POLITECHNIKA LUBELSKA

Marta Juszczyk

Rozbudowa Modelu Akceptacji Technologii dla potrzeb bezpiecznego wykorzystania tożsamości cyfrowej w małych i średnich przedsiębiorstwach

Cz. 1. Modelowanie

MONOGRAFIE

Lublin 2020

Rozbudowa Modelu Akceptacji Technologii dla potrzeb bezpiecznego wykorzystania tożsamości cyfrowej w małych i średnich przedsiębiorstwach

Cz. 1. Modelowanie

Monografie – Politechnika Lubelska

Politechnika Lubelska
Wydział Zarządzania
ul. Nadbystrzycka 38
20-618 Lublin

Marta Juszczyk

Rozbudowa Modelu Akceptacji Technologii dla potrzeb bezpiecznego wykorzystania tożsamości cyfrowej w małych i średnich przedsiębiorstwach

Cz. 1. Modelowanie

Wydawnictwo Politechniki Lubelskiej
Lublin 2020

Recenzent:
prof. dr hab. Ewa Ziemba, Uniwersytet Ekonomiczny w Katowicach
dr hab. inż. Janusz Wielki, Politechnika Opolska

Monografia powstała na podstawie pracy doktorskiej autorki pt. „Rozbudowa modelu akceptacji technologii dla potrzeb bezpiecznego wykorzystania tożsamości cyfrowej w małych i średnich przedsiębiorstwach" napisanej pod kierunkiem dr. hab. Zbigniewa Pastuszaka, prof. UMCS i promotora pomocniczego dr hab. Izabeli Jonek-Kowalskiej, prof. PŚ a obronionej w 2017 roku na Wydziale Organizacji i Zarządzania Politechniki Śląskiej.

Publikacja wydana za zgodą Rektora Politechniki Lubelskiej

© Copyright by Politechnika Lubelska 2020

ISBN: 978-83-7947-452-3

Wydawca: Wydawnictwo Politechniki Lubelskiej
www.biblioteka.pollub.pl/wydawnictwa
ul. Nadbystrzycka 36C, 20-618 Lublin
tel. (81) 538-46-59

Druk: DjaF – 30-092 Kraków, ul. Kmietowicza 1/1
www.djaf.pl

Elektroniczna wersja książki dostępna w Bibliotece Cyfrowej PL www.bc.pollub.pl
Nakład: 50 egz.

Spis treści

Streszczenie

W pracy przedstawiono opracowaną metodykę przygotowania autorskiego Modelu Akceptacji Tożsamości Cyfrowej (Digital Identity Acceptance Model DIAM), utworzonego na bazie Modelu Akceptacji Technologii (Technology Acceptance Model, TAM). W celu jego sporządzenia przeprowadzono kilkuetapowy ciąg działań badawczych.

Na pierwszym etapie badań literaturowych dokonano teoretycznego rozpoznania tematu tożsamości cyfrowych. Źródłem wiedzy były artykuły naukowe, raporty organizacji badających bezpieczeństwo informacyjne oraz rozwój e-gospodarki, a także dokumenty generowane przez przedsiębiorstwa IT, ze szczególnym uwzględnieniem tzw. białych ksiąg.

Wybrano model TAM jako podstawę do objaśnienia czynników powodujących, że pracownicy korzystają z uwierzytelnienia w określony sposób. W celu rozbudowy modelu dokonano krytycznej analizy literatury pod kątem badań nad czynnikami wpływającymi na bezpieczeństwo użytkowania systemów IT (w tym m.in. analiza teorii motywacji oraz dotychczasowego stosowania modelu TAM).

Następnie, w ramach stażu badawczego, prowadzono badania we współpracy z firmą software'ową. Korzystając z doświadczeń pracowników tego przedsiębiorstwa określono przy pomocy metody delfickiej, problematyczne obszary wpływające na stosowanie tożsamości cyfrowych w warstwie implementacji technicznej, organizacyjnej i przede wszystkim praktyki stosowania tożsamości cyfrowych przez pracowników. Ten ostatni obszar wybrany został do sformułowania problemu badawczego.

W kolejnym etapie opracowano i poddano krytyce ekspertów scenariusz wywiadu otwartego, a następnie przeprowadzono badania z jego wykorzystaniem na grupie 10 menedżerów. Pozwoliły one na poznanie postrzegania przez osoby na kierowniczych stanowiskach celowości i motywacji do stosowania tożsamości cyfrowych w przedsiębiorstwie, opinii na temat różnych sposobów dostępu do danych w systemach informatycznych oraz sposobów na zarządzanie pracownikiem tak, by z powierzonego mu dostępu korzystał w przewidziany sposób. Wyniki wywiadów pozwoliły na zdiagnozowanie potencjalnych luk w sposobie zastosowania tożsamości cyfrowych.

Na podstawie badań z wykorzystaniem metody delfickiej oraz wyników wywiadów otwartych, opracowano kwestionariusz badawczy. Kwestionariusz ten wykorzystano do przeprowadzenia badań wstępnych na ograniczonej próbie pracowników polskich przedsiębiorstw. Badania te dotyczyły korzystania z tożsamości cyfrowych w kontekście organizacji dostępu do danych, oraz postrzegania różnych narzędzi uwierzytelnienia przez pracowników przedsiębiorstw. Rezultaty badań wstępnych zostały poddane analizie i wykorzystane w przygotowaniu kwestionariusza do badań ilościowych.

Abstract

In the work, the development of Digital Identity Acceptance Model (DIAM), created on the basis of the Technology Acceptance Model (TAM) was presented. In order to prepare it, a series of research activities were conducted.

In the first stage of literature research, theoretical identification of the topic of digital identities was made. The sources of knowledge were scientific articles, reports of organizations investigating information security and development of e-economy, as well as documents generated by IT companies, with particular reference to white papers.

The TAM model was chosen as the basis for explaining the factors that make employees use authentication in a certain way. To develop the model, critical analysis of the literature has been carried out in order to investigate factors influencing the security of IT systems use (including the analysis of motivation theories and the use of the TAM model).

Then, during the research internship, a preliminary research was conducted in cooperation with a software company. Using the experience of employees of this company, the problematic areas that influence the use of digital identities in the layer of technical implementation, organization and, above all, the practice of using digital identities by employees, have been identified with the Delphi method.
This area was chosen to formulate a research problem.

In the next stage, an open interviews scenario was developed and critiqued by the experts, followed by a study of its use on a group of 10 managers. This allowed to perceive managers perceptions of purposefulness and motivation to use digital identities in an enterprise, their point of view on different ways of accessing information in IT systems, and ways to manage an employee so that he or she is using the assigned access as intended. The results of the interviews have allowed author to diagnose potential gaps in the way which digital identities are used.
Based on the research using the Delphi method and the results of open interviews, a research questionnaire was developed. This questionnaire was used to conduct preliminary research on a limited sample of employees of Polish enterprises. These studies initially concerned: the area of using digital identities with the extension of research in the context of the organization of access to data (individual accounts vs. accounts used by a group of employees), and the perception of various authentication tools by company employees. The results of the preliminary research were analyzed and used in the preparation of the questionnaire for the quantitative research.

1. Wprowadzenie

Systemy informatyczne pełnią bardzo ważną rolę w przedsiębiorstwie. Są to skomputeryzowane części systemu informacyjnego, który jest wielopoziomową strukturą, umożliwiającą użytkownikowi przetwarzanie za pomocą procedur i modeli informacji wejściowych w wyjściowe[1]. Ich głównym zadaniem jest wspierać procesy biznesowe przedsiębiorstwa m.in. poprzez gromadzenie, przetwarzanie i przesyłanie informacji. Przyjmuje się, że dane gromadzone w systemach, takie jak bazy klientów czy własność intelektualna są jednym z najcenniejszych aktywów przedsiębiorstwa. Ponadto, systemy informatyczne są wykorzystywane do zarządzania kapitałem finansowym przedsiębiorstwa, a także systemem produkcji, dystrybucji itp. Co więcej, w wielu przypadkach nie da się oddzielić technologii od realizowanych zadań, a utrata danych lub dostępu do usług mogą skutkować niemożnością prowadzenia działalności. Stąd potrzeba ochrony systemów informatycznych, czyli ochrony danych i zasobów przed przypadkowymi lub złośliwymi działaniami, takimi jak modyfikacja, zniszczenie, dostęp, ujawnienie lub pozyskanie, jeśli działania te nie są uprawnione[2]. Przez ochronę danych zawartych w systemach informatycznych należy rozumieć wdrożenie środków administracyjnych, technicznych lub fizycznych w celu ochrony przed nieuprawnionym dostępem do danych[3]. W niniejszej pracy jako zasoby systemów informatycznych rozumiane będą składniki systemu spełniające funkcję prezentacji, pamiętania, transmisji lub przetwarzania informacji[4] oraz wszelkie dane, do których użytkownik ma dostęp.

Franciszek Wołowski i Janusz Zawiła-Niedźwiecki wskazują, że czynnikami ryzyka systemów informatycznych organizacji są zdarzenia zewnętrzne, procesy, aspekty techniczne oraz ludzie. I to właśnie ludzie, a dokładniej ich działania są często przyczyną wystąpienia incydentów naruszenia bezpieczeństwa[5]. Jednym ze sposobów spowodowania incydentu naruszenia bezpieczeństwa jest skompromitowanie swojej tożsamości cyfrowej przez pracownika. W efekcie inna, nieuprawna osoba może skutecznie uzyskać dostęp do zasobów podając się za upoważnionego do tego pracownika, wskutek przejęcia elementów poświadczających w systemie deklarowaną tożsamość (identyfikatory, hasła, przedmioty). Skutki takiej sytuacji mogą być bardzo poważne, do upadłości

[1] Kisielnicki, J., Soroka, H. (2005). *Systemy informatyczne biznesu – informatyka dla zarządzania*. Warszawa: Placet, s. 18.

[2] *PN-ISO/IEC 2382-1:1996 Technika informatyczna – Terminologia – Terminy podstawowe.*

[3] *PN-ISO/IEC 2382-8 2001 Technika Informatyczna – Terminologia – Bezpieczeństwo.*

[4] Wołowski, F., Zawiła-Niedźwiecki, J. (2012). *Bezpieczeństwo systemów informacyjnych: praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*. Kraków; Warszawa: edu-Libri, s. 68.

[5] Tamże, 82.

przedsiębiorstwa włącznie. Dlatego badania prowadzące do zwiększenia bezpieczeństwa tożsamości cyfrowej w systemach informatycznych są niezwykle ważne nie tylko z naukowego, ale i praktycznego punktu widzenia. Z uwagi na gospodarowanie niskim budżetem (ograniczenia w nabywaniu specjalistycznego oprogramowania do zarządzania tożsamością cyfrową i dostępem) oraz znaczenie bliskich relacji z pracownikiem, badania dotyczące roli aspektu ludzkiego, relacji kierownictwa i pracowników wykonawczych w budowaniu bezpieczeństwa informatycznego, są bardzo pożądane dla przedsiębiorstw sektora MSP.

1.1. Problem badawczy

Dostęp do zasobów systemów teleinformatycznych przedsiębiorstwa, jest jednym z obszarów, który powinien być poddany zarządzaniu. Jego ochrona wpływa bowiem na działalność organizacji dwojako. Z jednej strony zapewnienie bezpieczeństwa dostępu obniża efektywność działania pracownika, gdyż powoduje konieczność poświęcenia czasu na procesy uwierzytelnienia, nierzadko wielokrotne. Z drugiej jednak strony zabezpiecza przedsiębiorstwo przez skutkami wycieku danych, ich utraty, zmiany czy niewłaściwego wykorzystania, które mogą mieć poważne skutki – z upadłością przedsiębiorstwa włącznie. Bilansowanie tak pojętych strat (efektywności) i korzyści (bezpieczeństwa) jest zadaniem kierownictwa organizacji na różnych poziomach, w ramach ustalenia zasad, ich wdrożenia i przestrzegania.

Osiągany poziom bezpieczeństwa zasobów gromadzonych w systemach informatycznych zależy zarówno od bezpośredniego użytkownika, jak i czynników zewnętrznych, w tym tych, które na użytkownika oddziałują, a w szczególności od działań kierownictwa przedsiębiorstwa.

Co zatem sprawia, że użytkownicy systemów informatycznych korzystają z zasobów w systemach teleinformatycznych w sposób bezpieczny?

W pracy skupiono się na poniższych zagadnieniach, które jednocześnie stanowią główny problem badawczy:

1. Czy i w jakim stopniu zapewnienie bezpieczeństwa dostępu do zasobów w systemach teleinformatycznych wpisuje się w strategię przedsiębiorstw?
2. Czy w przedsiębiorstwach sektora MSP stosowane są rozwiązania techniczne i systemowe podnoszące bezpieczeństwo dostępu do zasobów w systemach IT?
3. Jaki jest poziom dowolności działań pracowników w sposobie uzyskiwania dostępu do zasobów w systemach IT?
4. Jakim poziomem bezpieczeństwa charakteryzują się działania pracowników w tym obszarze?

5. W jaki sposób kadra zarządzająca wpływa na pracowników w celu zapewnienia oczekiwanego poziomu bezpieczeństwa dostępu do zasobów w systemach IT?
6. Czy działania te są oceniane przez pracowników jako skuteczne?
7. Czy istnieje różnica między postrzeganiem bezpieczeństwa, skutecznością działań motywacyjnych oraz osiąganym poziomem bezpieczeństwa między kadrą zarządzającą a pracownikami wykonawczymi?
8. Jakie czynniki wpływają na postawę pracowników wobec sposobu korzystania z zasobów systemów IT?

1.2. Cel pracy

Cel główny

Podstawowym celem naukowym pracy jest modelowanie akceptacji bezpiecznego wykorzystania tożsamości cyfrowej przez pracowników sektora MSP.

Cel utylitarny:

1. Opracowanie procedury badawczej, umożliwiającej pozyskanie rzetelnych danych do utworzenia i kwantyfikacji Modelu Akceptacji Tożsamości Cyfrowej (Digital Identity Acceptance Model, DIAM).
2. Przygotowanie modelu DIAM, który po skwantyfikowaniu posłuży do formułowania rekomendacji dla kadry zarządzającej, określających sposób zwiększenia bezpieczeństwa wykorzystania tożsamości cyfrowej pracowników sektora MSP oraz jego implementację.

1.3. Aspekty metodyczne budowy modelu akceptacji tożsamości cyfrowej

Aby osiągnąć główny cel pracy, czyli zbudować Model Akceptacji Tożsamości Cyfrowej przyjęto następujący tok działań:

- wybór i eksploracja obszaru badawczego,
- postawienie problemu badawczego,
- opracowanie koncepcji rozwiązania problemu.

Działania te zgrupowano w następujące etapy:

1. badania wstępne,
2. modelowanie.

W pierwszym etapie badań (tabela 1.1.) dokonano teoretycznego rozpoznania tematu tożsamości cyfrowych. Źródłem wiedzy były artykuły naukowe, raporty organizacji badających bezpieczeństwo informacyjne oraz rozwój e-gospodarki,

a także dokumenty generowane przez przedsiębiorstwa IT, ze szczególnym uwzględnieniem tzw. białych ksiąg.

Wybrano model akceptacji technologii (*Technology Acceptance Model*, TAM) jako podstawę do objaśnienia czynników powodujących, że pracownicy korzystają z uwierzytelnienia w określony sposób. W celu rozbudowy modelu dokonano krytycznej analizy literatury pod kątem badań nad czynnikami wpływającymi na bezpieczeństwo użytkowania systemów IT (w tym m.in. analiza teorii motywacji oraz dotychczasowego stosowania modelu TAM).

Następnie, w ramach stażu badawczego prowadzono badania we współpracy z firmą software'ową. Korzystając z doświadczeń pracowników tego przedsiębiorstwa określono, przy pomocy metody delfickiej, problematyczne obszary wpływające na stosowanie tożsamości cyfrowych w warstwie implementacji technicznej, organizacyjnej i przede wszystkim praktyki stosowania tożsamości cyfrowych przez pracowników. Ten ostatni obszar wybrany został do sformułowania problemu badawczego.

Dalsze badania podążały dwutorowo: w kierunku tworzenia podstaw teoretycznych z zakresu teorii motywacji (analiza literatury) oraz w kierunku dalszego, praktycznego badania zdefiniowanego problemu badawczego.

W tym celu opracowano i poddano krytyce ekspertów scenariusz wywiadu otwartego, a następnie przeprowadzono badania z jego wykorzystaniem na grupie 10 menedżerów. Pozwoliły one na poznanie postrzegania przez osoby na kierowniczych stanowiskach celowości i motywacji do stosowania tożsamości cyfrowych w przedsiębiorstwie, opinii na temat różnych sposobów dostępu do danych w systemach informatycznych oraz sposobów na zarządzanie pracownikiem tak, by z powierzonego mu dostępu korzystał w przewidziany sposób. Wyniki wywiadów pozwoliły na zdiagnozowanie potencjalnych luk w sposobie zastosowania tożsamości cyfrowych.

Na podstawie badań z wykorzystaniem metody delfickiej oraz wyników wywiadów otwartych, opracowano kwestionariusz badawczy. Kwestionariusz ten wykorzystano do przeprowadzenia badań wstępnych na ograniczonej próbie pracowników polskich przedsiębiorstw. Badania wstępne dotyczyły:

- Obszaru korzystania z tożsamości cyfrowych z rozszerzeniem o badanie sposobu dostępu do danych (konta indywidualne vs. konta wykorzystywane przez grupę pracowników).
- Postrzegania różnych narzędzi uwierzytelnienia przez pracowników przedsiębiorstw.

Rezultaty badań wstępnych zostały poddane analizie i wykorzystane do utworzenia kwestionariusza badań właściwych.

Tabela 1.1. Proces badawczy – badania wstępne

Etap badań	Zadania badawcze	Rezultaty
Badania wstępne.	1. Analiza literatury.	• Zdiagnozowane problemy związane z tożsamością cyfrową w MSP. • Analiza teorii motywacji oraz zdiagnozowana stosowalność modelu TAM.
	2. Badania metodą delficką.	Obszary badań bezpiecznego wykorzystania tożsamości cyfrowej w MSP.
	3. Opracowanie scenariusza wywiadu otwartego.	Scenariusz wywiadu otwartego.
	4. Przeprowadzenie wywiadów otwartych – niestrukturalizowanych z menedżerami i pracownikami dotyczących stosowania tożsamości cyfrowych (wstępne rozpoznanie zagadnienia).	Rezultaty wywiadów.
	5. Analiza rezultatów badania metodą delficką oraz przy pomocy wywiadów otwartych.	Raport.
	6. Opracowanie kwestionariuszy badań wstępnych.	Kwestionariusze badań wstępnych dotyczące: • typów tożsamości cyfrowych stosowanych w MSP (badanie wstępne pierwsze), • sposobów uwierzytelniania stosowanych w MSP (badanie wstępne drugie).
	7. Badania wstępne na ograniczonej próbie badawczej.	Dane z badań wstępnych.

Źródło: opracowanie własne.

Drugim etapem badań było opracowanie teoretycznego Modelu Akceptacji Tożsamości Cyfrowej (*Digital Identity Acceptance Model* – DIAM) przez pracowników małych i średnich przedsiębiorstw (tabela 1.2.).

Model opracowano na podstawie modelu akceptacji technologii TAM, z uwzględnieniem innych modeli, przeglądu literatury w obszarze badań empirycznych oraz wniosków z obu badań wstępnych.

Oryginalny model TAM zmodyfikowano w dwóch kierunkach:

1. Rozbudowy – rozszerzono model TAM o dodatkowe czynniki potencjalnie tłumaczące sposób korzystania z tożsamości cyfrowych przez użytkowników systemów informatycznych w przedsiębiorstwach MSP
2. Redefinicji jednego z kluczowych elementów modelu – postrzeganej użyteczności (*Perceived Usefulness – PU*).

Tabela 1.2. Proces badawczy – modelowanie

Etap badań	Zadania badawcze	Rezultaty
Modelowanie	1. Analiza rezultatów badań wstępnych	Rezultaty analizy
	2. Opracowanie wstępnego modelu DIAM	Wstępny model DIAM

Źródło: opracowanie własne.

Tak przygotowany model będzie gotowy do skwantyfikowania w celu zbadania siły i istotności zależności między jego elementami.

2. Tożsamość cyfrowa w systemach informacyjnych zarządzania

2.1. Wprowadzenie do zagadnienia tożsamości cyfrowej

2.1.1. Istota pojęcia „tożsamość cyfrowa”

Dla zrozumienia istoty tożsamości cyfrowej konieczne jest nawiązanie do pojęcia *tożsamość* w świecie rzeczywistym.

Tożsamość można rozumieć dwojako; w sensie konstytuującym: *jako system cech*, które sprawiają, że można mówić o tożsamości; w ujęciu komparatywnym jako *identyczność dwóch obiektów*. Byty są tożsame jeśli są identyczne, czyli zachodzi równość wszystkich zmiennych (cech), które się na nie składają[6].

Według Waldemara Kamińskiego tożsamość to „*zespół wyobrażeń, uczuć, sądów, wspomnień i projekcji podmiotu, który odnosi on do siebie. W pojęciu tym mieszczą się takie składniki, jak: samoświadomość jednostki, świadomość kontynuacji i pozostawania sobą w zmieniających się warunkach życia, świadomość uczestnictwa podmiotu w grupach społecznych, koncepcja siebie, zdolność do porównań interpersonalnych i grupowych*"[7].

Według twórcy koncepcji tożsamości Erika H. Eriksona pojęcie to powinno być rozpatrywane w kontekście dwóch relacji: *stosunku do siebie samego* i *stosunku do innych ludzi* [8]. Wróblewska wskazuje na dwa wymiary tożsamości: biograficzno-wertykalny, którego istotą jest ciągłość tożsamości w czasie, oraz społeczno-horyzontalny, odnoszący się do elementów składających się na tożsamość w danym momencie czasu[9]. Natomiast Jianwei Liu i in. określają ją po prostu jako fakt bycia tym, kim lub czym jest osoba lub rzecz[10].

Wyobrażenia, sądy i przekonania człowieka o samym sobie[11] pozwalające na dostrzeżenie elementów odróżniających jednostkę od innych (poczucie

---

[6] *Słownik Języka Polskiego.* Online: http://sjp.pwn.pl, dostęp: 2011.09.20.

[7] Kamiński, W. (1996). *Człowiek dorosły w sytuacjach zagrożenia tożsamości*. W: Wujek, T., red. Wprowadzenie do andragogiki. Warszawa: Instytut Technologii Eksploatacji, s. 77.

[8] Warchał, M. (2009). *Językowe (re)konstrukcje tożsamości (psycho- i etnolingwistyczna analiza chorwackich wypowiedzi narracyjnych)*. Praca doktorska. Uniwersytet Śląski w Katowicach. Wydział Filologiczny. Katowice, s. 65.

[9] Wróblewska, M. (2013). *Kształtowanie tożsamości w perspektywie rozwojowej i edukacyjnej*. Pogranicze, Studia Społeczne. Tom XVII. s. 176–187, s. 178.

[10] Liu, J., Hodges, A., Clay, L., Monarch, J. (2020). *An analysis of digital identity management systems - a two-mapping view*. 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 92–96 s., s. 92.

[11] *Encyklopedia socjologii* (2002). Warszawa: Oficyna Naukowa, s. 252.

odrębności) określono jako **tożsamość osobową (indywidualną)**[12]. Natomiast system wiedzy dotyczący wspólnych właściwości z innymi osobami oraz poczucie przynależności do grupy zostały zdefiniowane jako **tożsamość społeczna**[13]. Tożsamość zatem jest dualna – opiera się na odrębności (różnicach) i przynależności (podobieństwach)[14]. Te cechy tożsamości osobowej znajdują odzwierciedlenie w tożsamości cyfrowej.

Według Polskiej Normy tożsamość jest elementem danych przypisanych podmiotowi i wykorzystywanych do jego identyfikowania np. imię i nazwisko[15].

Tożsamość jest manifestowana w zależności od okoliczności i kontekstu[16]. W różnych sytuacjach jednostka ujawnia zestaw cech i zachowań. Ta właściwość jest również odwzorowana w rzeczywistości wirtualnej.

Tożsamość cyfrowa należy do **tożsamości wirtualnych**, czyli istniejących w świecie wirtualnym (w tym przypadku generowanym przez komputery), który posiada wszelkie cechy realnego świata oprócz jednej – istnienia[17] i jest światem obrazowanym[18].

Przykładem świata wirtualnego może być rzeczywistość gier RPG[19], których uczestnicy tworzą tożsamości wirtualne, posiadające cechy tożsamości osobowych w świecie realnym (por. tabela 2.1.).

[12] Wróblewska, M. (2013). *Kształtowanie tożsamości w perspektywie rozwojowej i edukacyjnej*. Pogranicze. Studia Społeczne. Tom XVII. 176–187 s., s. 178.

[13] Tamże.

[14] Tamże.

[15] *PN-I-02000 poz. 3.4.093* za: Mielnicki, T. i inni red. (2013). *Identyfikacja i uwierzytelnienie w usługach elektronicznych. Forum Technologii Bankowych przy Związku Banków Polskich*. Warszawa. Online: https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf, dostęp: 2017.06.04.

[16] Knight, A., Saxby, S. (2014). *Identity crisis: Global challenges of identity protection in a networked world*. Computer Law & Security Review, Volume 30, Issue 6, s. 617–632.

[17] Sitarski, P. (2002). *Rozmowa z cyfrowym cieniem*. Kraków: Rabid, s. 14.

[18] Branicki, W. (2009). *Tożsamość a wirtualność*. Kraków: Nomos, s. 9.

[19] RPG (*Role Playing Game*) zwana też *grą wyobraźni* czy *grą fabularną to* gra, która polega na wcielaniu się w określone, fikcyjne postaci i podejmowaniu decyzji w ramach ustalonych przez narratora (Mistrza Gry). Gra bazuje na wyobraźni jej uczestników wspomaganej (lub nie) akcesoriami takimi jak kości (wprowadzenie elementu losowości), karty czy plansze. Przebieg gry, czyli pojawiające się sytuacje, działania bohaterów i ich skutki ma formę opowiadania lub dialogu (nierzadko w pierwszej osobie) graczy. Gra wymaga od uczestników improwizowania.

Tabela 2.1. Przykładowe zestawienie tożsamości realnej osoby i postaci z gry RPG

	Świat realny	**Świat wirtualny**
Tożsamość osobowa (indywidualna)	Cechy fizyczne, psychologiczne i behawioralne człowieka (np. wzrost)	Opis wyglądu, umiejętności czy parametrów postaci fikcyjnej (np. siła)
Tożsamość społeczna	Cechy warunkujące przynależność do grup społecznych (np. narodowość)	Opis afiliacji postaci fikcyjnej (np. przynależność do gildii)

Źródło: opracowanie własne.

