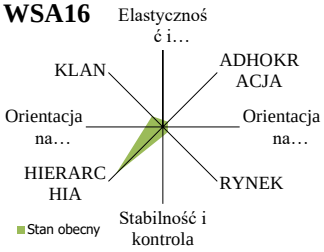
WSA14



WSA15

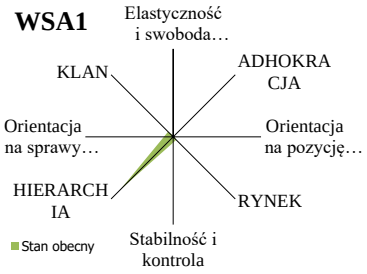


WSA16

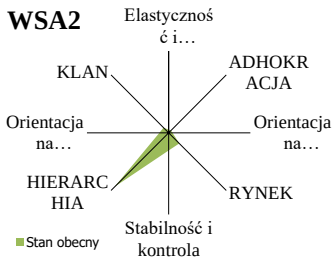


Załącznik 11. Wymiar kultury organizacyjnej „Kryteria sukcesu”

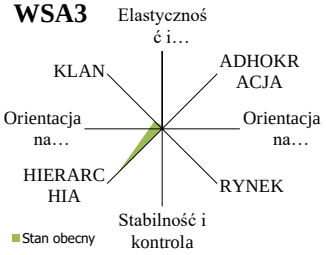
WSA1



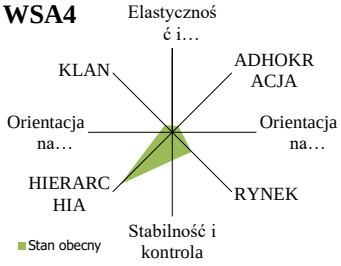
WSA2



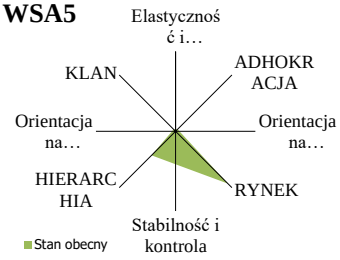
WSA3



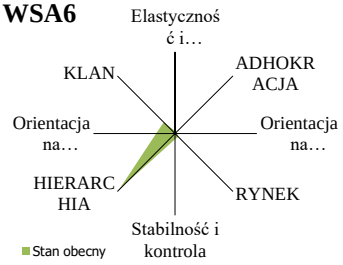
WSA4



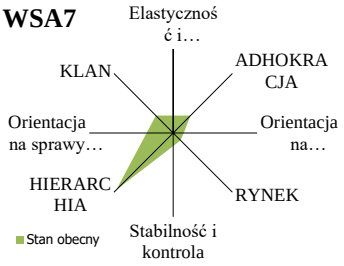
WSA5



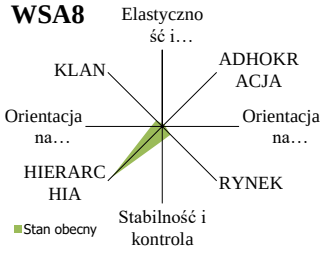
WSA6



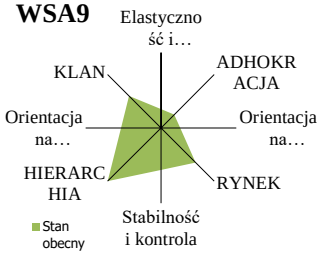
WSA7



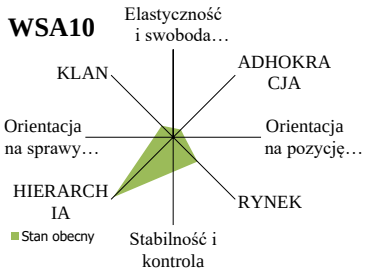
WSA8



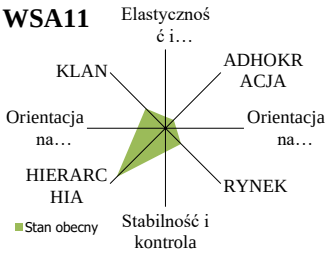
WSA9



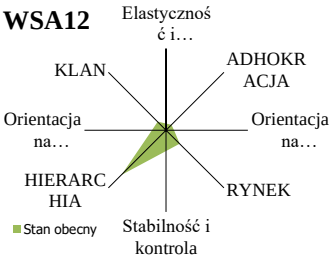
WSA10



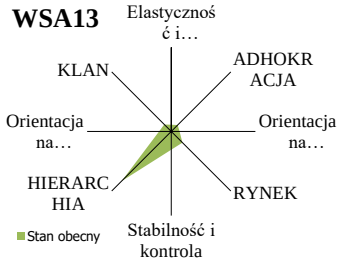
WSA11



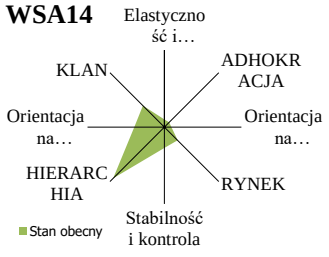
WSA12



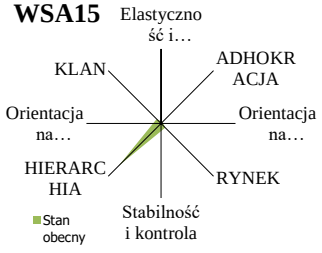
WSA13



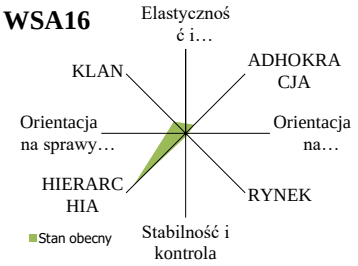
WSA14



WSA15



WSA16


Elastyczność i…
ADHOKRACJA
Orientacja na…
RYNEK
Stabilność i kontrola
HIERARCHIA
Orientacja na sprawy…
KLAN
Stan obecny

Spis tabel

Tabela 1.1. Zestawienie wybranych definicji dojrzałości procesowej organizacji oraz dojrzałości organizacji 14
Tabela 1.2. Poziomy zdolności dla procesów w modelu dojrzałości CPM 63
Tabela 1.3. Domeny, cele i zadania C2M2 68
Tabela 1.4. Poziomy dojrzałości C2M2 72
Tabela 2.1. Główne kierunki i nurty w teorii organizacji 80
Tabela 2.2. Paradygmaty badania kultury organizacyjnej 90
Tabela 2.3. Wybrane definicje kultury organizacyjnej 95
Tabela 2.4. . Dychotomiczne typologie kultur organizacyjnych 114
Tabela 3.1. Kryteria i wyniki przeszukiwań baz literaturowych 117
Tabela 3.2. Kryteria i wyniki rozszerzonych przeszukiwań baz literaturowych. 119