Zagadnienie tożsamości cyfrowej zrodziło się wraz z pojawieniem się świata wirtualnego, generowanego z użyciem nowoczesnych technologii telekomunikacyjnych (*Information and Communication Technologies,* ICT). Samo pojęcie tożsamość cyfrowa, to kombinacja dwóch słów: *tożsamość*, nawiązująca do przedstawionej uprzednio tożsamości osoby oraz *cyfrowa*, zawężającej manifestację tego bytu do zapisu w formie binarnej, interpretowanej przez komputer. **Innymi słowy jest to taka tożsamość, która może być zdigitalizowana, czyli tworzona, przetwarzana, przesyłana i przechowywana przy użyciu technologii i narzędzi ICT**.

Tożsamość osobowa, która znajduje się w kręgu zainteresowania zarówno filozofii, psychologii, jak i socjologii, jest pojęciem stosunkowo dobrze zdefiniowanym, i ściśle, choć wielorako, określonym. Tożsamość cyfrowa natomiast, jako pojęcie stosunkowo nowe, została zdefiniowana głównie przez praktyków-informatyków i stanowi, wraz z rozwojem technologii i jej przenikaniem do kolejnych sfer życia, coraz bardziej interesujący temat dla badaczy teoretyków, wywodzących się nie tylko wspomnianych uprzednio nauk (filozofia, psychologia i socjologia), ale także z dyscypliny nauk o zarządzaniu.

Tożsamość cyfrowa (*Digital Identity*) w ujęciu konstytuującym to abstrakcyjna reprezentacja **jednostki**, zwanej też **podmiotem cyfrowym**, w systemie komputerowym[20], przy czym jednostką tą nie musi być jedna, konkretna osoba. Celem tworzenia tożsamości cyfrowej nie jest często dokładne

[20] Johansson, J.M. (2009). *Security Watch: Thoughts on Identity, Part 1.* TechNet Magazine, June 2009. Online: https://technet.microsoft.com/en-us/magazine/2009.06.securitywatch, dostęp: 2017.06.04. oraz Gutierrez, A.J. (2006). *Towards better Digital Identity Management. Sensitive Information in a Wired World* CPSC 457b, s. 6. Online: http://zoo.cs.yale.edu/classes/cs457/spr06/info_paper.pdf, dostęp: 2017.06.04.

odwzorowanie (przeniesienie) obiektu istniejącego w świecie realnym, lecz utworzenie abstrakcyjnego obiektu powiązanego z obiektem istniejącym[21].

Definicja, którą można traktować jako podstawową dla obszaru badań niniejszej pracy, określa tożsamość cyfrową jako „*zbiór stwierdzeń podmiotu cyfrowego na swój własny temat lub na temat innego podmiotu cyfrowego*"[22]. Stwierdzenia, są to takie cechy, które da się porównać wykorzystując narzędzia teleinformatyczne, by stwierdzić identyczność (bądź nie) podmiotu deklarowanego (deklarowana tożsamość) z wzorcem (dana tożsamość cyfrowa). Tożsamość w świecie cyfrowym zatem to konstrukcja, która bazuje na *byciu tożsamym (identycznym)*, co można przedstawić jako[23]:

$$(P=Q)\rightarrow(P=Q)$$

Wspomniany **obiekt odwzorowany** przez podmiot cyfrowy może być osobą, ale także organizacją, programem, urządzeniem lub inną rzeczą, która wymaga dostępu do zasobów cyfrowych (np. system, strona internetowa czy baza danych), urządzeń lub relacji pomiędzy innymi podmiotami cyfrowymi[24].

Tożsamość cyfrowa, podobnie jak ta istniejąca w świecie realnym, obejmuje dwa aspekty: indywidualność (odrębność) i relację (przynależność). Z uwagi na specyficzną konstrukcję i środowisko, w którym funkcjonuje tożsamość cyfrowa, nie ma w zasadzie różnic pomiędzy tożsamością cyfrową osoby ludzkiej a przedmiotu (por. tabela 2.2.).

Tabela 2.2. Przykładowe porównanie tożsamości cyfrowej osoby i przedmiotu

	Tożsamość cyfrowa osoby	**Tożsamość cyfrowa przedmiotu**
Aspekt odrębności	Dane pozwalające na identyfikację osoby np. login	Dane pozwalające na identyfikację przedmiotu np. adres MAC
Aspekt przynależności	Dane wskazujące na przynależność do grupy tożsamości np. pracownik działu marketingu	Dane wskazujące na przynależność do grupy np. adres IP bramy

Źródło: opracowanie własne.

[21] Tamże.
[22] Cameron, K. (2005). *The Laws of Identity*. Online: http://myinstantid.com/laws.pdf, dostęp: 2017.06.04, s. 6.
[23] Johansson, J.M. (2009). *Security Watch: Thoughts on Identity, Part 1*. TechNet Magazine, June 2009. Online: https://technet.microsoft.com/en-us/magazine/2009.06.securitywatch, dostęp: 2017.06.04.
[24] Tamże.

Podobnie ujmuje to Philip J. Windley, określając tożsamość cyfrową jako zbiór danych, które jednoznacznie określają osobę lub rzecz, ale także zawierają jej relacje z innymi jednostkami (podmiotami cyfrowymi) [25]. Dane te dla uproszczenia nazywa atrybutami, ale dzieli na[26]:

- atrybuty (*Attributes*) – nietrwałe cechy/dane nabyte/gromadzone przez podmiot cyfrowy,
- preferencje (*Preferences*) – pożądane wybory/cechy,
- przymioty niezbywalne (*Traits*) – trwałe cechy/dane posiadane przez podmiot cyfrowy.

Przykładowe zastosowanie praktyczne tego podziału w odniesieniu do osób i rzeczy przedstawiono w tabeli 2.3.

Tabela 2.3. Przykładowe atrybuty tożsamości cyfrowej osoby i przedmiotu wg podziału Ph. J. Windley'a

	Tożsamość cyfrowa osoby	**Tożsamość cyfrowa przedmiotu**
Atrybuty	Stanowisko, adres zamieszkania	Numer IP
Preferencje	Ustawienia systemu, programów użytkowych	Sposób kodowania
Przymioty niezbywalne	Unikalny w skali systemu identyfikator, narodowość, numer PESEL, data zatrudnienia	Numer MAC urządzenia

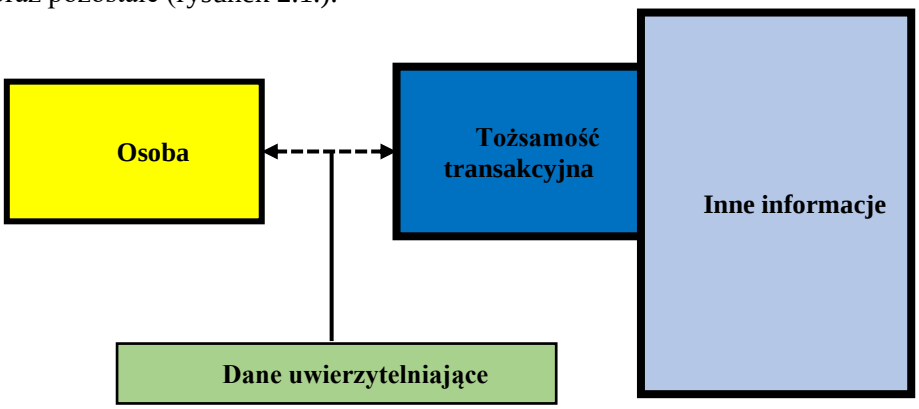
Źródło: pracowanie własne.

Inny podział zaproponowali Elisa Bertino i Kenji Takahashi. Punktem wyjścia były funkcje pełnione przez dane składające się na tożsamość cyfrową. Wyróżniają zatem[27]:

- **identyfikatory** (*Identifiers*), czyli serie bitów, znaków i symboli lub też wszelkie inne dane, które pozwalają na zidentyfikowanie podmiotu np. nazwa konta (login),
- **poświadczenia** (*Credentials*), czyli dane, które pozwalają na zweryfikowanie tożsamości np. hasło,
- **atrybuty** (*Attributes*), czyli dane opisujące cechy podmiotu cyfrowego takie jak np. dane osobowe, preferencje, afiliacje, reputacja.

[25] Windley, Ph. J. (2005). *Digital Identity*. Sebastopol: O'Reily, s. 8.
[26] Tamże.
[27] Bertino, E., Takahashi, K. (2011). *Identity Management, Concepts, Technologies, and Systems*. London: Artech House, s. 21–22.

Niektórzy autorzy (np. Clare Sullivan)[28] silnie akcentują cel, w jakim tożsamość cyfrowa jest tworzona, wyodrębniając tzw. tożsamość transakcyjną (*Transactional Identity*), rozumianą jako ograniczony zestaw danych, które określają tożsamość użytkownika w celach dokonania szeroko rozumianej transakcji. W tym modelu dodatkowo zidentyfikowane są: dane uwierzytelniające oraz pozostałe (rysunek 2.1.).



Rysunek 2.1. Relacje między osobą a jej tożsamością cyfrową
Źródło: Sullivan, C. (2012). Digital identity and mistake. International Journal of Law and Information Technology, Vol. 20, No 3, s. 8. (tłum. własne).

Tożsamość cyfrowa została też opisana w postaci modelu warstwowego, który zawiera[29]:

Warstwę 1. Identyfikator (*Identifier*) – unikalny i niepowtarzalny w skali systemu, odpowiadający za rozpoznawalność tożsamości np. PESEL.

Warstwę 2. Poświadczenia (*Credentials*) – dane, które służą potwierdzeniu deklarowanej tożsamości np. zdigitalizowany odcisk palca.

Warstwę 3. Główny profil (*Main Profile*) – dodatkowe dane (atrybuty), opisujące cechy tożsamości np. imię.

Warstwę 4. Kontekstowy profil (*Context-base Profile*) – dane, które są zrozumiałe tylko w kontekście systemu np. data zatrudnienia.

W tym ujęciu tożsamość może mieć jeden unikalny identyfikator, ograniczony zestaw poświadczeń i danych głównego profilu, ale nieograniczony zestaw danych kontekstowych.

[28] Sullivan, C. (2012). *Digital identity and mistake*. International Journal of Law and Information Technology, Vol. 20, No. 3, s. 8.

[29] Filho, F.G., (2008). *The Evolving Role of the Identity: From the Lone User to the Internet 2*. The Architecture Journal, Journal 16. Microsoft. Online: http://msdn.microsoft.com/en-us/library/cc837112.aspx, dostęp: 2015.01.06.

Podobnie tożsamość jest postrzegana przez specjalistów firmy Hewlett Packard[30], którzy wyodrębniają unikalne dane składające się na profil, dane identyfikacyjne i dane pozwalające na uzyskanie dostępu do zasobów. Każdy z wymienionych elementów może być związany z różnymi kontekstami i różną rolą posiadacza tożsamości w różnych systemach.

Relacje łączące tożsamości cyfrowe z obiektami w świecie rzeczywistym mogą być wielorakie:

- Jeden do jednego – tożsamość cyfrowa jest przypisana do jednej konkretnej osoby np. internetowe konto bankowe.
- Jeden do wielu – z jednej tożsamości korzysta wiele osób tj. za pomocą jednego identyfikatora i poświadczenia dostęp do danych uzyskuje więcej niż jedna osoba np. e-mail grupy studentów.
- Wiele do jednego – jedna osoba ma wiele różnych tożsamości cyfrowych (zwykle wykorzystywanych w określonym kontekście) np. posiadanie różnych kont na serwisach społecznościowych, forach, portalach itp.
- Wiele do wielu – gdy grupa osób korzysta z różnych tożsamości by uzyskać dostęp do różnych zasobów np. stosowanie różnych e-maili na potrzeby grupy studentów do celów formalnych (kontakty z wykładowcami) i nieformalnych (komunikacja członków grupy).

W świecie realnym tożsamość jest w posiadaniu podmiotu, który jest jej dysponentem. To stwierdzenie nie jest natomiast pewnikiem w świecie wirtualnym. Ciekawe spojrzenie na kwestię „własności" tożsamości wykazał David Sears, proponując autorską klasyfikację tożsamości cyfrowych. Według niego[31]:

- **Medentity** („moja" tożsamość) to klasycznie rozumiana tożsamość, przypisana do jednej osoby, będąca jej własnością i pod jej kontrolą. Pojawia się wraz z narodzinami człowieka.
- **Ourdentity** („nasza" tożsamość) jest tożsamością opartą na obopólnym porozumieniu dwóch stron: podmiotu (który korzysta z tożsamości) oraz współtwórcy tożsamości. Kontrola nad danymi wchodzącymi w skład tak rozważanej tożsamości jest dzielona pomiędzy obie strony. Przykładem jest konto na forum internetowym. Użytkownik może np. takie konto zakładać/usuwać oraz wykorzystywać w celach umieszczania postów w dyskusjach, jednak administrator strony może edytować posty lub zawieszać konto.
- **Theirdentity** („ich" tożsamość), to tożsamość abstrakcyjna, która jest tworzona przez trzecią stronę bez wyraźnej zgody podmiotu, którego dotyczy. Przykładem jest „wydobywanie tożsamości" przez

[30] Hewlett Packard (2005). *The HP Security Handbook. Protecting Your Business*, s. 24.

[31] Bertino, E., Takahashi, K. (2011). *Identity Management, Concepts, Technologies, and System*s. London: Artech House, s. 22–23.

wyszukiwarkę, która na podstawie e-mailowych cookies tworzy model (profil) użytkownika w celu dostosowania wyświetlanej na stronie reklamy, profilowania treści lub odsprzedaży gromadzonych atrybutów tożsamości specjalistom od analiz rynkowych. Podmiot jest często nieświadomy istnienia takiej tożsamości, i mimo, iż ją generuje, nie ma kontroli ani nad elementami, z których się składa, ani nad nią samą.

Implikacje z tworzenia tożsamości, na którą podmiot nie ma wpływu poruszają także inni autorzy szczególnie w kontekście społecznym i gospodarczym[32]. Jest to obecnie jeden z najbardziej istotnych obszarów badań tożsamości cyfrowej.

Tę samą kwestię, ale z punktu widzenia strony niebędącej podmiotem przedstawia Fernando Filho, dzieląc tożsamości cyfrowe na **zarządzalne** (np. tożsamość pracownika, dostawcy, drukarki itp.) i **niezarządzalne** (np. tożsamość klienta sklepu online, partnera biznesowego)[33]. Kryterium podziału jest poziom kontroli, jaki sprawowany jest nad tożsamością, możliwością przeprowadzenia audytu czy działań, które można podjąć w przypadku niewłaściwego korzystania z tożsamości (np. odcięcie od Internetu) i wynika ze zobowiązań osób w realnym świecie. Co prawda klient sklepu internetowego deklaruje zaznajomienie się z obowiązującymi go zasadami i deklaruje ich przestrzeganie, jednak zwykle jest to tylko namiastka prawdziwej odpowiedzialności, którą można wyegzekwować od użytkownika konta zarządzalnego.

Istotną różnicą pomiędzy światem wirtualnym i realnym jest fakt, że w świecie realnym, z uwagi na brak samoświadomości, rzeczy nie mogą być podmiotami tożsamości, w przeciwieństwie do świata cyfrowego, w którym jak wspomniano tożsamość cyfrową mogą posiadać rzeczy (komputery, urządzenia), organizacje czy programy.

Z uwagi na szeroki zakres pojęcia tożsamość cyfrowa i duże zróżnicowanie jego interpretacji, w niniejszej pracy ***tożsamość cyfrowa*** będzie rozumiana jako ***zbiór atrybutów pozwalających na jednoznaczną identyfikację i uzyskanie uprawnionego dostępu do zasobów przedsiębiorstwa przez pracownika lub pracowników i przez nich współtworzona i współzarządzana.***

[32] Beck, E.N., (2015). *The Invisible Digital Identity: Assemblages in Digital Networks.* Computers and Composition, Volume 35, March 2015, s. 125–140.

[33] Filho, F.G., (2008). *The Evolving Role of the Identity: From the Lone User to the Internet 2*. The Architecture Journal, Journal 16. Microsoft. Online: http://msdn.microsoft.com/en-us/library/cc837112.aspx, dostęp: 2015.01.06.

2.1.2. Potrzeba stosowania tożsamości cyfrowej

Powstanie, używanie i stałe dostosowanie tożsamości cyfrowej wynika z potrzeby zapewnienia bezpieczeństwa informacji generowanej, przechowywanej, przetwarzanej oraz przesyłanej w sposób cyfrowy[34].

Informacja uważana za bezpieczną, charakteryzuje się następującymi cechami[35]:

1. Poufnością i autentycznością, czyli dostępem ograniczonym wyłącznie do osób z potwierdzonym uprawnieniem dostępu.
2. Integralnością danych i systemu, czyli zapewnieniem, że na dane ani działanie systemu nie miały wpływu osoby nieuprawnione lub działające w sposób nieuprawniony.
3. Dostępnością i niezawodnością, rozumianymi jako możliwość dostępu do żądanych danych we właściwym miejscu i czasie w sposób powtarzalny (tj. dający te same skutki przy tych samych działaniach).
4. Rozliczalnością, czyli możliwością przypisania działań w systemach informatycznych konkretnemu użytkownikowi.

Z analizy wymienionych uprzednio cech wynika, że zapewnienie dostępu do szeroko rozumianych zasobów systemów informatycznych wyłącznie osobom autoryzowanym, w zakresie dla nich koniecznym, jest jednym z kluczowych elementów zapewnienia bezpieczeństwa informacji[36].

Znaczenie bezpieczeństwa informacji jest kluczowe z punktu widzenia przetrwania i rozwoju przedsiębiorstwa. Konieczne jest spełnianie wymogów prawnych, dotyczących np. danych osobowych (dane klientów czy kontrahentów) gromadzonych w bazach danych w przedsiębiorstwie[37], ochrony informacji niejawnych[38], czy poufnych, których ujawnienie narażałyby na szwank stronę trzecią np. współpracującą z przedsiębiorstwem jednostkę. Ponadto, zabezpieczenie informacji, określanej często jako jeden z najcenniejszych zasobów współczesnych organizacji[39] pozwala na zachowanie przewagi konkurencyjnej.

---

[34] Szyjewski, G. (2011). *Wykorzystanie modeli procesów biznesowych BPMN 2.0 do identyfikacji potrzeb zdalnego uwierzytelniania*. Metody Informatyki Stosowanej Nr 3/2011 (28), s. 167–178.

[35] *PN-13335-1*.

[36] Wielki, J. (2012). *Analiza wyzwań związanych z zarządzaniem przestrzenią elektroniczną przez współczesne organizacje gospodarcze*. Problemy Zarządzania, Vol. 10, Nr 3 (38), Uwarunkowania zastosowań systemów informatycznych w gospodarce, Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania UW, s. 54–66.

[37] *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883*.

[38] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Dz.U. 2010 nr 182 poz. 1228.*

[39] Milanowicz, M. (2012). *Elektroniczna wymiana danych (EDI) jako atrybut współczesnego społeczeństwa informacyjnego*. W: Społeczeństwo informacyjne –

Zastosowanie systemów informatycznych w firmie umożliwia stosowanie zarówno zarządzania relacjami z klientami (*Customer Relationship Management*, CRM), zarządzania wiedzą (*Knowledge Management*, KM)[40] jak i analitykę biznesową (*Business Intelligence*, BI)[41].

Korzystanie z tożsamości cyfrowych stało się konieczne w realiach gospodarki elektronicznej[42], gdy kontakt za pośrednictwem narzędzi ICT jest powszechny w ramach funkcjonowania przedsiębiorstwa, a pewność co do tożsamości osoby, z którą się komunikuje jest kluczowa[43]. Komunikacja ta może przebiegać na linii pracownik – interesariusz (pracownik, klient, kontrahent itp.), ale też, traktowana szerzej, może być elementem dokonywanej przez nich transakcji. Stąd, można wskazać dwa istotne obszary wykorzystania tożsamości cyfrowej przez przedsiębiorstwa: ochronę szeroko pojętych aktywów przedsiębiorstwa oraz ochronę szeroko pojętego procesu komunikacji.

2.2. Obszary stosowania tożsamości cyfrowej

Z uwagi na dwa podstawowe cele tożsamości cyfrowej, czyli potwierdzenia tożsamości użytkownika i umożliwienie dostępu do zasobów, staje się ona narzędziem uniwersalnym w kontakcie człowieka z komputerem, a w szczególności, za pośrednictwem sieci. Innymi słowy wszędzie tam, gdzie aktywność człowieka jest wspomagana przy użyciu technologii ICT, tożsamość cyfrowa będzie pełniła ważną rolę[44]. W celu uporządkowania tego wywodu określono:

1. Obszary działalności człowieka w ogóle oraz te, które są wspomagane przez technologie ICT.

uwarunkowania rozwoju. Zeszyty naukowe nr 680. Problemy zarządzania, finansów i marketingu Nr 21. Szczecin. Uniwersytet Szczeciński, s. 37.

[40] Ziemba, E. (2012). *Transformacja zarządzania relacjami z klientami w kierunku zarządzania wiedzą klienta – kanony i technologie informatyczne*. W: Ziemba, E., Olszak, C.M. red, Technologie informacyjne w transformacji współczesnej gospodarki. Katowice: Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, s. 32.

[41] Olszak, C.M. (2012). *Organizacja oparta na Business Intelligence*. W: Ziemba, E., Olszak, C.M. red., Technologie informacyjne w transformacji współczesnej gospodarki. Katowice: Wydawnictwo Uniwersytetu Ekonomicznego W Katowicach, s. 9–29.

[42] Ziemba, E., Obłąk, I. (2012). *Systemy informatyczne w organizacjach zorientowanych procesowo*. Problemy Zarządzania, Vol. 10, Nr 3 (38), s. 2–8.

[43] Szyjewski, G., Niemcewicz, P. (2016). *Zdalna realizacja usług w Internecie z uwzględnieniem profilu użytkownika*. Studia Informatica Pomerania, Nr 3 (41), s. 79–89.

[44] Wójtowicz, A., Cellary, W. (2010). *Representing User Privileges in Object-Oriented Virtual Reality Systems*. W: Camarinha-Matos, L.M., Pereira, P., Ribeiro, L. red. Emerging Trends in Technological Innovation. Proceedings of First IFIP WG 5.5/SOCOLNET Doctoral Conference on Computing, Electrical and Industrial Systems, DoCEIS 2010 Costa de Caparica, Portugal, February 22–24, 2010, s. 53–61.

2. Możliwości zastosowania tożsamości cyfrowej w poszczególnych obszarach.
3. Poziom zastosowania tożsamości cyfrowych w poszczególnych obszarach.

2.2.1. Obszary działalności człowieka wspomagane tożsamością cyfrową

Za punkt wyjścia do określenia obszarów wykorzystania tożsamości cyfrowych przyjęto raporty z badań bazujących na aktualnym wykorzystaniu nowoczesnych technologii przez Polaków. W raporcie „Korzystanie z mediów a podziały społeczne" sporządzonym w ramach projektu „*Poza stare i nowe media. Kompetencje komunikacyjne Polaków*", który poświęcono diagnozie kompetencji komunikacyjnych, ze szczególnym uwzględnieniem tych, które dotyczą korzystania z Internetu wyodrębniono 11 sfer, które są istotne dla Polaków[45]:

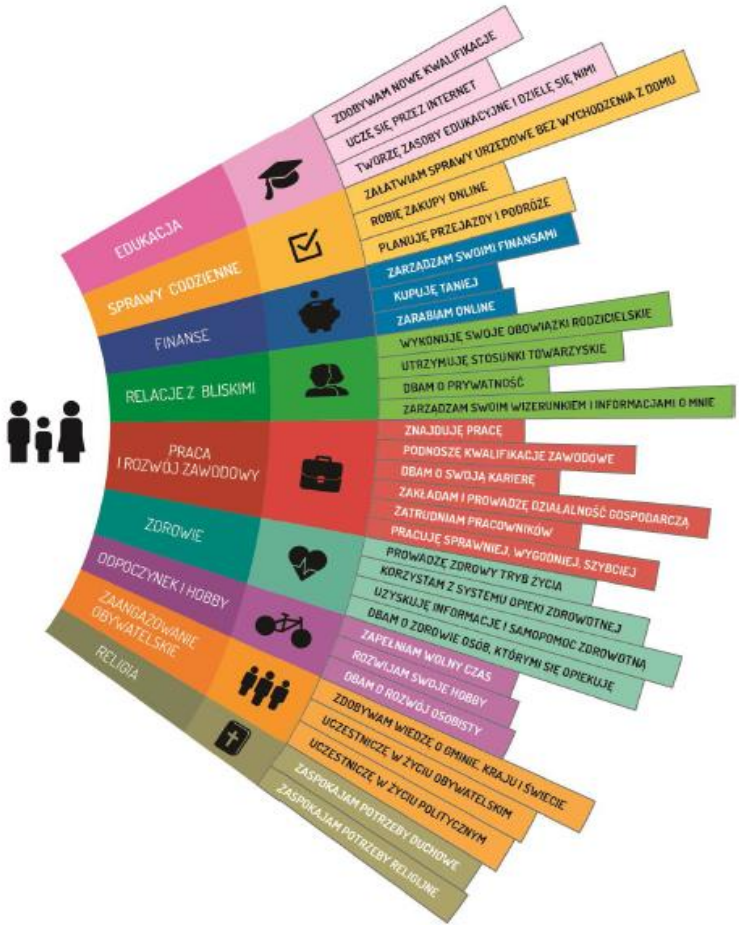
1. Rozwój zawodowy (związany z obecną pracą lub poszukiwanie nowej).
2. Relacje z bliskimi (rodziną, przyjaciółmi).
3. Życie towarzyskie (kontakty ze znajomymi).
4. Odpoczynek (w tym: nabieranie sił, relaks, oderwanie się od codziennych spraw, zabawa).
5. Realizacja zainteresowań (hobby).
6. Zdrowie (dbanie o kondycję i zdrowy styl życia, profilaktyka, wiedza o tym, jak sobie radzić w przypadku zachorowania).
7. Załatwianie codziennych spraw (m.in. obowiązki domowe, wizyty w urzędach).
8. Pieniądze (m.in. zarabianie, inwestowanie, oszczędzanie).
9. Refleksja nad sobą, własnym życiem lub przyszłością, kwestiami duchowymi lub religijnymi.
10. Wiedza o tym, co dzieje się w kraju i na świecie.
11. Działanie na rzecz innych (wolontariat, wspieranie lokalnej wspólnoty, zaangażowanie obywatelskie lub polityczne).

W raporcie „*Ramowy katalog kompetencji cyfrowych*" [46], te obszary stały się punktem wyjścia do określenia korzyści ze wspomagania się technologiami cyfrowymi, następnie do zidentyfikowania kompetencji cyfrowych koniecznych do osiągnięcia wspomnianych korzyści, a w efekcie, stworzenia ramowego

[45] Fliciak, M., Mazurek, P., Growiec, K. (2013), *Korzystanie z mediów a podziały społeczne. Kompetencje medialne Polaków w ujęciu relacyjnym*. Warszawa: Centrum Cyfrowe. s. 11–12, Online: http://ngoteka.pl/bitstream/handle/item/215/korzystanie%20.z%20mediow%20a%20podzialy%20spoleczne.pdf?sequence=3, dostęp: 2017.06.04.

[46] J. Jasiewicz, M. Filiciak, A. Mierzecka i in. (2014). *Ramowy katalog kompetencji cyfrowych*, Warszawa: Centrum Cyfrowe, s. 10–13. Online: https://cppc.gov.pl/wp-content/uploads/zal.-13-Ramowy_katalog_kompetencji_cyfrowych.pdf, dostęp: 2017.06.04.

katalogu funkcjonalnych kompetencji cyfrowych, który został przedstawiony na rysunku 2.2.



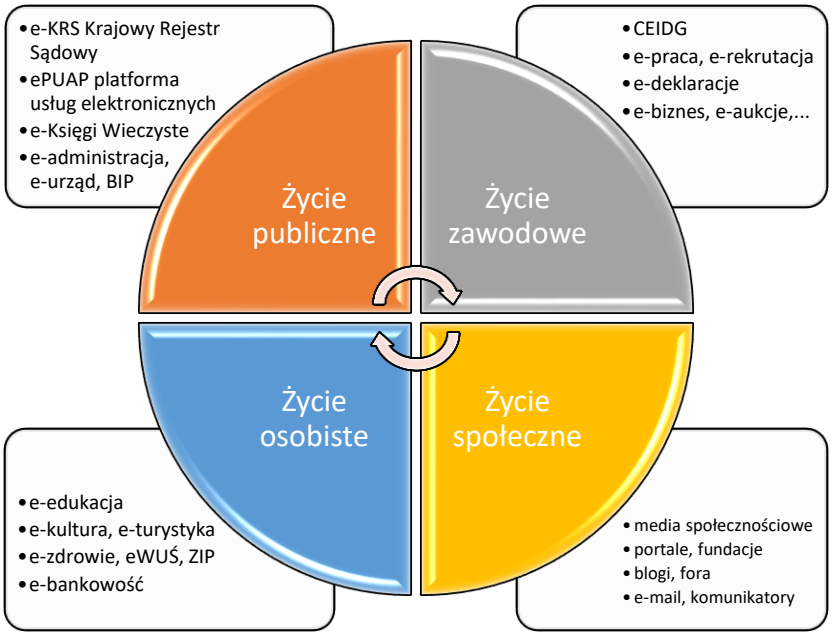
Rysunek 2.2. Ramowy katalog kompetencji
Źródło: Jasiewicz, J., Filiciak, M., Mierzecka, A. i in.(2014). Ramowy katalog kompetencji cyfrowych, Warszawa: *Centrum* Cyfrow, s. 13. Online: https://cppc.gov.pl/wp-content/uploads/zal.-13-Ramowy_katalog_kompetencji_cyfrowych.pdf.

Analiza zawartych w raporcie rozszerzonych opisów poszczególnych grup kompetencji funkcjonalnych (rysunek 2.3.) wskazuje, że korzystanie z tożsamości cyfrowej jest konieczne w ramach każdej z wymienionych umiejętności. Ponadto, istotne jest bezpieczeństwo wykorzystania technologii cyfrowych[47] obejmujące m.in. bezpieczeństwo komunikacji, pracy i transakcji.

[47] Jasiewicz, J. i in. (201). Ramowy katalog kompetencji cyfrowych. Warszawa: Centrum Cyfrowe, 68 s. Online: http://cppc.gov.pl/wp-content/uploads/zal.-13-Ramowy_katalog_kompetencji_cyfrowych.pdf, dostęp: 2017.06.04.

Inny raport, przygotowany przez Fundację ECCC w ramach projektu DIGCOMP, zawierający katalog kompetencji informatycznych i informacyjnych, wskazuje wprost na kompetencje związane z zarządzaniem tożsamością cyfrową rozumianym jako: „*umiejętność tworzenia, dostosowywania i zarządzania jedną lub wieloma tożsamościami cyfrowymi, umiejętność ochrony własnej reputacji w świecie wirtualnym, umiejętność zarządzania danymi zawartymi na jednym lub kilku kontach i/lub aplikacjach.*”[48]

Kolejny podział zaproponowano wychodząc od potrzeb jednostki funkcjonującej w konkretnym otoczeniu prawnym, społecznym i gospodarczym. Taka jednostka, posługująca się jedną lub wieloma tożsamościami cyfrowymi konstytuuje realno-wirtualny byt, który można nazwać e-obywatelem[49]. Na rysunku 2.3. przedstawiono główne aspekty jego działań wraz z przykładami.



Rysunek 2.3. Obszary życia e-Obywatela
Źródło: Miłosz, E. (2015). E-obywatel w społeczeństwie informacyjnym – możliwości, potrzeby, zagrożenia. W: Cichorzewska, M., Wit, B. Uwarunkowania prawne, informatyczne i społeczne e-obywatela w społeczeństwie informacyjnym, s. 16.

[48] Ferrari, A. (2013), tłum. Urban, K. (2016). *DIGCO MP Ramy odniesienia dla rozwoju i rozumienia kompetencji cyfrowych w Europie*, s. 9. Online: http://www.digcomp.pl/download/raport-eccc-digcomp-pl/?wpdmdl=396, dostęp: 2017.06.04.

[49] Chodacka, B., Miłosz, M. (2008). *E-obywatel – przezwyciężanie barier*. W: E-mentor nr 2 (24). Warszawa: Szkoła Główna Handlowa, s. 28.

Podsumowując, w oparciu o przedstawione zestawienia przyjęto, że tożsamość cyfrowa jest wykorzystywana praktycznie we wszystkich wspomaganych komputerowo aspektach działalności człowieka, czyli:

I. gospodarczym – do celów związanych z pełnieniem obowiązków w pracy zawodowej, przepływem pieniężnym, towarowym i usługowym,
II. społecznym – jako narzędzie do komunikacji z innymi osobami, tworzenie sieci powiązań,
III. obywatelskim – do kontaktu z jednostkami szeroko pojętej administracji państwowej,
IV. osobistym (rozumianym jako rozwój własny i rozrywka) – możliwość uczestniczenia w procesie tworzenia, udostępniania, wymiany czy korzystania z informacji.

2.2.2. Możliwości zastosowania tożsamości cyfrowej

Analizując zagadnienia charakterystyki i możliwości, tożsamość cyfrowa powinna być stosowana tam gdzie jest konieczności m.in.:

- potwierdzenia tożsamości stron procesu komunikacji lub transakcji,
- udzielania dostępu do zasobów wyłącznie osobom uprawnionym,
- udzielania dostępu tylko do wybranych zasobów,
- kontroli i ograniczenia możliwości działań użytkowników,
- przypisania działań do konkretnego użytkownika.

W niniejszej pracy wydzielono następujące obszary, w których tożsamość cyfrowa jest stosowana: biznes (stosowanie tożsamości cyfrowej na potrzeby realizacji zadań wynikających ze stosunku pracy), społeczeństwo (nawiązywanie i podtrzymywanie więzi międzyludzkich z wykorzystaniem nowych technologii), administracja publiczna (korzystanie z wirtualnych usług administracji publicznej) oraz życie prywatne (realizowanie działań w ramach hobby i spędzania wolnego czasu).

2.2.2.1. Biznes

W aspekcie działań człowieka związanych z działalnością gospodarczą przedsiębiorstw, które są wspomagane komputerowo z wykorzystaniem tożsamości cyfrowych, zarówno w celach pełnienia obowiązków pracy, jak i prywatnych, można wyróżnić przede wszystkim[50]:

- Stacjonarny dostęp do zasobów przedsiębiorstwa, a w szczególności: fizyczny lub software'owy dostęp do urządzeń firmowych (komputery, urządzenia wielofunkcyjne), szczególnie tych połączonych siecią

[50] *Digital identity management. Enabling Innovation and Trust in the Internet Economy* (2011). OECD, s. 11, 14. Online: http://www.oecd.org/sti/ieconomy/49338380.pdf, dostęp: 2017.06.04.

wewnętrzną; specjalistycznych programów i danych gromadzonych w bazach danych.

- Mobilny lub zdalny dostęp do zasobów przedsiębiorstwa, a w szczególności: dostęp z użyciem technologii mobilnych (np. smartfon), wykorzystanie technologii chmury (do np. przechowywania danych poza dyskami firmowymi), pracy zdalnej, szczególnie w grupie roboczej.
- Dokonywanie transakcji i rozliczeń szczególnie w e-commerce, czyli wykorzystanie profesjonalnych platform (np. Allegro, ePUAP), bankowości elektronicznej czy e-dokumentów, także w kontaktach z administracją państwową.
- Komunikację, zarówno w kontaktach między pracownikami, jak również z innymi interesariuszami z wykorzystaniem e-maila, strony firmowej (w tym w mediach społecznościowych), komunikatorów, profesjonalnych platform (np. GoldenLine).
- Zarządzanie i kontrolę procesów biznesowych, w szczególności w organizacjach z dużym stopniem wirtualizacji i z wykorzystaniem Internetu Rzeczy (*Internet of Things*, IoT), zjawiska powszechności użycia „inteligentnych" urządzeń[51], które, jak się przewiduje, spowoduje głębokie zmiany procesów gospodarczych[52].
- Tworzenie, wyszukiwanie, gromadzenie i przetwarzanie informacji dotyczących np. warunków konkurowania, poszukiwania możliwości biznesowych czy innowacji.
- Realizacją wspólnych zamierzeń przez grupę przedsiębiorstw.

[51] Wielki, J. (2012). *Internet rzeczy i jego wpływ na modele biznesowe współczesnych organizacji gospodarczych*. Monografie i Opracowania Uniwersytetu Ekonomicznego we Wrocławiu, Nr 211, s. 208–219.

[52] Wielki, J. (2016). *Analiza szans, możliwości i wyzwań związanych z wykorzystaniem Internetu Rzeczy przez współczesne organizacje gospodarcze*. Przedsiębiorczość i Zarządzanie, Tom XVII, Zeszyt 11, Część I, s. 127–140.

Raport „Katalog kompetencji cyfrowych małych firm” zawiera funkcjonalne obszary wspomagane komputerowo[53] (rysunek 2.4.).

Rysunek 2.4. Obszary wspomagane komputerowo w małych przedsiębiorstwach
Źródło: Buchner, A., Zaniewska, K. (2016). Katalog kompetencji cyfrowych małych firm. Warszawa: Centrum Cyfrowe Projekt Polska:, s. 16. Online: https://centrumcyfrowe.pl/wp-content/uploads/2016/03/IR-katalog-kompetencji.pdf.

[53] Buchner, A., Zaniewska, K. (2016). *Katalog kompetencji cyfrowych małych firm.* Warszawa: Centrum Cyfrowe Projekt Polska, s. 16. Online: https://centrumcyfrowe.pl /wp-content/uploads/2016/03/IR-katalog-kompetencji.pdf, dostęp: 2017.06.04.

Możliwość wykorzystania tożsamości cyfrowych do komputerowego wsparcia obszarów funkcjonalnych przedstawiono w tabeli 2.4.

Tabela 2.4. Analiza użyteczności tożsamości cyfrowej w obszarach funkcjonalnych przedsiębiorstwa

Obszar funkcjonalny przedsiębiorstwa	**Obszar zastosowania tożsamości cyfrowej**					
	Dostęp do zasobów systemów informatycznych	Transakcje, rozliczenia	Komunikacja	Zarządzanie i kontrola procesów biznesowych	Tworzenie, wyszukiwanie, gromadzenie i przetwarzanie informacji	Współpraca między przedsiębiorstwami
Sprzedaż	+	+	+	+	+	+
Komunikacja i promocja	+		+	+	+	+
Klienci	+		+	+	+	+
Produkt lub usługa	+		+	+	+	+
Rynek i konkurencja	+		+		+	+
Prowadzenie firmy	+	+	+	+	+	+

Źródło: opracowanie własne z wykorzystaniem Buchner, A., Zaniewska, K. (2016). Katalog kompetencji cyfrowych małych firm. Warszawa: Centrum Cyfrowe Projekt Polska:, s. 16. Online: https://centrumcyfrowe.pl/wp-content/uploads/2016/03/IR-katalog-kompetencji.pdf.

Jerzy Kisielnicki wyróżnia obszary, które wymagają wsparcia narzędziami ICT[54]:

- monitoring (narzędzia BI),
- współpraca, gromadzenie i przekazywanie wiedzy w realizacji zadań (BigData, cloud computing),
- wspomaganie rozwiązywania sytuacji problemowych (system wieloagentowy, sieć semantyczna),
- tworzenie elastycznych, zwinnych struktur organizacyjnych (Internet i narzędzia do budowy organizacji wirtualnych).

Obecnie jednym z krytycznych elementów e-gospodarki i wykorzystania systemów informatycznych do wsparcia procesów biznesowych jest kwestia zapewnienia bezpieczeństwa. Drugim, intensywnie badanym elementem jest rozbudowa dostępnych dla przedsiębiorcy funkcjonalności oraz technologii.

[54] Kisielnicki, J. (2015) *Technologia informacyjna jako narzędzie wspomagania systemu zarządzania – analiza trendów*. Problemy Zarządzania, Vol. 13, Nr 2 (52), T. 1, s. 13–23.

2.2.2.2. Społeczeństwo

W aspekcie relacji międzyludzkich, Internet może być dodatkowym, dwukierunkowym kanałem komunikacyjnym[55] lub substytutem relacji realizowanej twarzą w twarz (*Face to Face*) z drugą osobą. W tym kontekście wykorzystanie tożsamości cyfrowej jest szczególnie ważne w następujących obszarach[56]:

- komunikacja z wykorzystaniem narzędzi pojedynczych, dedykowanych (np. Skype) lub zintegrowanych tj. oferujących rożne funkcjonalności (np. konto Google, Facebook);
- tworzenie i wykorzystanie treści kierowanych do innych osób przy pomocy mediów społecznościowych (np. Facebook, Tweeter), blogów, forów itp.;
- tworzenie sieci powiązań osób lub organizacji (np. serwis Goldenline);
- uczestnictwo i współpraca w ramach grup kontaktujących się za pomocą Internetu np. przygotowanie i koordynacja Arabskiej Wiosny w 2001 r.

Komunikacja drogą internetową dała podstawę do stworzenia fenomenu zwanego społecznościami wirtualnymi. Stanowią one świat równoległy do rzeczywistego, w którym tożsamość cyfrowa staje się nie tyle dyskretnym narzędziem komunikacji czy dostępu do zasobów, ale pełni rolę pierwszoplanową i staje się odpowiednikiem osoby ludzkiej lub organizacji występującej w świecie realnym. W społecznościach wirtualnych tożsamości są świadomie kreowane w celu pozyskania jak najszerszego audytorium. W ramach powstawania, rozwoju i transformacji społeczności wirtualnych pojawiły się m.in.:

- osobowości internetowe, które silnie oddziałują na osoby śledzące ich dokonania (celebryci nowej kategorii)[57],

---

[55] Szyjewski, G., Niemcewicz, P. (2016). *Zdalna realizacja usług w Internecie z uwzględnieniem profilu użytkownika*. Studia Informatica Pomerania, Nr 3 (41), s. 79–89.

[56] *Digital identity management. Enabling Innovation and Trust in the Internet Economy* (2011). OECD, s. 14. Online: http://www.oecd.org/sti/ieconomy/49338380.pdf, dostęp: 2017.06.04.

[57] Bień, A. (2016). *Jak zmieniły się media społecznościowe na przestrzeni 5 lat?* Online: http://socialpress.pl/2016/03/jak-zmienily-sie-media-spolecznosciowe-na-przestrzeni-5-lat/, dostęp: 2017.06.04. oraz Dederko, J. (2015). *Internet należy do Maffashion, Jemerced i Make Life Easier.* Online: http://socialpress.pl/2015/10/internet-nalezy-do-maffashion-jemerced-i-make-life-easier/, dostęp: 2017.06.04. oraz Dederko, J. (2015). *O tym, jak ogromny wpływ na decyzje konsumenckie mają youtuberzy.* Online: http://socialpress.pl/2015/11/o-tym-jak-ogromny-wplyw-na-decyzje-konsumenckie-maja-youtuberzy/, dostęp: 2017.06.04. oraz Bień, A. (2016). *Raport: Internet najmocniej wpływa na sprzedaż kosmetyków.* Online: http://socialpress.pl/2016/07/raport-internet-najmocniej-wplywa-na-to-ktore-kosmetyki-kupic-warto-a-ktore-nie/, dostęp: 2017.06.04

- łatwa popularyzacja niszowych (tj. mało obecnych w mediach tradycyjnych) produktów lub usług wśród szerszego grona odbiorców,
- pozyskiwanie pomysłów od internautów przez organizacje,
- nowe sposoby reklamowania się, takie jak: sponsorowane posty osobowości internetowych, *content marketing*[58], lokowanie produktów na Youtube[59] oraz korzystanie z reklamy profilowanej (tj. dostosowanej do profilu użytkownika, definiowanego na podstawie jego tożsamości cyfrowej)[60].

Badania społeczności wirtualnych (*Virtual Community*, VC) dotyczą[61]:

- tworzenia i ewolucji VC, czyli: skupiania ludzi i zawiązywania się społeczności, budowania zaufania, źródeł motywacji dołączenia do społeczności wirtualnych oraz ich ewolucji;
- dynamiki VC, a w szczególności roli wzmacniania zaufania i personalizacji VC, formowania relacji oraz identyfikacji tych cech, które umożliwiają symulację działań w ramach VC (np. w ramach uczenia się i innowacji) oraz wykorzystywanych narzędzi;
- stosowania VC, tj. czerpania korzyści ze społeczności przez jej członków, potencjału VC w różnych obszarach gospodarki (np. ubezpieczenia, opieka zdrowotna, edukacja, przemysł turystyczny), wykorzystania VC do wzmocnienia zaufania w ramach e-commerce i m-commerce oraz do rozwoju produktu czy działań marketingowych.

Przedmiotem większości z tych badań są zachowania użytkowników odczytywane za pomocą ich tożsamości cyfrowych.

[58] Dederko, J. (2015). *W jakim kierunku zmierza polski content marketing?* Online: http://socialpress.pl/2015/11/w-jakim-kierunku-zmierza-polski-content-marketing/, dostęp: 2017.06.04.

[59] Dederko, J. (2015). *Czy warto lokować produkty na YouTube? Mamy raport!* Online: http://socialpress.pl/2015/10/czy-warto-lokowac-produkty-na-youtube-mamy-raport/, dostęp: 2017.06.04.

[60] Bień, A. (2016). *Branża e-commerce: zobacz, jaki budżet wydaje na posty sponsorowane na Facebooku*. Online: http://socialpress.pl/2016/05/branza-e-commerce-zobacz-jaki-budzet-wydaje-na-posty-sponsorowane-na-facebooku/, dostęp: 2017.06.04.

[61] Leimeister, J.M., Balaji, R. (2014). *Virtual Communities: 2014, Vol. 20. Advances in Management Information Systems*. Armonk: M.E. Sharpe, oraz Gupta, S., Kim, H.-W. (2004). *Virtual Community: Concepts, Implications, and Future Research Directions*. Proceedings of the Tenth Americas Conference on Information Systems, NewYork, August 2004, s. 26–85.

2.2.2.3. Administracja publiczna

W aspekcie kontaktu z administracją publiczną widoczne jest stałe zwiększanie się możliwości partycypacji w życiu obywatelskim i dostępu do usług zapewnianych przez państwo za pośrednictwem Internetu. E-administracja, czyli elektroniczna administracja „*opiera się na wykorzystaniu technologii informatycznych i telekomunikacyjnych w administracji publicznej. W ramach elektronicznej administracji zakłada się zmiany oraz usprawnienia organizacyjne, szeroką modernizację oraz optymalizację procesów administracyjnych pod kątem efektywności.*"[62]

Dostrzeżono szereg istotnych korzyści związanych z wirtualizacją usług administracji publicznej, jakimi w zamierzeniu miały być: zwiększenie konkurencyjności gospodarki, obniżenie kosztów i zwiększenie efektywności administracji, zwiększenie społecznego i intelektualnego kapitału obywateli[63], a także zwiększenia dostępności usług dla osób wykluczonych[64]. Miało to być osiągnięte poprzez[65] poprawienie jakości, szybkości, efektywności i dostępności usług (rozumianej jako obecność usługi świadczonej w formie elektronicznej oraz możliwość skorzystania z niej w każdym momencie czasu), które przekładać się miały na większe zaangażowanie obywateli, lepsze funkcjonowanie mechanizmów państwa i budowę społeczeństwa informacyjnego[66]. Dzięki e-administracji procedury zostałyby uproszczone, biurokracja zredukowana i odciążona (zmniejszone koszty działalności), a klienci poświęcaliby mniej czasu na załatwianie spraw urzędowych i stanie w kolejkach[67]. Na duże znaczenie

[62] *Elektroniczna administracja*. Online: http://www.eadministracja.pl/elektroniczna-administracja, dostęp: 2017.06.04.

[63] *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013* (2008). Ministerstwo Spraw Wewnętrznych i Administracji, s. 1–4. Online: http://www.umwd.dolnyslask.pl/fileadmin/user_upload/spoleczenstwo_informacyjne/dokumenty/Streszczenie.pdf, dostęp: 2017.06.04.

[64] Wolniak, R. (2015). *Ocena funkcjonowania e-administracji w Dąbrowie Górniczej z punktu widzenia osób niepełnosprawnych.* W: Zeszyty naukowe Politechniki Śląskiej Nr kol. 1940, s. 369–383.

[65] Górczyńska, A. *Wpływ Programu Operacyjnego Polska Cyfrowa (POPC) na rozwój innowacyjnej e-administracji w Polsc*e. W: Nowak, P.A. red. INNOWACJE 2015. Rozwój społeczeństwa informacyjnego w nowej perspektywie finansowej. Łódź: Urząd Marszałkowski Województwa Łódzkiego, s. 6–20.

[66] Dziedzic, K. (2013). *E-administracja w Polsce na tle państw w Unii Europejskiej*. W: Laskowski, P. red. Prace Naukowe Wałbrzyskiej Szkoły Zarządzania i Przedsiębiorczości, T. 24, Samorząd terytorialny a polityka lokalna, s. 7–16.

[67] Wolniak, R. (2015). *Ocena funkcjonowania e-administracji w Dąbrowie Górniczej z punktu widzenia osób niepełnosprawnych.* W: Zeszyty naukowe Politechniki Śląskiej nr kol. 1940, s. 377.

cyfryzacji usług administracyjnych wskazuje objęcie tego obszaru wsparciem w ramach Europejskiej Agendy Cyfrowej[68].

E-administracja czyli wirtualny kontakt obywatela z podmiotami publicznymi obejmuje lub może wspierać następujące obszary[69]:

- Udostępnianie informacji, w tym szczególnie: informacji dotyczącej urzędu, szczegółowych opisów procedur administracyjnych (karta usługi)[70], formularzy do samodzielnego wydruku w domu petenta.
- Gromadzenie, wyszukiwanie i umożliwienie wglądu w informacje petentowi lub zainteresowanej jednostce w ramach norm prawnych np. dane dotyczące ubezpieczenia zdrowotnego pacjenta na potrzeby rejestracji w przychodni lub przedstawianie ofert pracy przez urząd pracy.
- Przeprowadzanie procesu administracyjnego, dotyczącego danej sprawy drogą online – od przesłania plików po otrzymanie wnioskowanego dokumentu lub potwierdzenia (w formie elektronicznej lub drogą pocztową) np. wydanie dowodu tożsamości lub przyznanie dostępu do zasobów biblioteki miejskiej.
- Zarządzanie środkami pochodzącymi od obywateli (z podatków).
- Obsługa transakcji finansowych przez Internet.
- Komunikacja w relacji: urząd – petent, urząd – organizacja, ale także urząd – urząd, czyli m.in. współpraca z innymi urzędami tak, by zminimalizować dublowanie się operacji wykonywanych przez petenta np. przesyłanie jednego zaświadczenia do rożnych oddziałów urzędów skarbowych. Możliwa jest także komunikacja z administracją innego państwa.
- Kontrola spełniania obowiązków nakładanych na obywatela przez przepisy prawa np. realizacja obowiązku szkolnego.
- Wirtualizację dokumentacji urzędowej (np. e-recepty).
- Gromadzenie danych statystycznych.

---

[68] Grodzka, D. (2009). E-administracja w Polsce. W: Grodzka, D. red. Społeczeństwo informacyjne. Studia BAS, 2009, Nr 3 (19), s. 57–82, oraz Lörincz, B., i inni. (2010). *Digitizing Public Services In Europe: Putting ambition into action*, 9th Benchmark Measurement, s. 5. Online: http://ec.europa.eu/newsroom/document.cfm?action =display&doc_id=747, dostęp: 2017.06.04.

[69] Olszak, C., M.; Ziemba, E. (2011). *The stage of e-Government maturity in a Polish region – Silesia*. Journal of Economics & Management, Vol. 7, s. 87–103, oraz Chmielarz W. (2008). *Stadium rozwoju systemów e-Administracji w Polsce*. W: Gołuchowski, J., Frączkiewicz-Wronka, A. red. Technologie wiedzy w zarządzaniu publicznym, Katowice: Wydawnictwo Akademii Ekonomicznej w Katowicach, 115–127.

[70] Ziemba, E., Papaj, T., Będkowski, J. (2013). *Egzemplifikacja e-government w Polsce – analiza porównawcza SEKAP i ePUAP*. W: Roczniki Kolegium Analiz Ekonomicznych Nr 29/2013. Warszawa: Szkoła Główna Handlowa, s. 434.

- Realizowanie demokracji bezpośredniej drogą elektroniczną w formie zbierania opinii, głosowania i umożliwienia udziału obywatela w debacie np. dotyczącej rozdziału środków w ramach budżetów obywatelskich. Warto dodać, że przyszłościowym zastosowaniem tej funkcjonalności może być udział obywatela drogą elektroniczną w referendach ogólnokrajowych i lokalnych (np. odwołanie włodarza), wyborach (prezydenckich, parlamentarnych lub samorządowych) i innych działaniach wymagających legitymizacji społeczeństwa.

Określono pięć poziomów dojrzałości e-administracji[71]:

Poziom 1. Informacja online (poziom pierwszy), czyli umieszczone na stronie internetowej informacje o danym urzędzie i świadczonych przez niego usługach.

Poziom 2. Jednokierunkowa interakcja (poziom drugi), czyli, dodatkowo, możliwość pobrania formularzy ze strony urzędu.

Poziom 3. Dwukierunkowa interakcja (poziom trzeci), która oprócz wyszukania informacji i pobrania formularzy umożliwia ich odesłanie drogą elektroniczną.