Tabela 3.3. Zestawienie tłumaczenia na język polski nazwy tematów i koncepcji wyodrębnionych przez oprogramowanie VOSviewer wraz z przyporządkowaniem do klastra 123
Tabela 3.4. Plan badań empirycznych 144
Tabela 3.5. Wymagania poziomów dojrzałości 151
Tabela 3.6. Analiza rzetelności narzędzia do oceny poziomu dojrzałości SZBI 152
Tabela 3.7. Wynik analizy rzetelności dla wskaźnika „Bezpieczeństwo informacji” 154
Tabela 3.8. Matryca kodów zastosowana w analizie treści 158
Tabela 4.1. Zestawienie dokumentów według zaleceń, których zostały opracowane SZBI w wojewódzkich sądach administracyjnych 162
Tabela 4.2. Sposób informowania osób pracujących w wojewódzkich sądach administracyjnych o przepisach dotyczących SZBI 163
Tabela 4.3. Rozbieżności pomiędzy informacjami uzyskanymi podczas wywiadów a badaniem dokumentacji związanej ze SZBI 164
Tabela 4.4. Zestawienie uzyskanej liczby punktów przez poszczególne WSA w badaniu dokumentów dotyczących Systemu Zarządzania Bezpieczeństwem Informacji oraz informacja o uzyskanym poziomie dojrzałości SZBI 192
Tabela 4.5. Porównanie kultury organizacyjnej w stanie obecnym a pożądanym 182
Tabela 4.6. Różnice w zakresie kultury organizacyjnej w zależności od grupy zawodowej 183
Tabela 4.7. Korelacje wskaźników bezpieczeństwa informacji ze wskaźnikami kultury organizacyjnej 184
Tabela 4.8. Uczestnictwo w szkoleniach w zależności od poziomu dojrzałości SZBI 185
Tabela 4.9. Korelacje wskaźników wymiaru kultury organizacyjnej „Przywództwo w organizacji” z dojrzałością SZBI 187
Tabela 4.10. Korelacje wskaźników wymiaru kultury organizacyjnej „Styl zarządzania” z dojrzałością SZBI 189
Tabela 4.11. Rekomendowane działania dotyczące rozwoju kultury bezpieczeństwa informacji w organizacji. 204