Poziom 4. Transakcja (poziom czwarty), czyli możliwość załatwienia sprawy urzędowej w pełni przez Internet, od pobrania formularzy, przez uregulowanie płatności po uzyskanie pliku z urzędowym dokumentem lub potwierdzeniem odbioru

Poziom 5. Personalizacja (piąty poziom), czyli rozszerzenie usługi realizowanej w pełni przez Internet o personalizację obsługi.

Poziomy 1 i 2 wymagają zaufania obywatela co do prawdziwości zamieszczonych na stronie urzędu danych, kolejne poziomy wymagają pewności co do tożsamości obywatela, urzędnika i urzędu.

Zaufanie co do tożsamości osób biorących udział w komunikacji urzędowej drogą elektroniczną poprzez specjalne platformy np. ePUAP (*Elektroniczna Platforma Usług Administracji Publicznej)* czy SEKAP (*Electronic Communication System for Public Administration*)[72], zapewnia tożsamość cyfrowa utworzoną specjalnie w tym celu. Jest to tzw. profil zaufany, który tworzony jest specjalnie dla konkretnej osoby fizycznej lub organizacji (firmy, instytucji lub

[71] Olszak, C., Ziemba, E. (2011). *Rozwój e-administracji. Rodzaje i poziomy dojrzałości e-usług publicznych w regionie śląskim*. W: Babis, H., Czapiewski, R. Drogi dochodzenia do społeczeństwa informacyjnego. Stan obecny, perspektywy rozwoju i ograniczenia. Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 651, Ekonomiczne Problemy Usług, Nr 68, T. 2, s. 250–266, s. 256.

[72] Olszak, C., M.; Ziemba, E. (2011). *The stage of e-Government maturity in a Polish region – Silesia*. Journal of Economics & Management, Vol. 7, s. 87–103.

podmiotu publicznego). Elementami tożsamości cyfrowej tworzonej na platformie są[73]:

- identyfikator profilu (login) – unikalna w skali systemu nazwa użytkownika wybierana przez osobę zakładającą konto,
- atrybuty – m.in. imię, nazwisko, e-mail, dane teleadresowe, numer PESEL / REGON,
- afiliacje – dane organizacji,
- poświadczenia – hasło lub certyfikat kwalifikowany PKT,
- uprawnienia – możliwości działań przypisane do danych zasobów.

Główne działania związane z e-administracją nakierowane są na rozszerzenie zakresu dostępnych usług oraz osiąganie kolejnych poziomów dojrzałości. Dostosowanie tożsamości cyfrowych będzie odgrywało kluczową rolę w tym procesie. Dostęp do wrażliwych danych obywatela (np. historia medyczna, rozliczenia z urzędem podatkowym itp.) powoduje konieczność zwiększenia ochrony tożsamości cyfrowej, co może oznaczać konieczność zaadaptowania nowych narzędzi uwierzytelnienia pojawiających się wraz z rozwojem technologii.

2.2.2.4. Życie prywatne

W aspekcie wykorzystania Internetu do celów prywatnych, tożsamość cyfrowa może służyć m.in. w następujących celach:

- personalizacja treści[74];
- uzyskanie dostępu do treści umieszczonych na płatnych serwisach lub takich, które wymagają rejestracji w celu uzyskania dostępu do oferowanych zasobów (np. YouTube, Netflix, Spotify, Amazon, iTunes)[75]. W szczególności dotyczy to produktów, które można w prosty sposób zdigitalizować[76] (np. muzyki, książek) i niektórych usług (np. porad dietetycznych czy planów treningu);
- korzystanie z e-learningu;
- integracja narzędzi i serwisów np. konto e-mail, notatnik, kalendarz itp.;

[73] Elektroniczna Platforma Usług Administracji Publicznej. Instrukcja zakładania konta. Wersja 7.1. Ministerstwo Spraw Wewnętrznych i Administracji, Online: http://bip.zielonagora.pl/system/obj/25161_Instrukcja_zakladania_konta_71.pdf, dostęp: 2017.06.04.

[74] Chmielarz, W. (2015). *Determinanty rozwoju serwisów dystrybucji treści komercyjnych w Polsce*. Problemy Zarządzania, Vol. 13, Nr 2 (52), T. 1, s.52.

[75] Tamże, s. 57.

[76] Szyjewski, G., Niemcewicz, P. (2016). *Zdalna realizacja usług w Internecie z uwzględnieniem profilu użytkownika*. Studia Informatica Pomerania, nr 3 (41), s. 79–89.

- transakcje online i wsparcie komunikacji (*Customer to Customer*, C2C; *Customer to Business*, C2B; *Business to Customer*, B2C) oraz realizacji usług niewirtualnych np. rezerwacja i opłacenie biletu kinowego;[77]
- tworzenie i monetyzacja treści[78];
- oznaczanie treści w serwisach internetowych (np. like), uzyskiwanie informacji o nowych zasobach (subskrypcje).
- Korzystanie z treści dedykowanych np. systemu informacji geograficznej (*Geographic Information System*, GIS) w celach planowania wyjazdów turystycznych[79].

Tożsamością wykorzystywaną w celu personalizacji treści jest tożsamość współtworzona przez użytkownika np. konto google (*ourdentity*) oraz ta, którą tworzą wyszukiwarki na podstawie zachowań użytkownika identyfikowanego przez np. IP (*theirdentity*). Analiza zachowań użytkownika w przeszłości staje się podstawą do określenia jego preferencji i dopasowania do nich treści np. wyszukiwania lub reklam.

Tożsamość cyfrowa typu *ourdentity* oraz *theirdentity* w kontekście korzystania z serwisów, a w szczególności z mediów społecznościowych jest dynamicznie rozwijającym się obszarem badawczym szczególnie w kontekście analizy zjawisk takich jak kradzieże tożsamości, kształtowania się i wpływu na rzeczywistość więzi wirtualnych czy nowy sposób stosowania marketingu.

2.2.3. Poziom zastosowania tożsamości cyfrowych w praktyce

Czynniki wpływające na zastosowanie tożsamości cyfrowych pogrupowano na potrzeby, motywację do stosowania oraz koszty.

2.2.3.1. Poziom wykorzystania tożsamości cyfrowych w biznesie

W przypadku przedsiębiorstw widoczne jest zazwyczaj praktyczne podejście, w którym punktem wyjścia są realne potrzeby związane z zakresem i skalą operowania przedsiębiorstwa (potencjalne korzyści) oraz sprzętem i oprogramowaniem koniecznym do prowadzenia działalności (koszty). To, na ile tożsamości cyfrowe są stosowane zależy m.in. od[80]:

---

[77] Tamże.

[78] Pal, P. (2010). *Monetyzacja e-obecności*. Marketing w praktyce, Nr 4, s. 18–20.

[79] Chmielarz, W., Szumski, O. (2016). *Technologie mobilne geograficznych systemów informatycznych (GIS) w turystyce.* W: Chmielarz, W. red. Mobilne aspekty technologii informacyjnych, Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, s. 65–80.

[80] Stevens, T. i inni. (2010). *Stan rynku tożsamości elektronicznej. Technologie, infrastruktura, usługi i polityki*. Ipts, Komisja Europejska, Online: http://spiner.org.pl/biblioteka-erozwoju.html?download=135%3Asytuacja-rynku-tozsamosci-elektronicznej, dostęp: 2017.06.04.

- Potrzeby i gotowości do stosowania tożsamości cyfrowych, a w tym postrzegania korzyści mierzalnych i niemierzalnych, wdrożenia procedur przygotowujących przedsiębiorstwo na adaptację konkretnych rozwiązań, ale także zaufania[81].
- Motywacji do korzystania z tożsamości cyfrowych, a w tym spodziewanych oszczędności kosztów, zysków (obliczanych np. z wykorzystaniem metodyki ROI jako suma zmiany przychodów, kosztów i wydajności oraz korzyści niemierzalnych, pomniejszona o koszty nabycia systemu informatycznego[82]), konieczności (np. regulacje prawne, wymogi biznesowe lub organizacyjne).
- Usunięcia barier, a w tym: akceptowalnego kosztu wdrożenia i stosowania, dojrzałości infrastruktury i technologii, łatwości, zaufania i akceptacji użycia tożsamości cyfrowych.

Nowe technologie zmieniają sposób działania przedsiębiorstw lub wprowadzają nowe modele prowadzenia biznesu (telepraca, przedsiębiorstwa internetowe i wirtualne[83], handel danymi).

Jednym z warunków świadczenia telepracy jest posiadanie silnie chronionej (po stronie zarówno pracodawcy, jak i pracownika) tożsamości cyfrowej z prawidłowo przydzielonym dostępem do niezbędnych zasobów.

W przypadku przedsiębiorstw wirtualnych, rozumianych jako przedsiębiorstwo zdematerializowane, o wysokim stopniu elastyczności, pozwalającej na wykorzystanie nadarzających się szans, oparte o kluczowe kompetencje i wiedzę[84] oraz w przypadku przedsiębiorstw internetowych, czyli korzystających z Internetu jako kanału komunikacyjnego, tożsamość cyfrowa jego pracowników jest niezastąpionym i krytycznym elementem prowadzenia tego typu działalności.

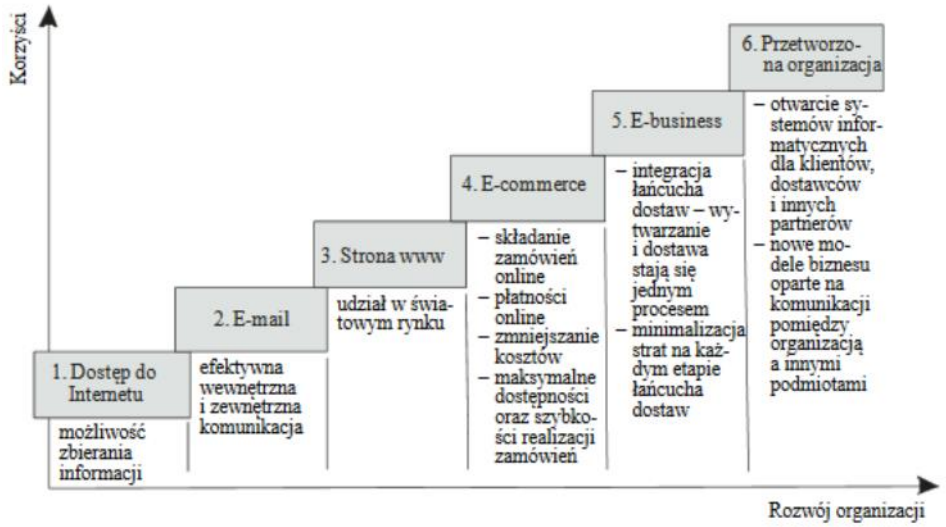
Polskie przedsiębiorstwa, w zależności od potrzeb, posiadanych funduszy oraz wizji, do której dąży zarząd, mogą realizować procesy biznesowe w sposób mniej lub bardziej zwirtualizowany (rysunek 2.5.).

[81] Zarańska, K. (2016). *Determinanty korzystania z mobilnego handlu elektronicznego*. W: Chmielarz, W. red., Mobilne aspekty technologii informacyjnych, Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, s. 34.

[82] Szplit, M. (2012). *Ekonomiczne Aspekty Działania Systemów Informatycznych w Przedsiębiorstwach.* Gospodarka elektroniczna, wyzwania rozwojowe, tom II, Uniwersytet Szczeciński. Zeszyty Naukowe nr 703. Ekonomiczne Problemy Usług nr 88. Szczecin. s. 101–108.

[83] Sobińska, M. (2014). *Innowacyjne modele biznesu dla IT – wyzwania i perspektywy rozwoju.* W: Informatyka ekonomiczna. Business Informatics. 1(31)/2014. Wrocław: Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, s. 128.

[84] Szpringer, W. (2008). *Wpływ wirtualizacji przedsiębiorstw na modele e-biznesu. Ujęcie instytucjonalne*. Warszawa: Oficyna Wydawnicza SGH, s. 31.



Rysunek 2.5. Adaptacja technologii informatycznych i komunikacyjnych przez przedsiębiorstwo Źródło: Wallis, A. (2011). Wpływ technologii informacyjnych na przedsiębiorczość. Przedsiębiorczość Szansą Rozwoju Regionu, Tom II, Kształtowanie Przedsiębiorczości, Uniwersytet Szczeciński. Zeszyty Naukowe Nr 725. Ekonomiczne Problemy Usług Nr 98, s. 384.

2.2.3.2. Wykorzystanie tożsamości cyfrowych w aspekcie więzi międzyludzkich

Poziom wykorzystania tożsamości cyfrowych w aspekcie społecznym uzależniony jest od szeregu czynników takich jak:

1. Dostępność i atrakcyjność oferowanych usług (np. serwisy społecznościowe), rozumianych jako odpowiedź na zapotrzebowanie (nowy sposób realizowania relacji międzyludzkich za pomocą Internetu), ale i nowa jakość utrzymywania relacji (np. zwiększona szybkość i dostępność kontaktu) realizowana z użyciem nowych narzędzi (smartfony).
2. Korzyści z przynależności do wirtualnych społeczności, gdzie obecność w np. mediach społecznościowych oddziałuje na jakość realnego życia jednostki (a brak powoduje konkretne, negatywne skutki).
3. Techniczne możliwości uzyskania dostępu i koszt korzystania z usług, czyli posiadanie połączenia z Internetem oraz opłaty związane z transmisją danych.

W ostatnich latach wykorzystanie serwisów społecznościowych gwałtownie wzrosło. Wśród przyczyn należy wymienić znaczną dojrzałość oferty w każdym aspekcie procesu komunikacji międzyludzkiej, realizowanej za pomocą narzędzi ICT tj.:

- bogata oferta samych usług (np. mnogość zróżnicowanych serwisów społecznościowych),
- duża dostępność Internetu szerokopasmowego, LTE i jego niski koszt,

- bogata oferta narzędzi, za pomocą których realizowany jest kontakt z drugą osobą i coraz większa podaż usług komplementarnych, podnoszących atrakcyjność stosowania tych urządzeń lub aplikacji.

Równie istotny jest czynnik ludzki, czyli dostosowanie sposobu realizowania relacji międzyludzkich do nowego sposobu funkcjonowania społeczeństwa (większe tempo życia, konieczność lepszego, wydajniejszego komunikowania się innymi by lepiej gospodarować coraz bardziej ograniczonym czasem). Ponadto, pojawiła się istniejąca w świecie wirtualnym tożsamość cyfrowa, jako wartość sama w sobie, kreowana niejako równolegle z tożsamością osobową na poziomie świadomym (np. ogół treści publikowanych na Facebooku) lub mniej świadomym (profilowanie użytkownika). Pojawiła się też presja na korzystanie z tego sposobu kontaktu oraz swoiste wykluczeni cyfrowe osób, które nie posiadają np. konta na serwisie społecznościowym.

Na początku 2016 r. prawie 26 mln Polaków korzystało z Internetu, a 14 mln z mediów społecznościowych[85]. W roku 2020 użytkownikami Internetu było już prawie 31 mln Polaków (wzrost o 19% przy mniejszej populacji), a z mediów społecznościowych 19 mln (wzrost o połowę)[86]. Przytoczone dane z jednej strony wskazują na to, że stosowanie tożsamości cyfrowych jest powszechnie wykorzystywane w kształtowaniu relacji międzyludzkich, a z drugiej, że to znaczenie ma trend wzrostowy.

Z podażowego punktu widzenia, o rozwoju serwisów umożliwiających kontakty z innymi osobami decyduje opłacalność tego internetowego modelu biznesowego, na którą składa się m.in. rozwój technik analitycznych stosowanych do big data, a co za tym idzie, duży potencjał reklamowy i popyt na usługi marketingowe wykorzystujące profilowanie. Szacuje się, że nakłady na reklamę w mediach społecznościowych stanowią ok. 10% wszystkich wydatków na reklamę w Internecie[87].

2.2.3.3. Dostępność i wykorzystanie usług oferowanych przez e-administrację z wykorzystaniem tożsamości cyfrowych

W Polsce wdrożono szereg usług oferowanych przez administrację publiczną. Są one realizowane w ramach różnych systemów, mniej lub bardziej ze sobą zintegrowanych, o różnych poziomach dojrzałości. Z punktu widzenia klienta, dostęp do nich może odbywać się przez platformę dostępu (np. ePUAP), z wyko-

[85] Majchrzyk, Ł. (2016). *Mobile i digital w Polsce i na świecie w 2016 r.* Online: https://mobirank.pl/2016/01/27/mobile-digital-w-polsce-na-swiecie-2016/, 2016.01.27.

[86] *Digital, mobile i social media w Polsce w styczniu 2020 roku*. Online: https://mobirank.pl/2020/02/23/digital-mobile-i-social-media-w-polsce-w-styczniu-2020-roku/, dostęp: 2020.12.14.

[87] *Raport Interaktywnie.com "Media społecznościowe 2016".* (2016). s. 10. Online: http://interaktywnie.com/biznes/artykuly/raporty-interaktywnie-com/raport-interaktywnie-com-media-spolecznosciowe-2016-253577, dostęp: 2017.06.04.

rzystaniem strony internetowej konkretnego urzędu (np. Urzędu Miasta) lub z wykorzystaniem osób trzecich (np. fakt ubezpieczenia może być sprawdzony przez osobę rejestrującą do lekarza).

Zintegrowaną platformą dostępu do poszczególnych usług jest platforma ePUAP, czyli elektroniczna Platforma Usług Administracji Publicznej. Jej założenia opracowano wstępnie w 2002 r. (w ramach projektu „*Wrota Polski"*), a przygotowano w latach 2005–2008 (w ramach projektu „Budowa elektronicznej Platformy Usług Administracji Publicznej") i rozszerzono o dalsze usługi w kolejnych latach (m.in. w 2008–2013 w ramach projektu *ePUAP2*)[88]. Równolegle budowane były lokalne platformy np. SEKAP (woj. Śląskie). Konkretne usługi, oferowane online pogrupowane są w działy takie jak: rodzina 500+ (przyjmowanie wniosków), prawy obywatelskie (np. rejestracja urodzeń), praca i zatrudnienie (np. nabór pracownika), przedsiębiorczość (np. wpis do rejestru przedsiębiorców), edukacja (np. przyjęcie na studia) itp. Niestety, obecnie nakłady na e-administrację są niewspółmiernie duże w stosunku do osiąganych efektów[89].

Problemy z tworzeniem e-administracji dotyczą m.in.:[90]

- braku interoperacyjności między usługami i urzędami,
- niewystarczającej infrastruktury internetowej w Polsce,
- niskiego stopnia wiedzy o świadczonych usługach,
- skomplikowania procedur i ich niespójności.

Co ciekawe, według Najwyższej Izby Kontroli, jedne z nieprawidłowości dotyczące zarządzania bezpieczeństwem informacji w kontrolowanych w 2015 r. urzędach dotyczyły bezpiecznego stosowania tożsamości cyfrowych przez urzędników[91]. Sytuacja w administracji rządowej i samorządowej nadal pozostawia wiele do życzenia[92].

---

[88] *ePUAP2*. Online: https://epuap.gov.pl/wps/portal, dostęp: 2017.06.04.

[89] Ratajczak, M. (2015) *E-administracja w Polsce kosztowała miliardy złotych. I wciąż jest gorsza niż w Rosji i Kazachstanie.* Money.pl. Online: http://news.money.pl/artykul/e-administracja-w-polsce-kosztowala-miliardy,48,0,1755184.html, 2015.04.08. oraz Maj, M. (2016). *Polska wśród państw "pozostających w tyle" jeśli chodzi o cyfryzację społeczeństwa.* Dziennik internautów Biznes i Prawo. Online: http://di.com.pl/polska-wsrod-panstw-pozostajacych-w-tyle-jesli-chodzi-o-cyfryzacje-spoleczenstwa-54512, dostęp: 2017.06.04.

[90] Nadybski, P. (2013). *Elektroniczna administracja w Polsce – ograniczenia i bariery.* Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy nr 9, s. 31–40.

[91] *NIK o wdrażaniu systemów teleinformatycznych w miastach i gminach.* (2015). NIK. Online: https://www.nik.gov.pl/aktualnosci/nik-o-wdrazaniu-systemow-teleinformatycznych-w-miastach-i-gminach.html, 2015.03.23.

[92] *Dane bez ochrony. NIK: samorządowe systemy informatyczne i gromadzone dane podatne na ataki hakerów* (2019). Online: https://samorzad.pap.pl/kategoria/archiwum

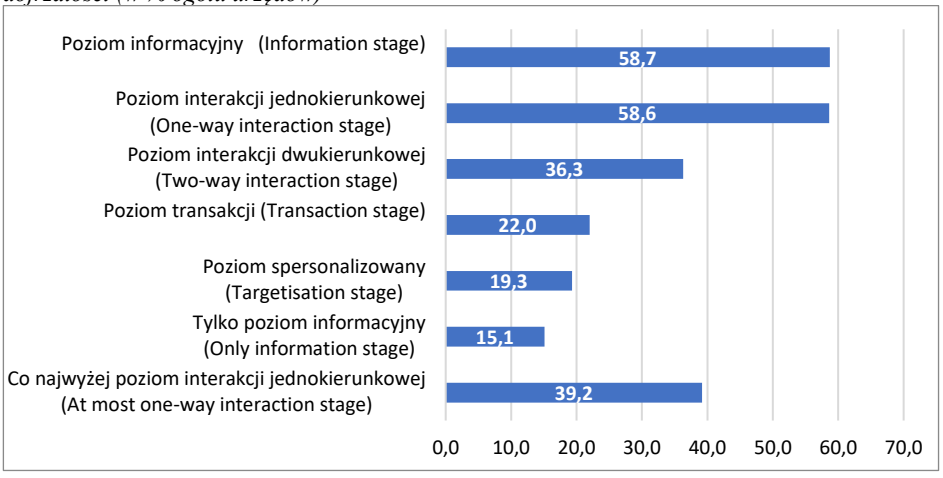
W 2014 r. większość urzędów oferowała usługi na 1–2 poziomie dojrzałości e-administracji (tabela 2.5., wykres 2.1.).

Tabela 2.5. Elektroniczne usługi udostępniane przez urzędy w 2014 r. według poziomu dojrzałości

Poziom dojrzałości usług *Maturity stages of services*	Usługi elektroniczne w % ogółu zadeklarowanych usług *Electronic services in % of total declared services*
Informacyjny *Information*	25,3
Interakcji jednokierunkowej *One-way interaction*	49,7
Interakcji dwukierunkowej *Two-way interaction*	16,1
Transakcji *Transaction*	7,1
Spersonalizowany *Targetisation*	1,8

Źródło: Berezowska, J., Huet, M., Kamińska, M. (2015). Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2011–2015. Główny Urząd Statystyczny. Warszawa. Online: http://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/1/9/1/spoleczenstwo_informacyjne_w_polsce_2011-2015.pdf, dostęp: 2017.06.04. s. 41.

Wykres 2.1. Urzędy, które w 2014 r. oferowały elektroniczne usługi publiczne według ich poziomu dojrzałości (w % ogółu urzędów)



Źródło: Berezowska, J., Huet, M., Kamińska, M. (2015). Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2011–2015. Główny Urząd Statystyczny. Warszawa. Online: http://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/1/9/1/spoleczenstwo_informacyjne_w_polsce_2011-2015.pdf, dostęp: 2017.06.04. s. 41.

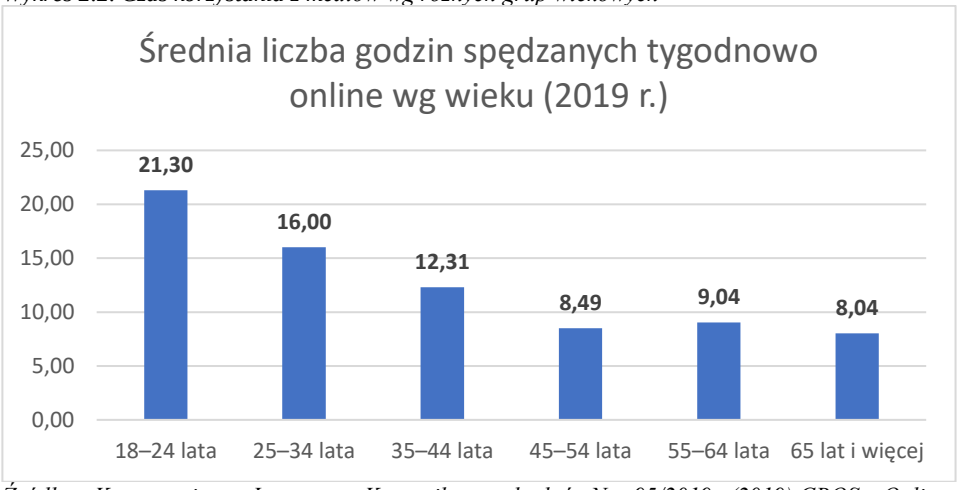
/dane-bez-ochrony-nik-samorzadowe-systemy-informatyczne-i-gromadzone-dane-podatne, 2019.05.10.

2.2.3.4. Zastosowanie tożsamości cyfrowych do celów prywatnych

Wykorzystanie Internetu w celach prywatnych jest powszechne, szczególnie w grupie nastolatków, którzy posiadali dostęp i korzystali z sieci od najmłodszych lat. Według badania z 2015 roku, w tej grupie 86,2% respondentów deklaruje, że korzysta z Internetu codziennie, a 43,2%, że stale jest online[93]. W badaniu CBOS z 2019 osoby w wieku między 18 a 24 lata w 100% korzystały z Internetu, z czego 57% było stale online[94]. Najpopularniejsze aktywności młodzieży w sieci w 2019 r. to: słuchanie muzyki (65,4%), oglądanie filmów (62,1%), komunikacja (61%), korzystanie z serwisów społecznościowych (59,4%) i odrabianie lekcji (50,6%)[95].

Ciekawa jest też analiza czasu poświęcanego na korzystanie z Internetu. Wynika z niej, że im młodszy użytkownik, tym więcej czasu spędza na korzystaniu z Internetu jako medium do pozyskania wiedzy i rozrywki (wykres 2.2.).

Wykres 2.2. Czas korzystania z mediów wg różnych grup wiekowych



Źródło: Korzystanie z Internetu, Komunikat z badań Nr 95/2019 (2019).CBOS. Online: https://www.cbos.pl/SPISKOM.POL/2019/K_095_19.PDF, dostęp: 14.12.2020.

Stąd należy się spodziewać, że wraz z wkraczaniem osób z młodszej grupy wiekowej w wiek produkcyjny, zwiększy się wykorzystanie tożsamości cyfrowych do celów związanych z prywatnym wykorzystaniem Internetu.

[93] Lange, R., Osiecki, J. (2014). *Nastolatki wobec Internetu*. Pedagogium Wyższej Szkoły Nauk Społecznych. Warszawa: NASK, s. 6.

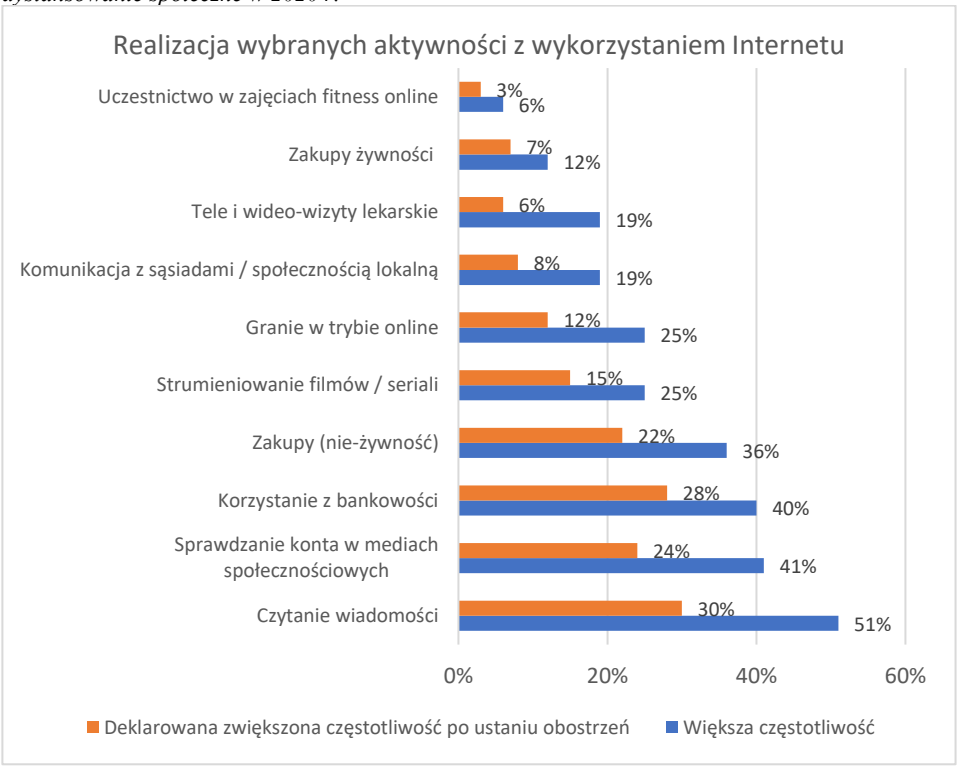
[94] *Korzystanie z Internetu, Komunikat z badań Nr 95/2019* (2019).CBOS. Online: https://www.cbos.pl/SPISKOM.POL/2019/K_095_19.PDF, dostęp: 14.12.2020.

[95] *Nastolatki 3.0* (2019). Red.: Bochenek, M., Lange, M. Raport NASK Państwowy Instytut Badawczy, Warszawa 2019.

Pandemia Covid-19 wpłynęła znacząco na sposób korzystania z Internetu. Co ciekawe, dotyczy to w istotny sposób szczególnie starszych użytkowników[96]. Przykładowo 45% osób w wieku 55–64 lata zaczęło korzystać z bankowości mobilnej i jest to największy odsetek z wszystkich grup wiekowych (średnia dla populacji wyniosła 40%).

Zmiany te mogą być też trwałe. Na wykresie 2.3 przedstawiono odsetek respondentów, którzy z powodu wymuszonej izolacji wykorzystywali Internet częściej do wybranych aktywności oraz tych, którzy deklarują utrzymanie tych zmian pomimo ustania dystansowania społecznego w przyszłości.

Wykres 2.3. Realizacja wybranych aktywności z wykorzystaniem Internetu wymuszona przez dystansowanie społeczne w 2020 r.



Źródło: opracowano na podstawie: Jak COVID-19 zmienił nasze zwyczaje w korzystaniu z usług cyfrowych? (2020). Digital Consumer Trends 2020. Online: https://www2.deloitte.com/pl/pl/pages/technology-media-and-telecommunications/articles/jak-COVID-19-zmienil-nasze-zwyczaje-w-korzystaniu-z-uslug-cyfrowych.html, listopad 2020.

[96] *Jak COVID-19 zmienił nasze zwyczaje w korzystaniu z usług cyfrowych?* (2020). Digital Consumer Trends 2020. Online: https://www2.deloitte.com/pl/pl/pages/technology-media-and-telecommunications/articles/jak-COVID-19-zmienil-nasze-zwyczaje-w-korzystaniu-z-uslug-cyfrowych.html, listopad 2020.

2.3. Zarządzanie tożsamością cyfrową

Zarządzanie tożsamością cyfrową można rozpatrywać na kilku płaszczyznach:

- Sposób uzyskiwania dostępu do zasobów za pomocą tożsamości cyfrowych w różnych strukturach (modele zarządzania tożsamością cyfrową).
- Kwestie związane z zarządzaniem pojedynczym kontem (proces tworzenia, blokowania i usuwania, modyfikacji uprawnień).
- Aspekty związane z wykorzystaniem narzędzi uwierzytelnienia opartych o różne metody uwierzytelnienia (wiedza, przedmiot, cecha).

2.3.1. Modele zarządzania tożsamością cyfrową

Tożsamość cyfrowa dla użytkownika, w kontekście sposobu jej użycia, może być utworzona i można nią zarządzać na kilka sposobów[97]. W zależności od tego, kto jest faktycznym posiadaczem i decyduje w kwestii tożsamości cyfrowej oraz kto zawiaduje informacją o użytkowniku można wyróżnić następujące modele[98]: autonomiczny (*Siloed model*), scentralizowany (*Centralized model*), sfederowany (*Federated model*) oraz kontrolowany przez użytkownika (*User-centric model*).

Pierwszą, podstawową możliwością jest zaimplementowanie tożsamości cyfrowej lokalnie. W przypadku np. nielicznych użytkowników, niewielkich zasobów w systemie informatycznym, czy ich nie współdzieleniu (praca na komputerach niepołączonych siecią wewnętrzną), tożsamość może być tworzona jako konto lokalne na danym urządzeniu lub mogą być tworzone odrębne konta dla każdego z użytkowników na poszczególnych serwerach (na każdym serwerze będzie wtedy osobna baza danych zawierająca informacje o użytkownikach). Zaletą tego rozwiązania jest mniejszy zasięg potencjalnych strat w przypadku kompromitacji konta (dostęp do zasobów, poznanie powiązań użytkownika itp.), wadą natomiast trudność sprawnego zarządzania kontem i niższa efektywność (nieefektywne wykorzystanie zasobów, duplikowanie czynności oraz trudniejsze zarządzanie kontem)[99].

---

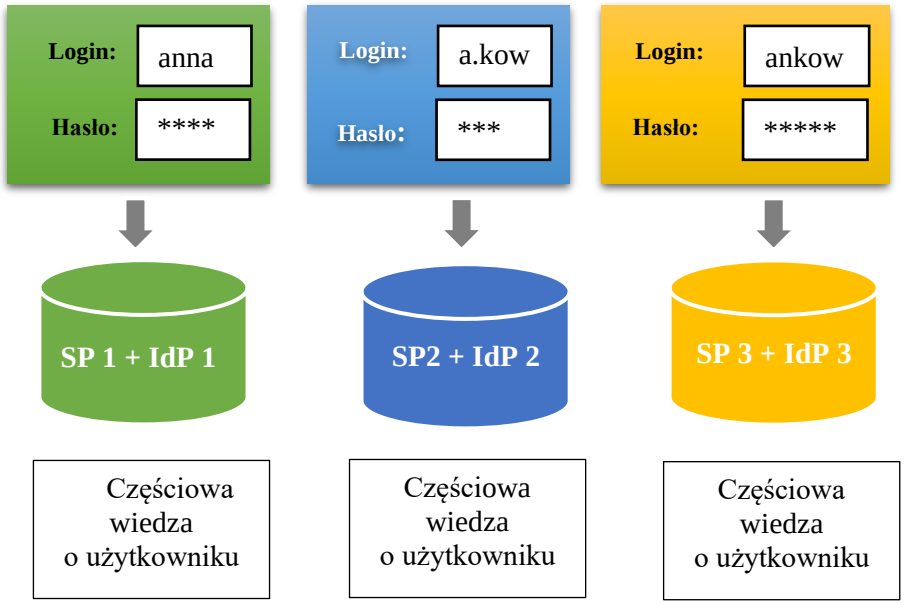
[97] Palfrey, J., Gasser, U. (2007). *Case Study. Digital Identity, Interoperability and eInnovation*. Berkman Publication Series, s. 5–21.

[98] Greenwood, D. *Context, Terms, Models and Options for Digital Identity Management*, OECD, s. 3 Online: http://www.oecd.org/sti/ieconomy/38584991.pdf, dostęp: 2017.06.04. oraz *The role of digital identity management in the internet economy: A primer for policy makers*. (2009). OECD. Online: http://www.oecd.org/internet /ieconomy/43195291.pdf, June 2009, s. 16.

[99] Palfrey, J., Gasser, U. (2007). *Case Study. Digital Identity, Interoperability and eInnovation*. Berkman Publication Series, s. 19–21.

Przykładowa procedura dostępu do zasobów oferowanych przez dostawcę SP 1 (rysunek 2.6.):

1. Wysłanie przez użytkownika żądania dostępu do zasobów SP 1 na serwer zawiadujący żądaną usługą.
2. Proces uwierzytelnienia przeprowadzony z udziałem dostawcy tożsamości IdP 1.
3. Udzielenie dostępu do zasobów lub jego odmowa.



SP x (*Service Provider*) – dostawca usług (zasobów) x
IdP x (*Identity Provider*) – dostawca tożsamości na potrzeby korzystania z zasobów x (lokalna baza użytkowników)

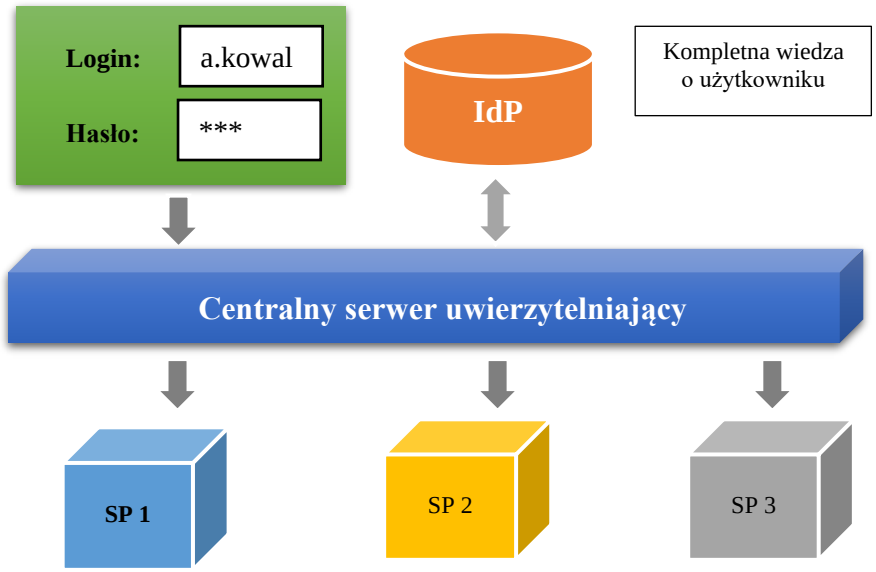
Rysunek 2.6. Autonomiczny model zarządzania tożsamością – przykład
Źródło: opracowanie własne.

Drugą możliwością jest scentralizowanie danych o użytkownikach w ramach organizacji, czyli utworzenie jednego konta (jednej tożsamości cyfrowej) dla każdego z użytkowników i zapisania go w centralnej bazie danych (np. z wykorzystaniem usługi Active Directory)[100]. To rozwiązanie znacznie ułatwia zarządzanie np. uprawnieniami użytkowników. Jest to obecnie najbardziej rozpowszechniony model.

[100] Pato, J. (2003). *Identity Management: Setting Context*. Encyclopedia of Information Security, (Summer/Fall).

Przykładowa procedura dostępu do zasobów oferowanych przez dostawcę SP 1 (rysunek 2.7.):

1. Wysłanie przez użytkownika żądania dostępu do zasobów SP 1 na centralny serwer uwierzytelniający.
2. Proces uwierzytelnienia przeprowadzony z udziałem centralnego dostawcy tożsamości IdP.
3. Udzielenie dostępu do zasobów SP 1 lub jego odmowa.



SP x (*Service Provider*) – dostawca usług (zasobów) x
IdP (*Identity Provider*) – dostawca tożsamości (centralna baza użytkowników)

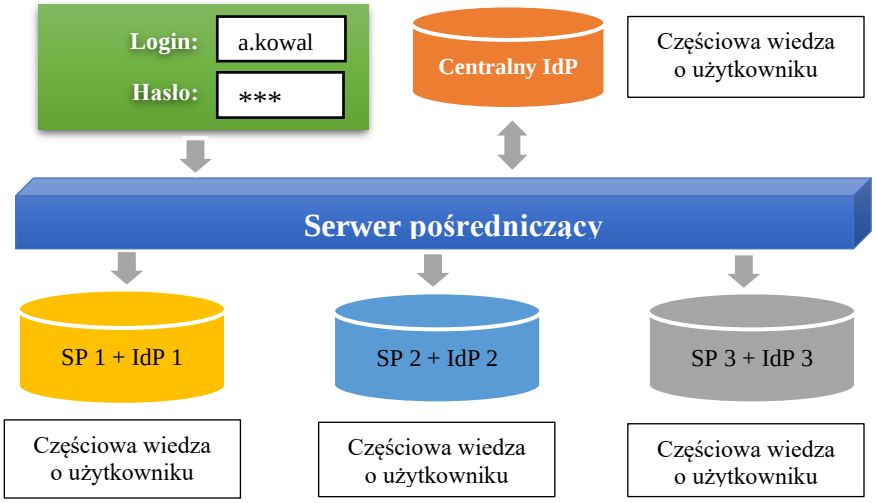
Rysunek 2.7. Scentralizowany model zarządzania tożsamością – przykład
Źródło: opracowanie własne.

Trzecią możliwością jest tzw. tożsamość sfederowana. Konto utworzone dla użytkownika umożliwia uzyskanie dostępu do zasobów także spoza tych, które kontrolowane są przez daną jednostkę, a należących do jednostek będących z tzw. kręgu zaufania (*Circle of trust*). Potwierdzenie praw do zasobów odbywa się z udziałem dostawcy tożsamości (*Identity Provider*) i dostawcy usług (*Service Provider*) w przypadku modelu rozproszonego. W przypadku modelu scentralizowanego w procesie dodatkowo uczestniczy federacyjny serwer, który, w uproszczeniu, zarządza procesem uwierzytelnienia (pośredniczy w procesie uwierzytelnienia przez macierzystą jednostkę), przechowuje informacje o afiliacjach użytkowników i odpowiada na pytania innych jednostek z federacji dotyczących tego czy i w jakim zakresie dana tożsamość ma prawo do dostępu do żądanych zasobów. Zaletą tego rozwiązania jest oszczędność czasu i środków sfederowa-

nych jednostek (brak konieczności powielania kont dla wszystkich użytkowników ich zasobów lub usług) oraz, szczególnie w przypadku wdrożenia rozwiązań typu SSO (*Single Sign-On*) użytkowników kont (jedno konto umożliwia dostęp do wielu zasobów), wadą natomiast poważniejsze skutki kompromitacji konta.

Przykładowa procedura dostępu do zasobów oferowanych przez dostawcę SP 1 (rysunek 2.8.):

1. Wysłanie przez użytkownika żądania dostępu do zasobów SP 1 na serwer pośredniczący.
2. Odnalezienie z wykorzystaniem centralnego IdP, macierzystego IdP x (tu: IdP 2).
3. Proces uwierzytelnienia przeprowadzony z udziałem macierzystego dostawcy tożsamości IdP 2 i SP 1.
4. Udzielenie dostępu do zasobów SP 1 lub odmowa.



SP x (*Service Provider*) – dostawca usług (zasobów) x należący do federacji
IdP x (*Identity Provider*) – dostawca tożsamości na potrzeby korzystania z zasobów x należący do federacji
Centralny IdP (*Identity Provider*) – centralny dostawca tożsamości, który gromadzi informacje o tym, które tożsamości w ramach poszczególnych IdP x należą do tego samego użytkownika (za pomocą linkowania) w ramach federacji

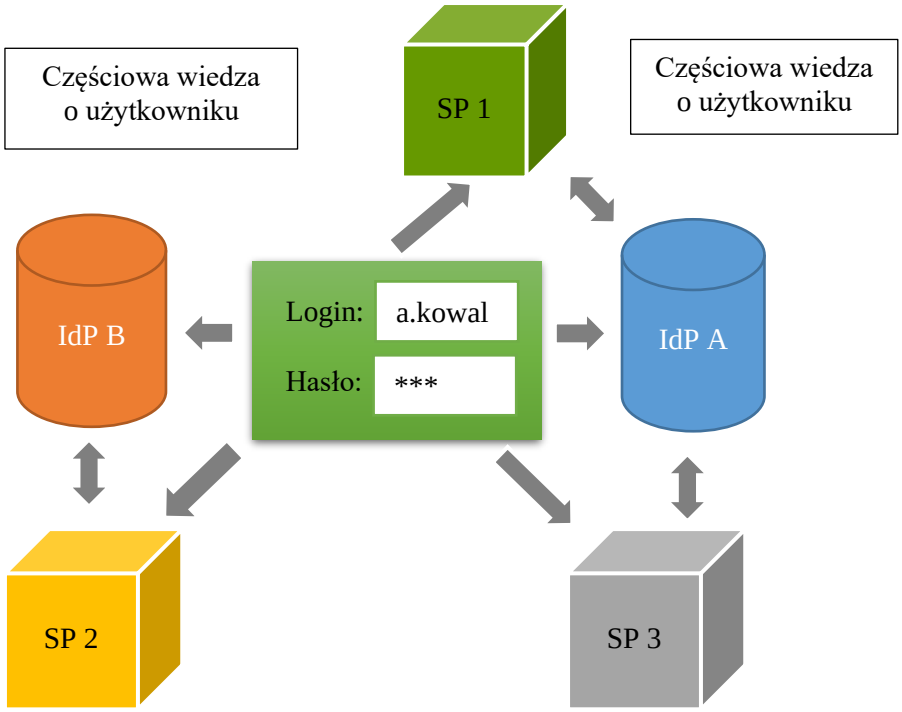
Rysunek 2.8. Scentralizowany federacyjny model zarządzania tożsamością – przykład
Źródło: opracowanie własne.

Czwartą możliwością jest tożsamość cyfrowa scentralizowana wokół użytkownika (*User-centric model*). W tym modelu to użytkownik decyduje kto będzie jego dostawcą tożsamości i jakie dane zostaną mu przez niego udostępnione. Dostawca tożsamości (IdP), zwany też zaufaną trzecią stroną (*Trusted third party*) nie musi należeć do federacji, w której znajduje się dostawca

żądanych zasobów, który w tym modelu jest określany jako strona zależna (*Relying party*).

Przykładowa procedura dostępu do zasobów oferowanych przez dostawcę SP 1 (rysunek 2.9.):

1. Wysłanie przez użytkownika żądania dostępu do zasobów SP 1
2. SP 1 uzyskuje potwierdzenie tożsamości użytkownika od IdP A
3. Udzielenie dostępu do zasobów SP 1 lub odmowa



SP x (*Service Provider*) – dostawca usług (zasobów) x ufający niezależnemu IdP X
IdP X (*Identity Provider*) – niezależny dostawca tożsamości

Rysunek 2.9. Scentralizowany wokół użytkownika model zarządzania tożsamością – przykład
Źródło: opracowanie własne.

Porównanie cech modeli przedstawiono w tabeli 2.6.

Tabela 2.6. Porównanie modeli zarządzanie tożsamością cyfrową

	Autonomiczny	Scentralizowany	Sfederowany	Scentralizowany wokół użytkownika
Metoda uwierzytelnienia	Uwierzytelnienie do każdego konta osobno.	Uwierzytelnienie do jednego, głównego konta.	Uwierzytelnienie na macierzystym serwerze w celu dostępu do usług w ramach federacji.	Uwierzytelnienie do IdP, na którym polega dostawca żądanych usług.
Lokalizacja danych uwierzytelniających	Oddzielne konta IdP.	Jedno, główne konto (superkonto) na centralnym IdP.	Oddzielne konta poszczególnych IdP należących do federacji.	Dane są przechowywane przez wybranego przez użytkownika IdP.
Linkowanie (łączenie profili)	Brak.	Brak.	Federacyjny IdP jest w stanie wskazać konta tej samej osoby.	W celu uniknięcia linkowania wykorzystywana jest kryptografia.
Zaufanie i zależność	Użytkownik jest uzależniony od ochrony jego danych przez usługodawcę. Prywatność zapewnia brak wymiany informacji.	Prywatność i bezpieczeństwo danych użytkownika zależy od ochrony zapewnianej przez centralny IdP.	Federacja posiada przewagę w posiadaniu danych o użytkowniku.	Użytkownicy mogą zachować oddzielne konta i większą prywatność, ale ponoszą większą odpowiedzialność.
Wygoda	Niewygodne (wiele uwierzytelnień, zbędne wprowadzanie informacji i brak przepływu danych).	Wygodne (tylko jedno poświadczenie).	Wygodne (inni członkowie federacji unikają ciężaru zarządzania certyfikatami, organizacje świadczące usługi dla użytkownika mogą koordynować świadczenie usług).	Wygodne, jednak wymaga od użytkownika umiejętności i przygotowania do zarządzania własnymi danymi (także luką w zabezpieczeniach).

	Autonomiczny	Scentralizowany	Sfederowany	Scentralizowany wokół użytkownika
Bezpieczeństwo	IdP zarządzają dostępem do pojedynczego konta, mają lepszy definiowany i silniejszy obszar bezpieczeństwa, ograniczoną ekspozycja na awarie i kompromitację uwierzytelnienia.	Duże ryzyko spowodowane kontrolą przez IdP całego profilu osoby; co oznacza poważne skutki w przypadku podszycia się intruza.	Duża zależność od zabezpieczeń członków federacji, przeniknięcie intruza pociąga skutki dla całej federacji.	Koncentracja IdP na rynku może nieść negatywne skutki, brak możliwości zabezpieczenia danych po ich udostępnieniu.

Źródło: opracowanie na podstawie http://www.oecd.org/internet/ieconomy/43195291.pdf

Opisane modele bazują na dostawcy tożsamości, którego silna pozycja generuje szereg ograniczeń i zagrożeń (np. niemożność potwierdzenia tożsamości w przypadku awarii technicznej dostawcy, wyciek danych czy odmowa potwierdzenia tożsamości jako forma represji). Odpowiedzią może być model suwerennej tożsamości (ISS, ang. *Self Sovereign Identity*) będący rodzajem zdecentralizowanej tożsamości wykorzystujący zdecentralizowane identyfikatory (DID, ang. *Decentralized Identifiers*)[101] w technologii Block Chain, gdzie dane dotyczące tożsamości są analogiczne do danych transakcyjnych[102].

Pierwszym krokiem do utworzenia tożsamości cyfrowej w tym modelu będzie utworzenie pierwszego bloku zawierającego dane biometryczne (np. odcisk palca). Jest to tak zwany stały atrybut tożsamości[103]. Następnie tworzone są powiązane w sposób szyfrowany kolejne bloki zawierające atrybuty, które mogą być dowolnie modyfikowane (np. adres). Dzięki temu użytkownik jest de facto dostarczycielem własnej tożsamości, samodzielnie ją modyfikuje i nią zarządza.

Ten model jest obecnie w fazie rozwoju, ale jego zalety zostały już dostrzeżone[104] i można spodziewać się rozwoju regulacji prawnych, a co za tym idzie szerszego zastosowania w np. bankowości.

[101] *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations* (2020). W3C Working Draft 24 November 2020. Online: W3C Working Draft 24 November 2020. Online: https://www.w3.org/TR/did-core/, dostęp: 20.11.2020.

[102] Gulati, H., Huang, C.-T. (2019). *Self-Sovereign Dynamic Digital Identities based on Blockchain Technology*. 2019 SoutheastCon, s. 1–6.

[103] *Tamże* .

[104] *EIDAS supported Self-Sovereign Identity* (2019). Dokumenty Komisji Europejskiej. Online: https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf, dostęp: 30.11.2020.

Inny podział modeli według różnych źródeł zaufania do tożsamości cyfrowej wyszczególnia[105]:

1. Modele oparte na autorytecie państwa (*Authority based model*) wynikające z uwarunkowań prawa publicznego np. paszporty.
2. Modele oparte na przewadze (*Power based model*), narzucane przez duże organizacje posiadające przewagę swoim kontrahentom.
3. Modele oparte o dobrowolne porozumienie dwóch, równych sobie stron (*Agreement based model*), które zgadzają się na stosowanie wspólnych standardów i praktyk.

2.3.2. Zarządzanie kontem użytkownika

W zabezpieczeniu dostępu do zasobów za pomocą tożsamości cyfrowych można wydzielić trzy procesy[106]: rejestracji, zarządzania i uwierzytelnienia.

Proces rejestracji, czyli utworzenia tożsamości cyfrowej i powiązania jej z konkretną osobą powinien być poprzedzony zbadaniem roli biznesowej użytkownika i określeniem do jakich zasobów i w jakim stopniu powinien mieć on dostęp oraz jakie działania może na tych zasobach wykonać. Zasadą ograniczającą ryzyko związane z dostępem do danych nieuprawnionych pracowników przedsiębiorstwa jest stosowanie zasady minimalnego dostępu, czyli uprawnień nie większych niż te, które umożliwiają wykonywanie obowiązków. Zidentyfikowane role determinują uprawnienia, które można przypisać dla grupy użytkowników (np. pracowników jednego działu) oraz indywidualne (np. dla kierownika tego działu). Przydzielenie uprawnień (*Provisioning*) może odbyć się na trzy sposoby[107]:

- uznaniowo, gdy administrator sieci przydziela wybrane przez siebie zasoby. Jest to najbardziej popularne rozwiązanie dla niewielkich przedsiębiorstw, gdzie administrator posiada wiedzę wystarczającą do określenie potrzeb użytkowników w obszarze dostępu do zasobów;

---

[105] Greenwood, D. *Context, Terms, Models and Options for Digital Identity Management*. Online: http://www.oecd.org/sti/ieconomy/38584991.pdf, dostęp: 2017.06.04. s. 4.

[106] Mielnicki, T. i inni red. (2013). *Identyfikacja i uwierzytelnienie w usługach elektronicznych*. Forum Technologii Bankowych przy Związku Banków Polskich. Warszawa, s. 13. Online: https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf, dostęp: 2017.06.04. oraz OECD (2011). *Digital identity management. Enabling Innovation and Trust in the Internet Economy, s. 10*. Online: http://www.oecd.org/sti/ieconomy/49338380.pdf.