Spis rysunków

Rysunek 0.1. Schemat przebiegu postępowania badawczego 8
Rysunek 1.1. Poziomy dojrzałości według pierwotnej koncepcji CMM. 18
Rysunek 1.2. Genealogia CMM Integration 20
Rysunek 1.3. Systematyka badanych modeli dojrzałości 21
Rysunek 1.4. Związek między cyberbezpieczeństwem a innymi rodzajami bezpieczeństwa 34
Rysunek 1.5. Piętnaście państw z największą liczbą aktualnych certyfikatów zgodności ISMS z wymaganiami ISO/IEC 27001:2013 w 2022 r. 41
Rysunek 1.6. Piętnaście państw z największym wzrostem liczby aktualnych certyfikatów zgodności ISMS z wymaganiami ISO/IEC 27001:2013 do roku 2022 (po usunięciu z zestawienia państw z ogólną liczbą certyfikatów poniżej 20) 42
Rysunek 1.7. Przykład zabezpieczeń organizacyjnych zawartych w załączniku do normy ISO/IEC 27001:2022 47
Rysunek 1.8. Przykład opisania zabezpieczenia w normie ISO/IEC 27002:2022 48
Rysunek 1.9. Struktura dokumentów IT-Grundschutz 50
Rysunek 1.10. Elementy systemu wartości usług 55
Rysunek 1.11. Cztery wymiary zarządzania usługami 56
Rysunek 1.12. Model COBIT 60
Rysunek 1.13. Przykładowa macierz z modelem FAM z dziedziny funkcjonalnej architektury korporacyjnej 74
Rysunek 1.14. Macierz modelu ISFAM 2.0. (ang. Information Security Focus Area Maturity) 76
Rysunek 2.1. Organizacja jako system społeczno-techniczny 82
Rysunek 2.2. Typy organizacji 84
Rysunek 2.3. Przestrzeń organizacyjna z dominacją kultury organizacyjnej 87
Rysunek 2.4. Cztery paradygmaty w naukach społecznych 89
Rysunek 2.5. Nurty rozumienia kultury organizacyjnej 95
Rysunek 2.6. Poziomy kultury według E. Scheina 98
Rysunek 2.7. „Diagram cebuli" przejawy kultury na różnych poziomach głębokości 100
Rysunek 2.8. Dynamika kultury organizacji 105
Rysunek 2.9. Model wartości konkurujących 107
Rysunek 3.1. Liczba pozycji analizowanej literatury 117
Rysunek 3.2. Mapa tematów i koncepcji wyodrębniona w analizowanej literaturze 123
Rysunek 3.3. Struktura organizacyjna Wojewódzkiego Sądu Administracyjnego w Łodzi 137
Rysunek 3.4. Liczba respondentów z podziałem na grupy zawodowe 147
Rysunek 3.5.Procentowy udział osób pracujących w danym WSA w badaniu ankietowym 148
Rysunek 3.6. Schemat realizacji badania – równoległa strategia triangulacyjna 156
Rysunek 3.7. Chmura słów najczęściej używanych przez respondentów 157
Rysunek 4.1. Słowa kojarzone z pojęciem kultura organizacyjna 170
Rysunek 4.2. Profile kultury organizacyjnej poszczególnych wojewódzkich sądów administracyjnych 177
Rysunek 4.3. Wymiar kultury organizacyjnej „przywództwo w organizacji" w wojewódzkich sądach administracyjnych 179

Rysunek 4.4. Wymiar kultury organizacyjnej „zarządzanie pracownikami” w wojewódzkich sądach administracyjnych 180
Rysunek 4.5. Pożądany stan kultury organizacyjnej wojewódzkich sądów administracyjnych 182
Rysunek 4.6. Osoby udzielające informacji o przepisach dotyczących bezpieczeństwa przetwarzanych informacji 185
Rysunek 4.7. Profile kultury organizacyjnej dla wymiaru „Przywództwo w organizacji” w podziale na grupy według osiągniętej dojrzałości SZBI w wojewódzkich sądach administracyjnych 188
Rysunek 4.8. Średnie wartości wskaźników wymiaru kultury organizacyjnej „Przywództwo w organizacji” dla poszczególnych poziomów dojrzałości SZBI 189
Rysunek 4.9. Profile kultury organizacyjnej dla wymiaru „Styl zarządzania” w podziale na grupy według osiągniętej dojrzałości SZBI w wojewódzkich sądach administracyjnych 191
Rysunek 4.10. Średnie wartości wskaźników wymiaru kultury organizacyjnej „Przywództwo w organizacji” dla poszczególnych poziomów dojrzałości SZBI 191
Rysunek 4.11. Podejmowane działania najwyższego kierownictwa wskazane podczas wywiadów z dyrektorami WSA 195
Rysunek 4.12. Czynniki wpływające na kulturę bezpieczeństwa informacji wyodrębnione podczas wywiadów z dyrektorami WSA 199