[107] Rouse, M. (2010). *Definition of user account provisioning.* TechTarget Network. Online: http://searchsecurity.techtarget.com/definition/user-account-provisioning, dostęp: 2017.06.04.

- we współpracy z użytkownikiem, gdy część działań związanych z zarządzaniem kontem (zwykle dotyczy to kwestii związanych z hasłem) jest w gestii na użytkownika;
- na podstawie przepływu pracy (*Workflow*), gdzie konkretne uprawnienia przydzielane są przez administratora na wniosek osób decyzyjnych (zarządzających), odpowiedzialnych za zasoby lub wyniki pracy podległego im użytkownika. Ta sytuacja ma miejsce zwykle w większych organizacjach.

Po utworzeniu konta, użytkownik powinien otrzymać informacje dotyczące sposobu użytkowania konta, a w tym informacje o loginie i haśle (jeśli są), wytycznych i procedur związanych z korzystaniem z konta (szkolenie wstępne). Powinien otrzymać przedmioty uwierzytelniające (jeśli są) wraz z instrukcją korzystania i niekiedy inicjalizacji (np. poprzez aktywację karty). Pracownik powinien pisemnie potwierdzić zarówno otrzymanie informacji, przedmiotów, instrukcji, jak i zrozumienie warunków ich użycia[108].

W ramach zarządzania istniejącym kontem można wyróżnić szereg działań, które są zbieżne z cyklem pracy pracownika w przedsiębiorstwie:

- Wydawanie, zmiana (np. po upłynięciu czasu ważności), zawieszanie (np. po zagubieniu) oraz niszczenie (np. po odejściu pracownika) danych (login, hasło, numer PIN), aplikacji (np. token w postaci aplikacji na telefon komórkowy) lub urządzeń uwierzytelniających (karty, tokeny). W procesie zarządzania hasłami mogą brać udział sami użytkownicy konta, szczególnie w przypadku wyboru nowego hasła i odzyskiwania utraconego hasła.
- Modyfikacja uprawnień, polegająca na dostosowaniu uprawnień użytkownika do jego stanowiska pracy lub wykonywanych zadań. Istotne jest by unikać kumulacji uprawnień, która ma miejsce, gdy uprawnienia są tylko rozszerzane, bez odbierania uprawnień do zasobów, które nie są już niezbędne do pełnienia nowych obowiązków. Szczególnym przypadkiem jest oddelegowanie pracownika do projektu. W przypadku projektów, do których pracownik powinien mieć dostęp tylko na pewnym etapie, dostęp do wyników projektu powinien być mu odebrany niezwłocznie po zakończeniu udziału w nim pracownika.
- Ewidencja działań związanych z wykorzystaniem konta oraz danych uwierzytelniających oraz okresowy ich audyt.
- Zablokowanie lub usunięcie konta (*Deprovisioning*), które ma miejsce wtedy, gdy dane konto jest zbędne, czyli najczęściej po opuszczeniu przez pracownika przedsiębiorstwa. Konta byłych pracowników powinny być

[108] Wołowski, F., Zawiła-Niedźwiecki, J. (2012). *Bezpieczeństwo systemów informacyjnych: praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*. Kraków; Warszawa: edu-Libri, s. 244.

zawieszane na jakiś czas, gdyż w razie wykonania przez nich późno wykrytych działań na szkodę przedsiębiorstwa, usunięcie konta będzie skutkowało usunięciem historii działań dokonywanych z jego użyciem.

Trzeci proces, który związany jest z tożsamościami cyfrowymi wiąże się z uzyskiwaniem dostępu do zasobów. Podzielony jest on na kilka etapów, które nie muszą jednak wystąpić zawsze:

1. Zadeklarowanie tożsamości przez użytkownika i jego identyfikacja (*Identification*), czyli proces zautomatyzowanego rozpoznania danego użytkownika w systemie, z wykorzystaniem jego unikalnego identyfikatora.[109] Deklaracją tożsamości może być podanie loginu lub wczytanie odcisku palca (w tym wypadku jest to jednocześnie wysłanie potwierdzenia).
2. Uwierzytelnienie (*Authentication*), czyli zweryfikowanie deklarowanej tożsamości jednostki[110]. Odbywa się ono z wykorzystaniem szeregu metod uwierzytelnienia. Wynikiem tego działania jest zgodność lub niezgodność identyfikatora z poświadczeniem.
3. Autoryzacja (*Authorization*), czyli nadanie praw, obejmujących przyznanie dostępu na podstawie praw dostępu[111]. Innymi słowy następuje sprawdzenie czy i w jakim zakresie dana tożsamość ma dostęp do żądanych zasobów.
4. Reakcja na nieudaną próbę uwierzytelnienia (np. blokowanie dostępu do danego konta po określonej liczbie prób zalogowania) lub przełamania zabezpieczeń systemu[112].

2.3.3. Metody i narzędzia uwierzytelnienia

Najczęściej stosowanymi metodami uwierzytelnienia są[113]:

1. Metody oparte na wiedzy (*Something you know*).
2. Metody oparte o posiadanie przedmiotu (*Something you have*).
3. Metody oparte o cechy biometrię (*Somehing you are*).
4. Inne metody oparte np. o lokalizację, czas dostępu.

---

[109] *PN-I-02000*, poz. 3.1.031.

[110] *PN-ISOIIEC 2382-8*, poz. 08.01.I1.

[111] *PN-I-02000*.

[112] Mielnicki, T. i inni red. (2013). *Identyfikacja i uwierzytelnienie w usługach elektronicznych*. Forum Technologii Bankowych przy Związku Banków Polskich. Warszawa, s. 106. Online: https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf. oraz *Digital identity management. Enabling Innovation and Trust in the Internet Economy.* (2011). OECD, s. 10. Online: http://www.oecd.org/sti/ieconomy/49338380.pdf.

[113] Windley, Ph. J. (2005). *Digital Identity.* Sebastopol: O'Reily, s. 50–62.

Wśród metod bazujących na wiedzy użytkownika najpopularniejsze są hasła i numery PIN, czyli ciągi znaków (liczby i znaki alfanumeryczne oraz specjalne) używanych jako informacja uwierzytelniająca[114]. Innym przykładem jest symbol odblokowania, czyli wzór rysowany na dotykowym ekranie urządzenia mobilnego w celu jego odblokowania, czy np. wybór z podanego zestawu twarzy znanych uprawnionemu użytkownikowi. Wszystkie te narzędzia bazują na „tajemnicy" jaką jest skład hasła, kolejność połączenia wybranych punktów lub wiedza pochodząca z indywidualnego doświadczenia użytkownika. Bezpieczeństwo zasobów chronionych narzędziem opartym o wiedzę, zależy od zachowania „tajemnicy".

Proces uwierzytelnienia polega w tym przypadku na wpisaniu w żądane miejsce loginu (jeśli jest tajny), loginu i hasła, numeru PIN, połączenie wybranych punktów w określony sposób lub zaznaczenie właściwej odpowiedzi. Podstawowymi zaletami tej metody jest brak kosztów i powszechność. Pierwsze zastosowanie hasła miało miejsce już w 1961 r., choć powodem zastosowania kont nie były kwestie bezpieczeństwa, tylko podział czasu pracy procesora[115]. Użytkownicy są zwykle przyzwyczajeni do weryfikacji za pomocą loginu i hasła, gdyż z uwagi na prostotę, łatwość i uniwersalność tej metody jest ona stosowana praktycznie we wszystkich wymagających autoryzacji dostępu urządzeniach (np. telefon, komputer) oraz usługach (np. bankowość elektroniczna, konto pocztowe). Wady tego rozwiązania wynikają z nieprzystosowania ludzkiego umysłu do zapamiętywania niekojarzących się ciągów znaków: długie hasła są trudne do zapamiętania, krótkie – łatwe do złamania, stąd pokusa podejmowania działań ułatwiających użytkownikowi korzystanie z haseł, ale wystawiających hasło na ryzyko kompromitacji i obniżających tym samym bezpieczeństwo danych. Przykłady takich „ułatwień" to m.in.:

- przechowywanie zapisu hasła w nieodpowiedni sposób (np. naklejona na komputerze karteczka, plik nieszyfrowany);

[114] *PN-ISO/IEC 2382-8:2001 Technika informatyczna – Terminologia – Bezpieczeństwo.*

[115] Pierwszym rozwiązaniem, które umożliwiało dzielenie czasu pracy procesora pomiędzy użytkowników, był system operacyjny CTSS (*Compatible Time-Sharing System*) stworzony przez zespół Fernando J. Corbató w MIT (*Massachusetts Institute of Technology*) w 1961 r. Ponadto system zwiększył możliwości interakcji człowieka i komputera poprzez zdalny dostęp do komputera za pomocą łącz telefonicznych. Uzyskanie dostępu dokonywane było z użyciem nazwy użytkownika i prostego, indywidualnego hasła. Już rok później dochodzi do pierwszej, można powiedzieć, kradzieży tożsamości. Doktorant Allan Scherr, posiadający dostęp do maszyny IBM 7094 z zaimplementowanym oprogramowaniem CTSS, postanowił zwiększyć swój czterogodzinny limit czasu. W tym celu napisał program, który umożliwił mu wydrukowanie listy haseł wszystkich użytkowników. W efekcie korzystał z komputera w nieograniczonym zakresie. W tym czasie pojawił się także pierwszy sprzętowy incydent naruszenia bezpieczeństwa. Z powodu usterki programu, wszyscy użytkownicy otrzymali dostęp do wspomnianej już listy haseł.

- stosowanie prostych, słownikowych lub łatwych do odgadnięcia haseł o nieodpowiedniej długości i składzie (rodzaje użytych znaków);
- stosowanie jednego hasła do różnych kont w pracy i życiu prywatnym;
- nie zmienianie okresowe haseł;
- przekazywanie haseł osobom nieuprawnionym intencjonalnie (np. współpracownikowi) lub nieumyślnie (np. w rozmowie z współpracownikiem przy kliencie).

Metody oparte na posiadaniu przedmiotu potwierdzającego uprawnienia jego właściciela wykorzystują szereg przedmiotów, takich jak:

- karty kryptograficzne (stykowe i bezstykowe), zawierające klucze prywatne posiadacza i wymagające korzystania z dodatkowych urządzeń (czytnik kart);
- tokeny występujące najczęściej w formie:
  - urządzenia USB, czyli odpowiednika karty kryptograficznej zintegrowanej z czytnikiem (nie wymaga dodatkowego urządzenia – łączy się za pomocą portu USB),
  - tokena OTP (*One Time Password*), czyli generatora haseł jednorazowych, wykorzystywanych podczas uwierzytelnienia, bazujących na synchronizacji czasowej lub liczniku,
  - urządzenia hybrydowego łączącego token OTP z tokenem USB,
  - aplikacji zainstalowanej na urządzeniu mobilnym, stacjonarnym lub przeglądarce (*Soft token*);
- karty haseł jednorazowych, zawierającej określoną liczbę krótkich ponumerowanych ciągów cyfr.

Stosowanie tych przedmiotów polega na zbliżeniu lub włożeniu przedmiotu do czytnika (karty) albo portu USB (tokeny USB i hybrydowe) na żądanie systemu lub podaniu na żądanie generowanego hasła (token OTP), lub hasła generowanego w odpowiedzi na konkretne dane podczas żądania (tokeny typu challenge – response oraz karty haseł jednorazowych).

Bezpieczeństwo zasobów chronionych za pomocą przedmiotów zależy głównie od tego, czy nie znajdą się w niepowołanych rękach. Przedmioty często umożliwiają weryfikację wielostopniową, tj. są dodatkowo zabezpieczone numerem PIN, co zabezpiecza je dodatkowo przed nieautoryzowanym użyciem.

Przedmioty uwierzytelniające są stosunkowo tanim i rozpowszechnionym rozwiązaniem, które (w przypadku np. kart elektronicznych) może łączyć funkcje dostępu do zasobów informacyjnych jak i fizycznych przedsiębiorstwa. Do wad tego sposobu potwierdzania uprawnień należy ryzyko kradzieży lub skopiowania przedmiotu (częściowo może być zmniejszone poprzez stosowanie urządzeń zabezpieczonych numerem PIN), które może przełożyć się zagrożenie wszystkich zasobów, do których dostęp jest chroniony danym przedmiotem. Kolejna kwestia związana jest z zawodnością urządzeń, czyli podatnością na uszkodzenie fizyczne czy wyczerpanie się baterii, czego skutkiem jest niemożność uzyskania dostępu

do zasobów i często dłuższy czas oczekiwania na wydanie lub naprawienie przedmiotu. Mimo, iż ceny urządzeń nie są duże, to jednak sumarycznie mogą stanowić pewne obciążenie finansowe tym bardziej, że zwykle mają ograniczony czas działania (termin ważności lub liczba generowanych haseł jednorazowych).

Kolejną grupą są metody oparte na biometrii, czyli cechach fizycznych lub behawioralnych uprawnionego użytkownika. Najpopularniejsze wśród nich to:

- odciski palców (linie papilarne),
- układ naczyń krwionośnych,
- geometria dłoni, twarzy,
- naczynia krwionośne siatkówki oka,
- wzór tęczówki,
- analiza głosu,
- analiza sposobu pisania na klawiaturze.

Proces uwierzytelnienia się z użyciem metod biometrycznych poprzedzony jest utworzeniem wzorca referencyjnego, czyli pobraniem odcisku palca, zeskanowaniu układu naczyń krwionośnych, tęczówki i siatkówki, zarejestrowaniem próbki głosu itd. Wzorzec ten jest wykorzystywany do przeprowadzenia porównania z wczytanymi podczas uwierzytelnienia danymi użytkownika deklarującego posiadanie uprawnień do żądanych zasobów. Wynik porównania decyduje o przyznaniu bądź odmowie dostępu. Z uwagi na zmiany cech fizycznych w czasie (głównie starzenie się) wzorzec referencyjny ulega korekcie podczas uwierzytelniania się. Zalety tego rozwiązania są związane głównie z wygodą użytkownika. Weryfikacja biometryczna jest dla użytkownika najmniej obciążająca, gdyż wystarczy, że użytkownik „jest". Nie musi wykonywać dodatkowych działań zabezpieczających, ani nie może „pożyczyć" czy „zgubić" swojej tożsamości[116]. Jednakże w przypadku tej metody pojawiają się kwestie etyczne podnoszone głównie przez organizacje broniące praw obywatelskich takie jak ACLU (American Civil Liberties Union) lub NO2ID[117]. Główną siłą, ale i słabością weryfikacji biometrycznej jest bowiem oparcie się na cechach nierozerwalnie związanych z konkretną osobą, a co za tym idzie większe ryzyko w przypadku kompromitacji, która w tej sytuacji oznacza przede wszystkim kradzież wzorca referencyjnego. Jest to w zasadzie kradzież danych osobowych, których utrata stanowi nieodwracalną szkodę dla konkretnej osoby. W metodach biometrycznych kluczem do zasobów jest sama osoba (a dokładniej jej cechy), stąd występują tu specyficzne zagrożenia przy próbie użycia tego „klucza" w celu

[116] Poznański, R., Szacki, K. (2011). *Bezpieczne uwierzytelnianie biometryczne na przykładzie rozwiązania AXSionics Internet Passport*. Techniki komputerowe biuletyn informacyjny XLV, Nr 1. Warszawa: Wyd. Instytut Maszyn Matematycznych, s. 160–162.

[117] Plucińska, M., Ryżko, J. (2010). *Rozwój i perspektywy biometrii na świecie.* Techniki komputerowe biuletyn informacyjny, XLV, Nr 1. Warszawa: Wyd. Instytut Maszyn Matematycznych, s. 9–21.

dotarcia do chronionego zasobu, takie jak przymuszenie do uwierzytelnienia czy zagrożenie zdrowia i życia. W przypadku większości metod zmienność cech fizycznych czy behawioralnych powoduje ryzyko nieudzielenia osobie autoryzowanej dostępu do zasobów w przypadku nagłej zmiany cech np. skaleczenia przy metodzie bazującej na odcisku palca czy chrypce w przypadku analizy głosu. Są też przypadki, gdy osoba w ogóle nie posiada badanych przez system cech (np. osoby nieme czy z adermatoglifią). Z punktu widzenia przedsiębiorców prawdopodobnie największą wadą tych rozwiązań jest wysoki koszt specjalistycznych urządzeń (skanery, czytniki, urządzenia rejestrujące), ale także brak zaufania czy opór pracowników.

Metodą o stosunkowo najmniejszym ryzyku związanym z odmową udzielenia dostępu jest metoda oparta o analizę układu naczyń krwionośnych czy siatkówki oka, jednak najpowszechniejszą – czytnik odcisków linii papilarnych, który powoli staje się standardowym elementem konfiguracji sprzętowej komputerów i urządzeń mobilnych. Mimo wad tego rozwiązania, z uwagi na wygodę, uwierzytelnienie biometryczne może zyskać wielu zwolenników[118]. O tym, że techniki biometryczne są postrzegane jako rozwiązanie wiarygodne i przyszłościowe świadczy m.in. gwałtowny rozwój technologii biometrycznych[119] czy wprowadzenie we wrześniu 2012 r. weryfikacji dostępu do konta bankowego na podstawie układu naczyń krwionośnych w jednym z banków w Polsce[120].

[118] Koziczak, A. (2010). *Społeczna akceptacja identyfikacji biometrycznej. Rozwój i perspektywy biometrii na świecie*. Techniki komputerowe biuletyn informacyjny XLV, Nr 1. Warszawa: Wyd. Instytut Maszyn Matematycznych, s. 41–46.

[119] Pacut, A. (2012). *Nie uciekniemy już od biometrii*. Online: http://centrumpr.pl/artykul/nie-uciekniemy-juz-od-biometrii,39105.html, dostęp: 2012.09.28.

[120] Starkowski, M. T. *Palec zamiast karty* (2012). Online: http://www.biztok.pl/Palec-zamiast-karty-a5617, dostęp: 2012.10.04. oraz Beata Zduńczyk-Golędzinowska (2012*). Identyfikacja biometryczna w Banku BPH*, informacja prasowa, Warszawa. Online: http://www.bph.pl/repo/bph/PR/informacje_prasowe/2012/120919.pdf, dostęp: 2012.09.20.

3. Zarządzanie tożsamością cyfrową w przedsiębiorstwach sektora MSP

3.1. Charakterystyka sektora MSP w kontekście wykorzystania narzędzi teleinformatycznych i rozwiązań tożsamości cyfrowej

Sektor małych i średnich przedsiębiorstw (MSP) jest podzbiorem sektora mikro, małych i średnich przedsiębiorstw (MMSP).

W dokumencie OECD zatytułowanym Small and Medium Enterprise Outlook 2002[121] podano, że „*brak jest jednej definicji sektora MSP, a liczba pracowników nie musi być pojedynczym kryterium definiującym. Jednakże, przedsiębiorstwa sektora MSP są generalnie autonomicznymi i niezależnymi firmami zatrudniającymi mniej niż określoną liczbę osób*."[122] Raport definiuje dwie skale[123]:

- ogólnoświatową, uwzględniającą specyfikę krajów takich jak USA, według której przedsiębiorstwa dzielą się na bardzo małe i małe (20–99), średnie (99–499) i duże (powyżej 500 pracowników),
- uwzględniającą specyfikę Europejską (zapisana w zaleceniach Komisji Europejskiej i powielona w polskim prawodawstwie)[124], która definiuje przedsiębiorstwa jako: mikroprzedsiębiorstwa (do 9 pracowników), małe (10–49), średnie (50–249) i duże (powyżej 250 pracowników).

Przedziały zatrudnienia małych i średnich przedsiębiorstw kształtują się różnie w poszczególnych państwach w zależności od specyfiki danej gospodarki. W Polsce, według art. 105-106 Ustawy o swobodzie działalności gospodarczej z dnia 2 lipca 2004 roku: „*za małego przedsiębiorcę uważa się przedsiębiorcę, który w co najmniej jednym z dwóch ostatnich lat obrotowych:*

1) *zatrudniał średniorocznie mniej niż 50 pracowników oraz*
2) *osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz operacji finansowych nieprzekraczający równowartości w złotych 10 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 10 milionów euro.*

---

[121] OECD (2002). *Small and Medium Enterprise Outlook 2002, Enterprise, Industry and Services*, s. 7.

[122] Tłum. własne.

[123] Tamże.

[124] *Zalecenie Komisji Nr 96/280/WE z 3.04.1996 r. dotyczące definicji małych i średnich przedsiębiorstw (Dz.U. L 107 z 30.04.1996), Rozporządzenie Komisji (WE) nr 70/2001 (Dz. Urz. UE L 10 z 13.01.2001, s. 33), Zalecenie Komisji z 6.05.2003 r. dotyczące definicji mikroprzedsiębiorstwa oraz małych i średnich przedsiębiorstw (Dz.U. WE Nr L. 124 z 20.05.2003), Rozporządzenie 364/2004 (Dz. Urz. UE L 63 z 28.02.2004), Ustawa o swobodzie działalności gospodarczej z dnia 2 lipca 2004 roku*.

Za średniego przedsiębiorcę uważa się przedsiębiorcę, który w co najmniej jednym z dwóch ostatnich lat obrotowych:

1) *zatrudniał średniorocznie mniej niż 250 pracowników oraz*
2) *osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz operacji finansowych nieprzekraczający równowartości w złotych 50 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 43 milionów euro."* [125]

Przedstawiony podział jest oparty na kryterium ilościowym i utworzony został na potrzeby statystyczne i prawne. Najbardziej lakonicznym opisem przedsiębiorstw z sektora MMSP jest „działalność na małą skalę"[126]. Nie oznacza to jednak, że przedsiębiorstwo z tego sektora jest po prostu mniejszą wersją dużego przedsiębiorstwa[127]. Posiadając z reguły mniejsze zasoby są szczególnie narażone na ryzyko i borykają się z problemami, na które duże przedsiębiorstwa są bardziej odporne szczególnie dotyczącymi kwestii pozyskania funduszy czy know how. Są więc m.in. podmiotami celowego wsparcia rządowego i UE. Stąd kryterium dotyczące obrotów bądź posiadanych aktywów, które ogranicza korzystanie ze wsparcia przez te podmioty, które nie potrzebują szczególnej ochrony i pomocy. Przyczyną wsparcia sektora MMSP jest jego szczególne znaczenie w gospodarce[128].

- znaczny udział w produkcie krajowym brutto (PKB),
- znaczny udział w tworzeniu miejsc pracy,
- wysoka innowacyjność sektora, spowodowana wyższą elastycznością, szybszą reakcją na sygnały rynkowe i dostosowaniem się do klienta,
- czynnik integrujący społeczeństwo, umożliwiający kumulowanie i przekazywanie wiedzy i kształtowanie postaw przedsiębiorczych,
- czynnik dywersyfikacji rynku wspierający zdrową konkurencję.

---

[125] *Ustawa o swobodzie działalności gospodarczej z dnia 2 lipca 2004 roku*.

[126] Piecuch, T. (2010). *Funkcjonowanie małych i średnich przedsiębiorstw w gospodarce*. W: Matejun, M., red. Wyzwania i perspektywy zarządzania w małych i średnich przedsiębiorstwach. Warszawa: C.H. Beck, s. 15–29, s. 16.

[127] *Słownik innowacji – leksykon haseł*. Online: http://www.pi.gov.pl, dostęp: 2017.06.04.

[128] Czerwińska-Lubszczyk, A., Michna, A., Męczyńska, A. (2013). *Determinanty rozwoju małych i średnich przedsiębiorstw sektora budowlanego*. Zarządzanie i Finanse, Tom 4 Nr 2, s. 81–82, oraz Mikołajczyk, B., Krawczyk, M. (2006). *Sektor przedsiębiorstw mikro, małych i średnich w krajach Unii Europejskiej*. Studia Europejskie / Centrum Europejskie Uniwersytetu Warszawskiego, Nr 2, s. 68–69, oraz Łapacz, D. (2015). *Udział małych i średnich przedsiębiorstw w wytwarzaniu PKB – Polska na tle Unii Europejskiej*. Electronic Scientific Journal, 6 Issue 1, s. 43, oraz Zadura-Lichata, P. (2012). *Małe i średnie przedsiębiorstwa a dobre zarządzanie – Raport o stanie sektora MSP w Polsce*. Warszawa: PARP. Online: http://badania.parp.gov.pl, dostęp: 2017.06.04.

Przedsiębiorstwa sektora MSP znacząco różnią się od dużych przedsiębiorstw. Ma to przełożenie na stosowanie przez nie rozwiązań korzystających z konceptu tożsamości cyfrowej oraz ich jakość.

Anna Michna, Anna Męczyńska i Roman Kmieciak określają szereg cech charakterystycznych dla małych i średnich podmiotów gospodarczych, a wśród nich m.in.[129]:

1. Ubogie zasoby finansowe – oznaczają z jednej strony małe budżety na zabezpieczenia, w tym narzędzia uwierzytelnienia, a z drugiej małe rezerwy finansowe na pokrycie szkód z tytułu strat powodowanych incydentem naruszenia bezpieczeństwa. Stąd, skuteczny atak na przedsiębiorstwo może oznaczać utratę płynności finansowej i bankructwo.
2. Ograniczony dostęp do specjalistów – powodowany jest zarówno kwestiami finansowymi jak i postrzeganiem przez osoby zarządzające potrzeby konsultacji. W przypadku zagadnień związanych z bezpieczeństwem oznacza to, że przedsiębiorcy mogą bagatelizować kwestie prawidłowych zabezpieczeń i bazują na wiedzy przypadkowych osób, pracowników lub właściciela. Przekłada się to na dobór i konfigurację sprzętu i oprogramowania, szkolenia, dobór i podnoszenie kompetencji pracowników oraz doskonalenie zabezpieczeń.
3. Brak planów strategii rozwoju – obejmujących także długoterminową realizację wizji zapewnienia bezpieczeństwa systemom informatycznym. Oznacza to, że pewne decyzje mogą być podejmowane ad hoc, a sam system może być złożony z elementów dobranych przypadkowo.
4. Silna pozycja i duże znaczenie osoby zarządzającej, która zwykle pełni rolę właściciela i lidera. Jest ona zwykle mocno zaangażowana w pracę i podejmuje nieskrępowane decyzje, co ma swoje dobre i złe strony. Właściciel posiada szerokie kompetencje w wielu dziedzinach, ale niekoniecznie związanych z nowoczesnymi technologiami. Od jego świadomości zagrożeń, zaangażowania i przekonań zależy wdrożenie nowych rozwiązań np. uwierzytelnień biometrycznych[130]czy rozwiązań analityki biznesowej[131]. Od przywództwa zależy również budowanie

[129] Michna, A., Męczyńska, A., Kmieciak, R. (2011). *Niewykorzystywane źródła przewagi konkurencyjnej MSP*. Zarządzanie i Edukacja nr 78/ 2011, s. 46.

[130] Michna, A., Męczyńska, A., Kmieciak, R. (2011). *Małe i średnie przedsiębiorstwa wobec wyzwań współczesnej gospodarki.* W: Knosala, R., red. Komputerowo zintegrowane zarządzanie. T. 2. Opole: Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją, s. 109.

[131] Olszak, C.M., Ziemba, E. (2012). *Critical Success Factors for Implementing Business Intelligence Systems in Small and Medium Enterprises on the Example of Upper Silesia, Poland*. Interdisciplinary Journal of Information, Knowledge & Management, Vol. 7, s. 129–150.

pozytywnego klimatu w przedsiębiorstwie[132], co przekłada się m.in. na powodzenie wdrożenia nowych rozwiązań.

Mimo, iż przedsiębiorstwa mogą działać na rynku lokalnym, (choć często nowe technologie, a w szczególności Internet stają się dla nich swoistą bramą na cały świat[133]), to zagrożenia, którym muszą stawić czoła są globalne. Niestety sektor staje się coraz bardziej atrakcyjnym łupem dla cyberprzestępców[134]. Co więcej, głównym motywem atakujących jest kradzież środków finansowych oraz kradzież tożsamości cyfrowej.[135]

Zapewnienie bezpieczeństwa zasobom, a w szczególności danym osobowym jest dla przedsiębiorstw sektora MSP dużym wyzwaniem. Od 25 maja 2018 roku obowiązują nowe wytyczne Unii Europejskiej (rezolucja RODO) dotyczące zasad przetwarzania danych osobowych. Wdrożenie wymaganych rozwiązań jest szczególnie problematyczne dla małych i średnich przedsiębiorstw[136] z uwagi na potrzebę specjalistycznego doradztwa na etapie projektowania rozwiązań (*Privacy by Design*), wymogu przeprowadzenia analizy ryzyka utraty prywatności (*Privacy Impact Assesment*) oraz sporządzeniu planu reagowania na incydent naruszenia bezpieczeństwa (*Breach Response Plan*). Zrealizowanie tych zadań wymaga wysokich kompetencji w zakresie cyberbezpieczeństwa.

[132] Paliszkiewicz, J., Gołuchowski, J., Koohang, A. (2015). *Leadership, trust, and knowledge management in relation to organizational performance: Developing an instrument.* Online Journal of Applied Knowledge Management, Vol. 3 Issue 2, s. 19. Online: http://www.iiakm.org/ojakm/articles/2015/volume3_2/OJAKM_Volume3_2pp19-35.pdf.

[133] Mullins, R. i inni (2007). *A Web Based Intelligent Training System for SMEs.* Electronic Journal of e-Learning, Vol. 5, No 1, s. 39─48. Online: *www.ejel.org /issue/download.html?idArticle=29*.

[134] *Sektor MŚP będzie coraz bardziej atrakcyjnym i zyskownym łupem dla hakerów* (2016). Online: http://interaktywnie.com/biznes/newsy/bezpieczenstwo/sektor-msp-bedzie-coraz-bardziej-atrakcyjnym-i-zyskownym-lupem-dla-hakerow-253102, 2016.04.22.

[135] *Ataki na klientów banków nasilają się także w sektorze MŚP* (2016). Online: http://www.polskatimes.pl/strefa-biznesu/pieniadze/a/ataki-na-klientow-bankow-nasilaja-sie-takze-w-sektorze-msp,10154496/, 2016.04.21.

[136] Kosior, A. (2017) *RODO - niejasne wytyczne, kary rzędu nawet 20 mln euro. Kto zyska na nowej unijnej rezolucji?* Dziennik internautów. Biznes i prawo. Online: http://di.com.pl/rodo-niejasne-wytyczne-kary-rzedu-nawet-20-mln-euro-kto-zyska-na-nowej-unijnej-rezolucji-56984, 2017.03.24.

3.2. Zagrożenia związane z korzystaniem z narzędzi teleinformatycznych w kontekście tożsamości cyfrowych

3.2.1. Przesłanki do ochrony systemów informatycznych

Duże znaczenie stosowania narzędzi ICT w działalności przedsiębiorstwa powodowane jest przez fakt powszechności stosowania systemów informatycznych oraz znacznej wirtualizacji procesów przedsiębiorstwa. Przykładem procesów biznesowych realizowanych z użyciem narzędzi ICT jest wirtualizacja dokumentacji (np. faktur)[137] czy wykorzystywanie platform sprzedażowych. Przyczyną tego stanu rzeczy są m.in. wygoda, kwestie finansowe lub wymogi interesariuszy (np. przedsiębiorstw partnerskich), skutkiem natomiast uzależnienie pracy przedsiębiorstwa od prawidłowości działania systemu informatycznego.

Pandemia SARS-CoV-2 spowodowała pogłębienie tej zależności. Od marca 2020 nastąpiło masowe przejście na pracę zdalną nie tylko pracowników biurowych, ale także tych, którzy do tej pory korzystali z niej sporadycznie lub wcale (psycholodzy, sprzedawcy nieruchomości, wykładowcy)[138]. Spowodowało to znaczący wzrost zagrożeń związanych z transmisją danych poza organizację[139].

Brak możliwości korzystania z zasobów systemów informatycznych niesie za sobą poważne konsekwencje, które mogą doprowadzić do poważnego zaburzenia funkcjonowania czy nawet bankructwa organizacji[140]. Stanowi to istotną przesłankę do zabezpieczenia systemów informatycznych przed potencjalnymi zagrożeniami[141].

Kolejną kwestią, wpływającą na potrzebę ochrony systemów informatycznych jest fakt, że w jednym miejscu gromadzone są cenne dane w formie łatwej (bez ograniczeń związanych z gromadzeniem, czasochłonną selekcją czy transportem)

---

[137] Według raportu dotyczącego zrządzania bezpieczeństwem informacji (Góra, J. (2013). *Raport. Efektywne zarządzanie bezpieczeństwem informacji.* Online: https://www.us.edu.pl/sites/all/files/www/wiadomosci/pliki/RAPORT2013.pdf, dostęp: 2017.06.04) w 2013 r. tylko 43% dokumentacji miało formę papierową.

[138] Dolot A. (2020). Wpływ pandemii COVID-19 na pracę zdalną – perspektywa pracownika. E-mentor nr 1 (83) / 2020, s. 35–43.

[139] *Globalne cyberzagrożenia związane z pandemią* (2020). Online: https://www2.deloitte.com/pl/pl/pages/technology/articles/globalne-cyberzagrozenia-zwiazane-z-epidemia.html, dostęp: 30.11.2020.

[140] Góra, J. (2013). *Raport. Efektywne zarządzanie bezpieczeństwem informacji.* Online: https://www.us.edu.pl/sites/all/files/www/wiadomosci/pliki/RAPORT2013.pdf, dostęp: 2017.06.04, s. 21.

[141] *4. edycja badania stanu bezpieczeństwa informacji w Polsce. Ochrona biznesu w cyfrowej transformacji czyli 4 kroki do bezpieczniejszej firmy.* PWC. Online: https://www.pwc.pl/pl/pdf/ochrona-biznesu-w-cyfrowej-transformacji-pwc.pdf, dostęp: 2017.06.04, s. 10.

do przesyłu za pomocą będącego w powszechnym użyciu Internetu lub skopiowania na dużej pojemności urządzenia przenośne.

Ogólnym celem zabezpieczenia systemu jest zatem zapewnienie jego płynnej pracy oraz aktywna i pasywna ochrona przed niepowołanym dostępem czy szkodliwą ingerencją w system informatyczny (np. niewłaściwe przetwarzanie danych).

Elementy składające się na systemy informatyczne (oprogramowanie, urządzenia) nie są ani idealne ani niezawodne, stąd zapewnienie im bezpieczeństwa powinno uwzględniać kwestie wynikające z naturalnej skłonności urządzeń do psucia się takie jak robienie backupów (tworzenie kopii pełnych, przyrostowych lub różnicowych[142]), bieżąca konserwacja urządzeń i oprogramowania, stosowanie zasilaczy UPS, macierzy dyskowych do przechowywania danych itp.[143] Drugą kwestią związaną z zapewnieniem systemom bezpieczeństwa jest ochrona przed zagrożeniami, których źródłem są ludzie[144]. Szacuje się, że za 79% incydentów naruszenia bezpieczeństwa odpowiadają aktualni pracownicy.[145]

Według raportu z czwartej edycji badań stanu bezpieczeństwa informacji w Polsce, w roku 2016, 96% firm doświadczyło minimum 50 ataków na systemy informatyczne. Mimo to tylko 11% badanych przedsiębiorstw wdrożyło identyfikację wrażliwych zasobów, 72% nie prowadzi działań w tym zakresie, a 58% nawet nie rozważa podjęcia takiego działania.[146]

Mimo, iż tylko 17% przedsiębiorstw kategorycznie nie zezwala na korzystanie w pracy z własnych urządzeń, tylko 16% wymaga zainstalowania na tych urządzeniach rozwiązań typu MDM (*Mobile Device Management*).[147]

Wśród głównych skutków, które niosą za sobą incydenty naruszenia bezpieczeństwa respondenci tego badania wymieniają: narażenia na ryzyko prawne / proces sądowy (35%), straty finansowe (35%), utrata klientów (30%) oraz wyciek korespondencji firmowej (25%).[148]

---

[142] Tadeusiewicz, R. (2010). *Zagrożenia w cyberprzestrzeni*. Nauka 4.2010. s. 31–42.

[143] Tamże.

[144] Sapronov, K. *Czynnik ludzki a bezpieczeństwo informatyczne.* Securelist. Online: http://securelist.pl/threats/5480,czynnik_ludzki_a_bezpieczenstwo_informatyczne.html dostęp: 2017.06.04.

[145] *4. edycja badania stanu bezpieczeństwa informacji w Polsce. Ochrona biznesu w cyfrowej transformacji czyli 4 kroki do bezpieczniejszej firmy*. PWC, s. 16. Online: https://www.pwc.pl/pl/pdf/ochrona-biznesu-w-cyfrowej-transformacji-pwc.pdf, dostęp: 2017.06.04.

[146] Tamże, s. 19.

[147] Tamże, s. 10.

[148] Tamże, s. 16.

3.2.2. Klasyfikacje zagrożeń

Generalnie istnieje wiele podziałów zagrożeń systemów informatycznych. Ze względu na źródło można wyróżnić zagrożenia[149]:

- wewnętrzne, czyli losowe lub celowe uszkodzenie nośników lub utrata dostępu do usług sieciowych, czego klasycznym przykładem jest sabotaż zwolnionego z pracy pracownika, któremu nie odebrano praw dostępu do systemu;
- zewnętrzne, czyli związane z działaniami prowadzonymi przez osoby trzecie, użytkowników sieci lub systemem informatycznym, takie jak cyberatak;
- fizyczne, czyli konsekwencje awarii i katastrof.

Z uwagi na pochodzenie, zagrożenia podzielono na[150]:

- losowe, takie jak klęski żywiołowe, katastrofy lub wypadki, dotyczące sprzętu (nośniki i infrastruktura),
- tradycyjne zagrożenia informatyczne, czyli szpiegostwo, działalność dywersyjna lub sabotażowa,
- technologiczne, związane gromadzeniem, przechowywaniem, przetwarzaniem i przesyłem danych w sieciach,
- związane z niedostatecznymi rozwiązaniami organizacyjnymi i strukturalnymi.

Niektórzy autorzy wskazują, że skutki zagrożeń mogą być uciążliwe (np. spam) lub niosące poważne konsekwencje (np. finansowe) [151].

Zagrożenia można też podzielić też na losowe, będące dziełem przypadku lub ingerencji sił wyższych (np. związane z awarią urządzeń spowodowaną skokiem napięcia), intencjonalne, czyli będące skutkiem świadomych zamierzeń oraz nieintencjonalne, których przyczyną nie było działanie zamierzone.

Wśród zagrożeń intencjonalnych warto zwrócić uwagę na fakt, że szkodliwa działalność może być powodowana przez osobę z zewnątrz (np. hakera) lub samego pracownika czy też byłego pracownika. Motywacją do przeprowadzenia ataków może być np.[152]:

- motywacja finansowa, czyli np. kradzież tajemnic przedsiębiorstwa w celu ich spieniężenia,

---

[149] Opracowanie własne na podstawie: Król, K. (2015) *Organizacyjne aspekty zarządzania bezpieczeństwem danych z perspektywy zagrożeń phishingu*. Organizacja i Zarządzanie, Wyd. Kwartalnik naukowy 2 (30), Politechniki Śląskiej, s. 23

[150] Tamże, 23–24.

[151] Tamże, s. 24.

[152] Góra, J. (2013). *Raport. Efektywne zarządzanie bezpieczeństwem informacji.* s. 21. Online: https://www.us.edu.pl/sites/all/files/www/wiadomosci/pliki/RAPORT2013.pdf, dostęp: 2017.06.04.

- odwet ze strony byłego pracownika, chęć wyrządzenia dotkliwej szkody np. sabotaż produkcji.
- nieuczciwa konkurencja np. kradzież lub usunięcie bazy danych klientów.

W przypadku działania nieintencjonalnego zawodzą procedury (np. brak instrukcji działania na wypadek zaistnienia incydentu, brak przeszkolenia, nieodpowiedni dobór pracowników itp.), ludzie (np. brak staranności, zaangażowania w pracę, roztargnienie itp.) lub następuje niefortunny zbieg okoliczności.

Wśród sprawców zagrożeń można wymienić[153]:

1. Hakera, crackera motywowanych pobudkami osobistymi, chęcią podjęcia wyzwania, buntem. Stosują socjotechniki, wtargnięcia systemowe i nieuprawniony dostęp do systemu.
2. Przestępcę komputerowego motywowanego korzyścią pieniężną lub wandalizmem, wykorzystuje on oszustwa, przekupstwa, fałszowanie typu spoofing i wtargnięcia do systemu.
3. Terrorystę, którego pobudkami są szantaż, wykorzystanie, wandalizm i zemsta. Wykorzystuje w tym celu bomby, ataki na system, penetrację i manipulację systemu oraz prowadzi wojny informacyjne.
4. Szpiega przemysłowego, który dąży do osiągnięcia korzyści konkurencyjnych lub prowadzi szpiegostwo ekonomiczne na zlecenie innych przedsiębiorstw, obcych rządów lub agencji rządowych. Jego metodami są kradzież informacji, naruszenie prywatności osobistej, socjotechniki, penetracja systemu i nieuprawniony dostęp do niego oraz wykorzystywanie ekonomiczne.
5. Pracownika, który z jednej strony może być źle wykształcony i popełnić niezamierzony błąd, z drugiej zaś, może być rozczarowany lub nieuczciwy. Wtedy kieruje nim ego, pragnienie zemsty, korzyść pieniężna lub chęć przeprowadzenia wywiadu. Czasem motywacją bywa też ciekawość. Zagrożenie powodowane przez pracownika to: wtargnięcie, nadużycie komputerowe, nieuprawniony dostęp do systemu, napaść na pracownika, szantaż, przeglądanie informacji niejawnych, oszustwa i kradzieże, wprowadzanie fałszywych lub uszkodzonych danych, przechwytywanie informacji, sprzedaż danych osobowych, powodowanie błędów systemu, włamań lub sabotaż.

Zdarzenia będące wynikiem działań wymienionych uprzednio osób można podzielić na[154]:

1. Oszustwa wewnętrzne (działania nieuprawnione; kradzieże i oszustwa).
2. Oszustwa zewnętrzne (kradzież i oszustwo; bezpieczeństwo systemów).

---

[153] Wołowski, F., Zawiła-Niedźwiecki, J. (2012). *Bezpieczeństwo systemów informacyjnych: praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*. Kraków; Warszawa: edu-Libri, s. 83.

[154] Tamże, s. 85–86.

3. Praktyka kadrowa i bezpieczeństwo pracy (stosunki pracownicze; bezpieczeństwo środowiska pracy; podziały i dyskryminacja).
4. Klienci, produkty i praktyka biznesowa (obsługa klienta, ujawnianie informacji o klientach, zobowiązania względem klientów; niewłaściwe praktyki biznesowe lub rynkowe, wady produktów; klasyfikacja klientów i ekspozycje; usługi doradcze).
5. Uszkodzenie aktywów (klęski żywiołowe i inne zdarzenia).
6. Zakłócenia działalności i błędy systemów (systemy).
7. Dokonywanie transakcji, dostawa oraz zarządzanie procesami (wprowadzenie danych do systemu, wykonywanie, rozliczanie i obsługa transakcji; monitorowanie i sprawozdawczość; dokumentacja dotycząca klienta; zarządzanie zasobami klienta; uczestnicy procesów niebędący klientami; sprzedawcy i dostawcy).

3.2.3. Tożsamość cyfrowa jako obiekt ataku cyberprzestępców

Zagrożenie związane z tożsamością cyfrową jest ściśle związane z jej rolą w systemach informatycznych, jako swoistego narzędzia, który daje możliwość dostępu, przetwarzania, usuwania danych i zmiany konfiguracji systemu. Obiekty, które biorą udział w procesie uzyskiwania dostępu, czyli: użytkownik, narzędzia uwierzytelnienia, urządzenia, kanał komunikacyjny oraz system informatyczny mogą stać się źródłem ataku[155].

Użytkownik tożsamości cyfrowej, czyli osoba, która dokonuje procesu uwierzytelnienia może być przedmiotem ataków, których celem jest uzyskanie danych lub przedmiotów koniecznych do przeprowadzenia uwierzytelnienia, czyli:

1. Ataki phishingowe, polegające na próbie wyłudzenia danych za pomocą fałszywych stron internetowych lub e-maili. Zwykle użytkownik otrzymuje alarmującą wiadomość, skłaniającą go do kliknięcia w umieszczony w wiadomości link, przekierowujący go na fałszywą stronę logowania. Jeśli użytkownik przeprowadzi proces uwierzytelnienia tj. poda swój login i hasło, numer PIN lub hasło jednorazowe, dane te są wykorzystywane do włamania. Tego typu ataki stanowią najczęstszy incydent naruszenia bezpieczeństwa.[156]
2. Instalowanie złośliwego oprogramowania (*Malware*), wskutek skłonienia użytkownika do np. otwarcia załącznika wiadomości lub kliknięcia w link

[155] Szyjewski, G. (2011). *Wykorzystanie modeli procesów biznesowych BPMN 2.0 do identyfikacji potrzeb zdalnego uwierzytelniania*. Metody Informatyki Stosowanej Nr 3/2011 (28), s. 167–178.

[156] *4. edycja badania stanu bezpieczeństwa informacji w Polsce. Ochrona biznesu w cyfrowej transformacji czyli 4 kroki do bezpieczniejszej firmy*. PWC. Online: https://www.pwc.pl/pl/pdf/ochrona-biznesu-w-cyfrowej-transformacji-pwc.pdf, dostęp: 2017.06.04, s. 15.

powodujący instalację software'u (najczęściej to programy szpiegujące, trojany, *keyloggery*).

3. Kopiowanie przedmiotów uwierzytelniających (*Skimming*) oraz podejrzenie numeru PIN, to rodzaj przestępstwa, którego celem jest uzyskanie zarówno przedmiotu jak i zabezpieczającego ją numeru PIN po to, by uzyskać dostęp do np. konta bankowego[157]. Atak ten wykorzystuje brak ostrożności użytkownika oraz dwa urządzenia: specjalnej nakładki kopiującej (*Skimmer*) i kamery, odczytującej numer PIN z ruchu palców. Skimmer zawiera czytnik i dekoder zapisu magnetycznego, który np. podczas wkładania karty płatniczej do bankomatu (a dokładniej do specjalnej nakładki umieszczonej na bankomacie) kopiuje numer karty, jej datę ważności, informację o ew. posiadaniu chipu oraz kod serwisowy niezbędny do przeprowadzenia transakcji. Tak pozyskane dane mogą posłużyć do utworzenia tzw. białej karty (duplikatu karty) lub użyte do transakcji internetowych bez umieszczania na fizycznym nośniku.
4. Ataki socjotechniczne, czyli ataki wykorzystujące socjotechniki (manipulację użytkownika w celu osiągnięcia korzyści przez atakującego). Takim atakiem jest wspomniany uprzednio *phishing*. Często jednak atak jest wieloetapowy. Napastnik uzyskuje informacje cząstkowe, by za ich pomocą uwiarygodnić przybraną tożsamość (np. pracownika GUSu) i wskutek podszycia się (czyli przybierania fałszywej tożsamości) uzyskać chronioną informację (np. dotyczącą systemu zabezpieczeń w przedsiębiorstwie), która może służyć do dokonania profilowanego ataku na system informatyczny[158].

W roku 2019 największym zagrożeniem były phishing i pharming. W badaniach Eurostatu w 2019 r. odpowiednio 30% i 15% użytkowników zadeklarowało doświadczenie tej formy wyłudzenia danych[159].

Napastnik może również uzyskać dane pozwalające na uzyskanie dostępu jako osoba uprawniona atakując narzędzie uwierzytelnienia poprzez:

1. Poznanie hasła. W tym celu może przeprowadzić:
    - atak siłowy (*Brute Force*) – próba zalogowania się z wykorzystaniem haseł generowanych jako wszystkie możliwe kombinacje znaków,
    - atak słownikowy (*Dictionary Attack*), czyli próba logowania się z wykorzystaniem popularnych sekwencji, słów i typowych modyfikacji haseł np. zamiana znaku o na 0,

[157] Opitek, P. (2015). *Przestępstwo skimmingu*. Prokuratura i prawo 11, s. 66–82.

[158] Mitnick, K.D., Simon, W. (2003). *Sztuka podstępu. Łamałem ludzi, nie hasła*. Wyd. I. Gliwice: Wydawnictwo Helion.

[159] *Digital Economy and Society Index Report 2020 – Use of Internet Services* (2020). Online: https://ec.europa.eu/digital-single-market/en/use-internet-and-online-activities, dostęp: 30.11.2020.

- próbę odgadnięcia hasła. W tym celu posiłkuje się wiedzą o użytkowniku, jego danymi osobowymi, ważnymi datami, imionami, przedmiotami czy wydarzeniami,
- próbę podejrzenia hasła. Ta metoda opiera się głównie na zaniedbaniach użytkownika (np. zapisywanie haseł na karteczkach trzymanych pod klawiaturą, czy wręcz naklejonych przy ekranie, podejrzenie hasła wpisywanego przez użytkownika podczas logowania), choć nie jest to regułą (np. próba przechwycenia hasła umieszczonego w sejfie).

2. Przechwycenie kodu jednorazowego lub klucza prywatnego przedmiotu, który pozwala na generowanie kolejnych haseł jednorazowych:
   - kradzież przedmiotu i użycie go do celu uzyskania zwykle krótkotrwałego dostępu do zasobów,
   - kradzież przedmiotu, złamanie klucza i niepostrzeżony zwrot przedmiotu właścicielowi. Takie działanie pozwala na dłuższe korzystanie z dostępu do zasobów (użytkowi trudniej jest się zorientować, że padł ofiara ataku),
   - złamanie klucza tokena USB z wykorzystaniem złośliwego oprogramowania.
3. Przechwycenie wzorca biometrycznego:
   - włamanie do systemu i kradzież przechowywanych danych z centralnego repozytorium,
   - wykonanie imitacji badanej cechy[160] np. sztucznego odcisku palca (np. wydrukowanie zdjęcia w skali 1:1, nierówności nałożonego barwnika imitują linie papilarne).

Cyberprzestępca może zaatakować proces uwierzytelnienia wykorzystując słabości kanału komunikacyjnego, czyli sieci kablowej lub bezprzewodowej na różne sposoby np.:

- wykorzystywanie programów podsłuchujących (*Sniffer*) do przechwycenia haseł,
- dokonywanie ataków z ukrytym pośrednikiem (*Man In The Middle*, MITM), czyli nawiązanie kontaktu z dwoma komunikującymi się stronami tak, by samemu być niewidocznym (podszycie się pod obie strony) a przechwytywać cały strumień danych,
- tzw. zatruwanie tablic ARP (*Adress Resolution Protocol spoofing*), czyli przekierowywanie strumienia danych na inne urządzenie (np. komputer atakującego).

[160] Tomala, L. (2010). *Prof. Pacut o tym, czy można oszukać urządzenia biometryczne*. PAP Nauka w Polsce. Online: http://naukawpolsce.pap.pl/aktualnosci/news, 374692,prof-pacut-o-tym-czy-mozna-oszukac-urzadzenia-biometryczne.html, dostęp: 2017.06.04.

Atakujący może również wykorzystać słabości urządzenia (zarówno software'u i hardware'u) które uzyskuje dostęp do zasobów tj. odszukiwanie luk i niezabezpieczonych tzw. tylnych drzwi (*Backdoor*). Przykładem jest wykorzystanie oprogramowania sprzętowego dla procesora wykorzystywanego do obsługi protokołów kontrolnych OMA-DM (*Open Mobile Alliance Device Management*)[161] lub fakt, że brak odpowiedniego zabezpieczenia urządzeń obsługujących ruch w sieci jest powszechny[162]. Wraz ze wzrostem popularności bankowości mobilnej nasila się zjawisko tzw. sim-swappingu, czyli wyrabiania duplikatu karty SIM w celu przejęcia dostępu do konta bankowego.

System informatyczny może być zaatakowany przez. złośliwe oprogramowanie, czyli np.: wirusy, robaki. Aby złośliwe oprogramowanie pojawiło się w systemie komputerowym musi zaistnieć jedna z poniższych sytuacji:

- niedostateczna techniczna i fizyczna ochrona systemu np. brak zainstalowanego programu antywirusowego, nieaktualizowane oprogramowanie;
- wadliwe procedury lub niedopracowanie systemu zabezpieczeń np. brak wymogów co do haseł, brak systemu zarządzania urządzeniami mobilnymi (*Mobile Device Management*, MDM) przy praktyce korzystania z własnych urządzeń przez pracowników (*Bring Your Own Device*, BYOD)[163];
- nieintencjonalne, przypadkowe zainfekowanie systemu przez pracownika np. poprzez użycie zawirusowanego pendrive'a (jest to jedna z najczęstszych przyczyn występowania incydentów naruszenia bezpieczeństwa)[164];
- nieintencjonalne zainfekowanie systemu przez pracownika, ale wskutek przeprowadzonego ataku przez cyberprzestępcę np. otworzenie zainfekowanego pliku przesłanego e-mailem;
- intencjonalne zainfekowanie przez pracownika np. szpiegostwo przemysłowe, sabotaż, zemsta itp.;
- intencjonalne zainfekowanie przez osobę, która nie jest pracownikiem np. podszycie się pod pracownika po złamaniu hasła.

---

[161] *Jak po cichu zhackować dowolnego smartphona (oraz inne urządzenia komunikujące się po GSM)?* (2014). Niebezpiecznik. Online: https://niebezpiecznik.pl/post/jak-zhackowac-dowolnego-smartphona-oraz-inne-urzadzenia-komunikujace-sie-po-gsm/, 2014.08.13.