Streszczenie rozprawy w języku polskim

Kultura organizacyjna a dojrzałość systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych

Temat dojrzałości systemów zarządzania bezpieczeństwem informacji (skrót: SZBI) jest istotny w obliczu rosnącego ryzyka utraty bezpieczeństwa informacji przetwarzanych w organizacjach. Interesariusze od organizacji oczekują dostępności informacji w czasie i w miejscu im dogodnym przy zachowaniu jej poufności oraz integralności. Transformacja cyfrowa, której ulega organizacja, wpływa nie tylko na przyjęcie nowych rozwiązań technicznych, ale również na całą organizację, na jej zarządzanie, procesy, ludzi i kulturę organizacyjną. W literaturze przedmiotu, szczególnie w odniesieniu do organizacji sektora publicznego, przedstawionych jest niewiele badań dotyczących dojrzałości systemów zarządzania bezpieczeństwem informacji – z uwzględnieniem kontekstu kultury organizacyjnej. Badanie przeprowadzone na cele dysertacji obejmowało swoim zasięgiem wybraną grupę organizacji sektora publicznego – wszystkie wojewódzkie sądy administracyjne. Ograniczenie do jednej grupy organizacji wynikało z zamiaru dogłębnego przeanalizowania zjawiska będącego przedmiotem zainteresowań badawczych, z wykorzystaniem zarówno metod jakościowych, jak i ilościowych.

Odpowiedzi na postawione w dysertacji następujące pytania badawcze:

1. Jaki jest poziom dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych?
2. Jaki jest w ocenie pracowników dominujący profil kultury organizacyjnej w wojewódzkich sądach administracyjnych?
3. Czy istnieją cechy kultury organizacyjnej mające potencjalny związek z dojrzałością systemów zarządzania bezpieczeństwem informacji?

pozwoliły na realizację celu głównego dysertacji, tj. zdiagnozowanie dojrzałości systemów zarządzania bezpieczeństwem informacji w wojewódzkich sądach administracyjnych z uwzględnieniem kontekstu kultury organizacyjnej.

Na początkowym etapie postępowania badawczego przeprowadzono analizę literatury – dotyczącej problemów związanych z oceną dojrzałości systemów zarządzania bezpieczeństwem informacji oraz perspektyw rozumienia i badania procesów kulturowych, zachodzących w organizacjach. Kolejnym analizowanym

zagadnieniem był związek kultury organizacyjnej z dojrzałością systemów zarządzania bezpieczeństwem informacji. Analiza ta została przeprowadzona po dokonaniu systematycznego przeglądu literatury.

Odpowiedź na pierwsze pytanie badawcze uzyskana została na podstawie sondaży diagnostycznych, tj. wywiadów z dyrektorami, i badania dokumentów zawierających polityki bezpieczeństwa poszczególnych sądów. Do oceny dojrzałości SZBI zostało utworzone narzędzie, które może posłużyć za wzór w badaniach innych organizacji. Pięć wojewódzkich sądów osiągnęło pierwszy poziom dojrzałości, siedem poziom drugi, trzy poziom trzeci oraz jeden sąd poziom najwyższy, piąty.

W celu pozyskania informacji umożliwiających udzielenie odpowiedzi na drugi problem badawczy zastosowano metodę sondażu diagnostycznego i techniki badawcze – wywiad oraz ankietę. Cechy kultury hierarchicznej były zdiagnozowane jako dominujące w piętnastu sądach na szesnaście badanych, w jednym sądzie dominowały cechy kultury rynkowej.

W dwóch wymiarach kultury organizacyjnej dotyczących styli przywództwa i sposobów zarządzania pracownikami zauważono rozbieżności w badanych sądach. W pierwszym wymienionym wymiarze w połowie badanych sądów respondenci identyfikowali jako dominujące cechy charakterystyczne dla kultury rynkowej. W jednym z sądów dominowały cechy kultury klanowej, w pozostałych kultury hierarchicznej. Z kolei w wymiarze kultury dotyczącym zarządzania pracownikami w jednym z sądów dominował profil kultury rynkowej, w innym zaś obok cech kultury hierarchicznej porównywalnie istotne były cechy kultury klanowej, w pozostałych dominowały cechy kultury hierarchicznej.

Zauważone w badaniu różnice w wymiarach kultury dotyczących przywództwa w organizacji oraz zarządzania pracownikami, jak i różnice w poziomach dojrzałości SZBI w badanych organizacjach, pozwoliły na wyodrębnienie cech kultury organizacyjnej, mających potencjalny związek z dojrzałością SZBI, zatem odpowiedź na ostatnie pytanie problemu badawczego jest twierdząca. W wojewódzkim sądzie administracyjnym, który uzyskał najwyższy, piąty poziom dojrzałości SZBI w wymiarach „styl przywództwa" i „styl zarządzania pracownikami" w opinii respondentów obok cech kultury hierarchicznej nasilenie cech kultury klanowej było najwyższe wśród badanych sądów. Dostrzeżona koincydencja pomiędzy cechami kultury organizacyjnej a dojrzałością SZBI była podstawą sformułowania rekomendacji dotyczących rozwijania kultury bezpieczeństwa informacji w organizacji.

Słowa kluczowe: systemy zarządzania bezpieczeństwem informacji, ocena dojrzałości systemów zarządzania, kultura organizacyjna, kultura bezpieczeństwa informacji.

Streszczenie rozprawy w języku angielskim

Organizational culture and the maturity of information security management systems in provincial administrative courts

The subject of the maturity of information security management systems (ISMS) is important in view of the growing risk of losing the security of information processed in organizations. Stakeholders expect organizations to have information available at a time and place convenient to them while maintaining its confidentiality and integrity. The digital transformation that an organization undergoes affects not only the adoption of new technical solutions, but also the entire organization, its management, processes, people and organizational culture. In the literature, especially with regard to public sector organizations, there are not many researches presented on the maturity of information security management systems - with regard to the context of organizational culture. The research conducted for the dissertation covered a selected group of public sector organizations - all provincial administrative courts. The limitation to one group of organizations was due to the intention to analyse in depth the phenomenon of research interest, using both qualitative and quantitative methods.

Answering the following research questions posed in the dissertation:

1. What is the level of maturity of information security management systems in provincial administrative courts?
2. What is the dominant profile of organizational culture in provincial administrative courts in the opinion of employees?
3. Are there characteristics of organizational culture that have a potential relationship with the maturity of information security management systems?

made it possible to achieve the main goal of the dissertation, i.e. to diagnose the maturity of information security management systems in provincial administrative courts with the context of organizational culture.

At the initial stage of the research proceedings, an analysis of the literature was conducted - concerning the problems of assessing the maturity of information security management systems and perspectives on understanding and studying cultural processes occurring in organizations. The next subject analysed was the relationship of

organizational culture to the maturity of information security management systems. This analysis was conducted after a systematic literature review.

The answer to the first research question was obtained on the basis of diagnostic methods, i.e. interviews with directors, and analysis of documents containing security policies of individual courts. A tool was created to assess the maturity of the ISMS, which can be used as a model in studies of other organizations. Five provincial courts achieved the first level of maturity, seven the second level, three the third level and one court the highest level, the fifth.

A diagnostic poll method and research techniques - an interview and a survey - were used to obtain information to answer the second research problem. Hierarchical culture traits were diagnosed as dominant in fifteen courts out of the sixteen studied, and market culture traits were dominant in one court.

In two dimensions of organizational culture concerning leadership styles and ways of managing employees, discrepancies were noted among the studied courts. In the first mentioned dimension, in half of the studied courts, respondents identified as dominant characteristics of market culture. In one of the courts, the dominant characteristics were clan culture, and in the others - hierarchical culture. In turn, in the dimension of culture concerning employee management, in one of the courts the profile of market culture dominated, while in another court, in addition to the characteristics of hierarchical culture, characteristics of clan culture were equally important, and traits of hierarchical culture were dominant in the others.

The differences in the culture dimensions of organizational leadership and employee management noted in the research, as well as the differences in ISMS maturity levels in the studied organizations, made it possible to identify organizational culture characteristics with a potential relationship to ISMS maturity, so the answer to the last question of the research problem is affirmative. In the provincial administrative court, which obtained the highest, fifth level of maturity of the ISMS in the dimensions "leadership style" and "employee management style" in the opinion of respondents, in addition to the features of hierarchical culture, the intensity of clan culture characteristics was the highest among the studied courts. The perceived coincidence between the characteristics of organizational culture and the maturity of the ISMS was the basis for the formulation of recommendations for the development of information security culture in the organization.

Keywords: information security management systems, management systems maturity assessment, organizational culture, information security culture.