[162] Kaczmarek, S. (2016). *Bezpieczna firma w cyberprzestrzeni*. Online: http://it-filolog.pl/bezpieczna-firma-w-cyberprzestrzeni, 2016.02.15.

[163] Sarzyński, K. (2016). *Bring your own device (BYOD) – szansa czy zagrożenie dla przedsiębiorstwa?* Organizacja i Zarządzanie, Nr 4(36). Gliwice: Wydawnictwo Politechniki Śląskiej, s. 67–80.

[164] *4. edycja badania stanu bezpieczeństwa informacji w Polsce. Ochrona biznesu w cyfrowej transformacji czyli 4 kroki do bezpieczniejszej firmy*. PWC, s. 15. Online: https://www.pwc.pl/pl/pdf/ochrona-biznesu-w-cyfrowej-transformacji-pwc.pdf, dostęp: 2017.06.04.

Podczas pandemii SARS-CoV-2 w sposób istotny wzrosła zarówno cyberprzestępczość, jak i jej znaczenie. Październikowy raport Europolu IOCTA 2020 wskazuje nasilenie działań przestępczych w Internecie, a wśród największych problemów wymienia inżynierię społeczną i szkodliwe oprogramowanie. Coraz częstsze są także przestępstwa typu sim-swap.[165]

3.3. Normy i przepisy prawne regulujące kwestie tożsamości cyfrowej

3.3.1. Przyczyny wprowadzenia regulacji

Główną przesłanką do regulacji kwestii związanych z tożsamością cyfrową jest ochrona praw i wolności osób (a w szczególności poszanowanie sfery osobistej oraz prywatności) w realiach współczesnego świata. Na istotność regulacji kwestii związanych z danymi osobowymi wpłynęły następujące czynniki:

1. Powszechność wykorzystywania komputera, Internetu, szerokiej gamy serwisów, które prowadzą do wirtualizacji pewnych aspektów działalności człowieka i zostawiają „ślady" w Internecie w postaci danych, które coraz częściej można przypisać do konkretnej tożsamości cyfrowej[166].
2. Możliwość pozyskania, gromadzenia i przechowywania praktycznie w nieskończoność danych cząstkowych, które, dzięki wzajemnym powiązaniom, składają się na coraz dokładniejszy obraz jednostki korzystającej z danej tożsamości cyfrowej.
3. Silny rozwój federacyjnej tożsamości cyfrowej, skutkujący kumulacją danych cząstkowych przez dominujących dostawców tożsamości.
4. Zwiększenie możliwości obliczeniowych oraz nowe możliwości obróbki danych, umożliwiające tworzenie np. profili, przewidywanie zachowań konsumenckich itp.
5. Liczne możliwości wykorzystania danych oraz profili, szczególnie w obszarze gospodarczym (np. w marketingu, ubezpieczeniach), ale też związanym z działalnością administracji rządowej, co oznacza, że dane te mają wymierną wartość i same w sobie mogą stanowić przedmiot handlu.
6. Możliwość monetyzacji danych osobowych pociąga za sobą ryzyko działań o charakterze przestępczym, takich jak kradzież lub wyłudzenie danych osobowych (a także innych danych).

[165] *IOCTA 2020. Internet organized crime. Threat assessment* (2020). Europol. Online: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020, dostęp: 15.12.2020.

[166] *Handel danymi osobowymi* (2016). 4ITSecurity. Online: http://4itsecurity.pl/blog/2-Dane-osobowe/87-handel-danymi-osobowymi.html, 2016.08.25.

Podsumowując, dzięki rozwojowi technologii ICT możliwe jest gromadzenie i przetwarzanie danych konkretnych osób w sposób powszechny i kompleksowy. Stąd, regulacje dotyczą:

1. Danych osobowych, rozumianych jako „*wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej*."[167]
2. Przetwarzania danych osobowych, rozumianych jako „*jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych*".[168]

Szczególnemu uregulowaniu podlegają tzw. dane wrażliwe, które można podzielić na następujące kategorie[169]:

1. Dane ujawniające: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne lub przynależność wyznaniową, partyjną albo związkową.
2. Dane o: stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym.
3. Dane dotyczące: faktu skazania, orzeczeń o ukaraniu i mandatów karnych lub innych orzeczeń wydanych w postępowaniu sądowym czy administracyjnym.

3.3.2. Źródła prawa

Podstawą prawa międzynarodowego w kwestii uregulowań dotyczących danych osobowych stanowią m.in.: Powszechna Deklaracja (UNESCO) w sprawie genomu ludzkiego i praw człowieka z dnia 11 listopada 1997 r., rezolucja 45/95 Zgromadzenia Ogólnego ONZ z 26 czerwca 1985 r., Rekomendacja Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z dnia 23 września 1980 r., w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami oraz Rezolucja 34/169 Zgromadzenia Ogólnego ONZ.

W ramach regulacji Unii Europejskiej podstawą prawną jest Dyrektywa 95/46/EC Parlamentu Europejskiego i Rady z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych oraz dalsze akty prawne np. zestawy standardowych klauzul umownych: 2001/497/WE z dnia 15 czerwca 2001 r., 2004/915/WE z dnia 27 grudnia 2004 r. czy 2010/87/UE z dnia 5 lutego 2010 r. Od dnia 25 maja 2018 r. obowiązuje Rozporządzenie Parlamentu Europejskiego

[167] *Dz.U. 1997 Nr 133 poz. 883 USTAWA z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, art. 6 ust. 1.
[168] Tamże, art. 7 ust. 2.
[169] Tamże, art. 21.1.

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, w którym uregulowane zostały m.in. kwestie związane z tożsamością cyfrową[170]: prawo do bycia zapomnianym, ułatwienia w cyfrowym przepływie danych osobowych oraz uregulowanie zasad profilowania, wymóg udzielenia zgody na przetwarzanie danych osobowych, ze szczególnym uwzględnieniem dzieci, obowiązek uwzględniania bezpieczeństwa danych na etapie projektowania usług lub produktów, zmiany statusu Administratora Bezpieczeństwa Informacji oraz obowiązek zawiadamiania GIODO o incydentach naruszenia bezpieczeństwa.

Krajową podstawę prawną ochrony danych osobowych tworzą akty dotyczące poszanowania prywatności człowieka (np. Konstytucja w art. 30, 31, 41, 47, 50, 57), a także dedykowane przepisy, w szczególności Ustawa o ochronie danych osobowych, której celem jest określenie zasad przetwarzania danych osobowych przy użyciu komputera. Inne przepisy prawne regulujące kwestie związane z tożsamością cyfrową to m.in.:

1. Wspomniana już Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
2. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych.
3. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym.
4. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
5. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej.
6. Rozporządzenia m.in. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
7. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.
8. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych.
9. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

[170] *Nowe przepisy o ochronie danych osobowych* (2017). 4ITSecurity. Online: http://4itsecurity.pl/blog/2-Dane-osobowe/90-nowe-przepisy-o-ochronie-danych-osobowych.html, 2017.01.07.

10. Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych
11. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych.
12. Rozporządzenie Ministra Administracji i Cyfryzacji z 29 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji.
13. Rozporządzenie Ministra Administracji i Cyfryzacji z 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji przez administratora bezpieczeństwa.

Organem odpowiedzialnym za stan ochrony danych osobowych w Polsce jest Generalny Inspektor Ochrony Danych Osobowych (GIODO)[171], który oprócz funkcji doradczych, kontrolnych czy prowadzenia rejestrów zbiorów danych osobowych, nadzoruje zgodność praktyki z przepisami prawa i w razie potrzeby reaguje na nieprzestrzeganie prawa.

Skutki prawne wynikające z niepodporządkowania się wymogom można podzielić na[172]:

- Administracyjne (finansowe) – grzywna nakładana decyzją administracyjną Generalnego Inspektora w przypadku niewykonania przez Administratora danych osobowych decyzji Generalnego Inspektora, w wysokości do 10.000 zł dla osoby fizycznej i max. 50.000 zł dla osoby prawnej oraz jednostki organizacyjnej nieposiadającej osobowości prawnej.
- Karne – w postaci grzywny, kary ograniczenia lub pozbawienia wolności (1–3 lat).

3.3.3. Źródła standardów

Oprócz dokumentów regulujących kwestie związane z dostępem do danych (wspomniane dyrektywy unijne, ustawy, obwieszczenia, zarządzenia i rozporządzanie RM), których spełnienie należy do obowiązków osób zarządzających przedsiębiorstwem, wyróżnić można również wytyczne, które mogą być stosowane na zasadzie dobrowolności:

- normy – opracowane przez Międzynarodową Organizację Normalizacyjną ISO (np. PN-ISO/IEC 1779:2007. Praktyczne zasady zarządzania bezpieczeństwem informacji, Wymagania, PKN, Warszawa; PN-ISO/IEC 27001:2007, Technika informatyczna – Techniki bezpieczeń-

[171] *Dz.U. 1997 Nr 133 poz. 883 USTAWA z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, art. 12.

[172] Tamże, art. 49–54a.

stwa – Systemy zarządzania bezpieczeństwem informacji, Wymagania, PKN, Warszawa) lub przez Polski Komitet Normalizacji,
- inne zalecenia lub dobre praktyki publikowane przez organizacje związane z rynkiem IT czy zajmujące się kwestiami bezpieczeństwa lub poufności danych np. zalecenia firmy Microsoft lub Kaspersky.

Standardy mogą przyjąć różną postać: od ogólnych (np. Rezolucja Madrycka z dn. 5 listopada 2009 r.), po szczegółowe (PN-ISO/IEC 1779:2007) w zależności od tego, czy wyznaczają kierunki działań, czy określają wymagania do spełnienia w celu uzyskania konkretnych korzyści (np. certyfikatu). Ich wpływ ma różny zasięg: od wpływania na prawo krajowe (np. wspomniana Rezolucja Madrycka), po sugestie opracowane na potrzeby konkretnego przedsiębiorstwa.

Zalecenia dla przedsiębiorstw (tzw. dobre praktyki), publikowane przez organizacje z branży IT lub bezpieczeństwa informacji, formułowane są na podstawie monitoringu zagrożeń, czyli uwzględniają tendencje i kierunki rozwoju cyberprzestępczości, jak również nowe rozwiązania, w tym prawne, czy ogólny postęp technologii. Wskazują one słabe punkty (np. brak świadomości zagrożenia w MSP), największe zagrożenia (np. eskalację danego typu wirusów) czy sposoby na zapewnienie bezpieczeństwa zasobów w ramach nowych produktów czy technologii (np. chmura obliczeniowa, *Cloud Computing*).

3.4. Uwarunkowania zarządzania tożsamością cyfrową pracowników

Uwarunkowania związane z tożsamościami cyfrowymi wykorzystywanymi do zapewnienia bezpieczeństwa zasobów w przedsiębiorstwie podzielono i omówiono w następujących aspektach:
- rozwiązania organizacyjne,
- czynnik ludzki.

Na realne bezpieczeństwo tożsamości cyfrowych, a przez to zasobów przedsiębiorstwa, składają się zatem jakość i przestrzeganie procedur, właściwie dobrane i zaimplementowane zabezpieczenia związane ze sprzętem elektronicznym i oprogramowaniem oraz działania pracowników przedsiębiorstwa i osób powiązanych. Ostateczne bezpieczeństwo nie jest jednak średnią z poziomu bezpieczeństwa w tych trzech obszarach. Jego poziom określa tzw. najsłabsze ogniwo, czyli punkt, w którym kompromitacja danych lub dostępu do usług może nastąpić najczęściej lub najłatwiej.

3.4.1. Rozwiązania organizacyjne

Istnieje szereg czynników związanych z odpowiednią organizacją procesów i zasobów przedsiębiorstwa, które wpływają na bezpieczne korzystanie z tożsamości cyfrowej. Głównym narzędziem ochrony zasobów w obszarze organizacji jest wdrożenie systemu zarządzania bezpieczeństwem informacji, określonego

w normie PN-ISO/IEC 27001:2007[173] oraz PN-ISO/IEC 27001:2014-12[174]. Przesłankami do jego utworzenia są zarówno powody zdroworozsądkowe (np. zachowanie przewagi konkurencyjnej), jak i konieczność prowadzenia działalności w zgodzie z przepisami prawa (np. ochrona danych osobowych, akt pracowniczych, tajemnicy bankowej).

Podstawą takiego systemu są[175]:

1. Opracowanie i wdrożenie polityki bezpieczeństwa.
2. Opracowanie i wdrożenie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (a w tym, instrukcji na wypadek postępowania w przypadku naruszenia bezpieczeństwa danych osobowych).
3. Powołanie Administratora Danych Osobowych (ADO).

3.4.1.1. Polityka bezpieczeństwa

Polityka bezpieczeństwa informacji może być rozumiana jako „*zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonej organizacji*."[176] W innym ujęciu jest to „*regulacja wewnętrzna w przedsiębiorstwie, która powinna być jednym z narzędzi służącym właściwemu zabezpieczeniu danych w sposób zapewniający ich ochronę przed nieuprawnionym przetwarzaniem.*"[177] Polityka bezpieczeństwa powinna obejmować działania związane z zabezpieczeniem zarówno informacji przetwarzanej cyfrowo, jak i tradycyjnie.

Celem polityki bezpieczeństwa, jest określenie koniecznych działań, ustanowienie zasad i reguł postępowania, czyli „*zapewnienie przez kierownictwo wytycznych i wsparcia dla działań na rzecz bezpieczeństwa informacji zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami*."[178]

Polityka bezpieczeństwa (podobnie jak instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych) powinna posia-

---

[173] *PN-ISO/IEC 27001:2007*.

[174] *PN-ISO/IEC 27001:2007*.

[175] *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,* par. 3.1.

[176] *PNT-02000: Zabezpieczenia w systemach informatycznych – Terminologia*, PKN, 1998 za: Kaczmarek, A. *Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa.* GIODO. Online: www.giodo.gov.pl/plik/id_p/10212/j/pl/, dostęp: 2017.06.04.

[177] *Polityka bezpieczeństwa informacji.* Online: https://mikroporady.pl/zarzadzanie/item/1610-polityka-bezpieczenstwa-informacji.html, dostęp: 2017.06.04.

[178] *PN-ISO/IEC 27002:2013*.

dać formę pisemną[179], zapisy powinny być konkretne (nie abstrakcyjne), a reguły wyjaśnione i uzasadnione[180]. Sposób prowadzenia oraz zakres dokumentacji określa Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Wspomniana ustawa definiuje poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym (tabela 3.1.).

Tabela 3.1. Charakterystyka poziomów bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym

		Poziom bezpieczeństwa		
		Podstawowy	Podwyższony	Wysoki
Podstawa klasyfikacji	Przetwarzanie danych wrażliwych		x	x
	Podłączenie do Internetu			x
Wymogi	Zabezpieczenie dostępu	x	x	x
	Zapewnienie rozliczalności	x	x	x
	Długość hasła	Min. 6 znaków	Min. 8 znaków	Min. 8 znaków
	Częstotliwość zmiany	Max. co 30 dni	Max. co 30 dni	Max. co 30 dni
	Określony skład znakowy hasła		x	x

Źródło: opracowanie własne na podstawie Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, par. 6 oraz Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (poz. 1024).

Według PN-ISO/IEC 27001[181] polityka bezpieczeństwa realizowana jest według modelu Deminga: „*Planuj – Wykonuj – Sprawdzaj – Działaj*" (*Plan – Do*

[179] *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*, par. 3.2.

[180] *PN-ISO/IEC 27005:2011 Technika Informatyczna. Techniki bezpieczeństwa. Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie*.

[181] *PN-ISO/IEC 27001*.

– *Check – Act*)[182] i obejmuje przygotowanie polityki bezpieczeństwa, jej wdrożenie i eksploatację, kontrolę jej efektów oraz jej udoskonalanie.

W obszarze dotyczącym ochrony tożsamości cyfrowej, utworzenie i skuteczne przygotowanie polityki bezpieczeństwa powinno obejmować m.in.[183]:

1. Zdiagnozowanie: co i w jakim zakresie powinno być chronione, a także określenie ryzyka i skutków kompromitacji danych.
2. Określenie: kto i w jakim zakresie ma mieć dostęp do zasobów, wraz z przypisaniem zadań i odpowiedzialności.
3. Określenie celów, procesów oraz procedur dla zarządzania zdiagnozowanym ryzykiem.

Drugim etapem jest wdrożenie i eksploatacja polityki bezpieczeństwa. Wdrożenie powinno obejmować m.in. zaimplementowanie wytycznych z polityki bezpieczeństwa do systemów informatycznych oraz ich rozpropagowanie. Eksploatacja powinna obejmować dynamiczne przypisywanie uprawnień do aktualnie pełnionych ról biznesowych przez pracowników. Wskazane są także szkolenia[184], podczas których przekazywane są treści związane z bezpieczeństwem informacji oraz przypominane i ćwiczone procedury. Szkolenia pełnią istotną rolę w kształtowaniu postaw pracowników[185]. Podczas trzeciego etapu następuje sprawdzenie skuteczności procedur oraz ich efektywności. Jest to zadanie kadry kierowniczej (np. audyty wewnętrzne) oraz informatycznej (np. analiza aktywności użytkowników). Kontrole mogą generować dwa rodzaje informacji: wykrycie luk bezpieczeństwa oraz przesłanki do ulepszenia procedur, które powinny być uwzględnione w ostatnim etapie – doskonalenia polityki bezpieczeństwa informacji. Wśród wymogów formalnych polityki bezpieczeństwa znajdują się m.in.[186]:

1. Konieczność jej sporządzenia i podpisania przez Administratora Danych Osobowych.
2. Przechowywanie jej w formie papierowej lub elektronicznej.
3. Stała aktualizacja i przeglądanie poprawności stosowania procedur co najmniej raz w roku.

---

[182] Byczkowski M. (2010) *Zarządzanie bezpieczeństwem informacji i systemów,* W: Zawiła-Niedźwiecki, J., Rostek, K., Gąsiorkiewicz, A. red. Informatyka gospodarcza T.4 Warszawa: C.H.Beck, s. 392.

[183] *PN-ISO/IEC 27001*.

[184] *Nowe przepisy o ochronie danych osobowych* (2017). 4ITSecurity. Online: http://4itsecurity.pl/blog/2-Dane-osobowe/90-nowe-przepisy-o-ochronie-danych-osobowych.html, 2017.01.07.

[185] Ocieczek W., Łakomy K., Nowacki K. (2016). *Proces doskonalenia pracowników poprzez szkolenia w aspekcie kształtowania kultury bezpieczeństwa pracy*. Organizacja i zarządzanie nr 4(36). Gliwice: Wydawnictwo Politechniki Śląskiej, s. 53–66.

[186] Zegarek, P. (2010). *Podstawowe obowiązki administratora danych osobowych*. Online: http://blog-daneosobowe.pl/ochrona-danych-osobowych-podstawowe-obowiazki-administratora-danych-osobowych, 2010.03.18.

3.4.1.2. Instrukcja zarządzania systemem informatycznym

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych powinna zawierać m.in.:[187]

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania ich w systemie informatycznym, a także wskazanie osoby odpowiedzialnej za te czynności. Zasady powinny dotyczyć wszystkich operacji od utworzenia konta użytkownika, poprzez przydzielanie i modyfikację jego uprawnień aż po usunięcie konta z systemu informatycznego. Powinno się określić w sposób jednoznaczny zasady postępowania z hasłami użytkowników uprzywilejowanych (tzn. na poziomie administratorów systemów informatycznych), jak również zasady administrowania systemem informatycznym w przypadkach awaryjnych np. nieobecności administratora. Należy wskazać osoby odpowiedzialne za realizację procedur oraz rejestrowanie i wyrejestrowywanie użytkowników w systemie informatycznym.
2. Stosowane metody i narzędzia uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem, czyli tryb przydzielania haseł, tj. wskazanie ustnej lub pisemnej formy przekazania hasła oraz określenie zaleceń dotyczących stopnia ich złożoności, częstotliwości i metodzie zmiany hasła (wymuszona przez system lub nie). Powinno się również wskazać funkcjonalnie lub personalnie osoby odpowiedzialne za przydział haseł. Ponadto należy wskazać sposób przechowywania haseł użytkowników, którzy posiadają uprawnienia administratorów systemów informatycznych oraz sposób odnotowywania ich awaryjnego użycia. W sytuacji użycia innej metody uwierzytelnienia niż hasła (tj. opartej o przedmioty lub biometrię) powinny zostać umieszczone wytyczne dotyczące ich stosowania, a także wytyczne dotyczące procesu rejestrowania i przechowywania wzorców biometrycznych w systemie.
3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemu, czyli poszczególne czynności wykonywane przez użytkownika w celu uzyskania dostępu do zasobów (logowanie się), a także po zakończeniu pracy z systemem informatycznym (konieczność wylogowania się). Uregulowane powinny być też kwestie związane

[187] *GIODO, Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji*. Online: www.giodo.gov.pl/plik/id_p/550/, dostęp: 2017.06.04, oraz *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*, par. 5, pkt III ppkt 1, par. 7 ust. 1 pkt. 4.

z czasowym opuszczeniem stanowiska prac (zabezpieczenie wyświetlanych na monitorze danych przed podejrzeniem przez nieuprawnioną osobę). Powinny zostać opracowane procedury określające sposób postępowania w sytuacji podejrzenia naruszenia bezpieczeństwa systemu.

4. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji, które zawierają dane osobowe, a także sposób postępowania z nośnikiem by zapewnić bezpieczeństwo zgromadzonym na nim danym.
5. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

Wdrożenie instrukcji składa się z następujących etapów: akceptacja przez administratora danych osobowych, formalne przyjęcie instrukcji jako obowiązującego dokumentu oraz przekazanie wytycznych osobom odpowiedzialnym za realizacji postanowień zawartych w instrukcji. Podobnie jak w przypadku polityki bezpieczeństwa powinna ona spełniać wymogi formalne (m.in. przygotowanie i zatwierdzenie przez Administratora Danych Osobowych, właściwe przechowywanie i udoskonalanie).

Ważnym elementem systemu bezpieczeństwa jest opracowanie scenariuszy reakcji na incydenty i praktyczne sprawdzenie ich działania[188]. Mimo znaczenia instrukcji postępowania w przypadku naruszenia bezpieczeństwa danych osobowych, według badania Global Economic Crime Survey 2016, tylko 40% przedsiębiorstw ma przeszkolone zespoły na wypadek incydentu naruszenie bezpieczeństwa[189].

3.4.1.3. Podmioty odpowiedzialne za bezpieczeństwo danych

W procesy związane z bezpieczeństwem zasobów zaangażowane są m.in. następujące grupy osób[190]:

1. Właściciel organizacji – jego zadaniem jest realizowanie strategii, określa akceptowalne ryzyko.

---

[188] *Dokumentacja zarządzania incydentami bezpieczeństwa* (2016). 4ITSecurity. Online:http://4itsecurity.pl/blog/1-Bezpiecze%C5%84stwo-informacji/72-dokumentacja-zarzadzania-incydentami-bezpieczenstwa.html, 2016.06.06.

[189] *Adjusting the Lens on Economic Crime Preparation brings opportunity back into focus. Global Economic Crime Survey 2016*. (2016) PWC. Online: http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf, dostęp: 2017.06.04.

[190] Wołowski, F., Zawiła-Niedźwiecki, J. (2012). *Bezpieczeństwo systemów informacyjnych: praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*. Kraków; Warszawa: edu-Libri, s. 120–121.

2. Wyższe kierownictwo – decyduje o nakładach na zabezpieczenia adekwatnych do szacowanego ryzyka.
3. Bezpośredni użytkownicy kont – głównie w zakresie procesu uzyskiwania dostępu do zasobów, dbania o bezpieczeństwo narzędzi uwierzytelnienia oraz wykonywanie niektórych działań zarządczych (np. automatyczne przywracanie haseł, zmiana hasła czy wnioskowanie o przydzielenie dostępu do zasobów).
4. Osoby zarządzające ludźmi (menedżerowie), których zadaniem jest m.in. określenie zasobów, do których podwładni powinni mieć dostęp, zakres możliwych do wykonania przez nich działań na udostępnionych zasobach, wnioskowanie do administratora zasobów o zmianę przydziału praw dostępu podwładnego do zasobów (odebranie, przydzielenie lub modyfikacja), motywacja do właściwego (także bezpiecznego) korzystania z powierzonych kont i narzędzi uwierzytelnienia oraz kontrola tych działań.
5. Osoby zawiadujące aspektami technicznymi i będące bezpośrednio odpowiedzialne za realizację zadań określonych w Ustawie o ochronie danych osobowych i właściwych rozporządzeń, czyli m.in. Administrator Danych Osobowych (ADO), Administrator Bezpieczeństwa Informacji (ABI) oraz Administrator Systemów Informatycznych (ASI). Obowiązki ADO, ABI oraz ASI mogą być także pełnione przez jedną osobę (szczególnie w przypadku małych przedsiębiorstw).

ADO, którym w rozumieniu prawa jest organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych, z wyłączeniem osób fizycznych przetwarzających dane na cele osobiste lub domowe oraz podmiotów z siedzibą za granicą państwa Polskiego[191]. Odpowiedzialność za obowiązki ADO spoczywa na zarządzie przedsiębiorstwa (lub osobie najwyżej postawionej) ale ich pełnienie może być przekazane innemu podmiotowi na podstawie pisemnej umowy[192]. Podstawową rolą ADO jest określenie w jaki sposób chronione będą dane osobowe oraz zapewnienie, by dane osobowe były w danym przedsiębiorstwie przetwarzane zgodnie z prawem (rola kontrolna). Jego podstawowe obowiązki to m.in.:

1. Ochrona interesów osób, których dane są przetwarzane[193].
2. Informowanie o fakcie, celu i zakresie zbierania i przetwarzania danych[194].

[191] *Dz.U. 1997 Nr 133 poz. 883 USTAWA z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, art. 3, 7.
[192] Tamże art. 31.
[193] Tamże, art. 26.
[194] Tamże, art. 24, 25, 33.

3. Zapewnienie przetwarzanym danym aktualności, a także podejmowanie działań w przypadku cofnięcia zgody na przetwarzanie (czasowe lub trwałe usunięcie danych)[195].
4. Zapewnienie bezpieczeństwa danym osobowym poprzez stosowanie odpowiednich zabezpieczeń technicznych, logicznych i organizacyjnych[196].
5. Kontrolowanie tych aspektów zbioru danych, które związane są z pochodzeniem danych (kto i kiedy je zgromadził), ich ewidencją (jakie dane są zbierane) oraz przeznaczeniem (komu zostały przekazane)[197].
6. Ewidencjonowanie osób, które mają upoważnienie do przetwarzania danych osobowych, a także zgłaszanie do rejestracji GIODO zbioru[198].

ABI, wyznaczony przez ADO pełni funkcję wykonawczą, czyli wdraża procedury i techniczne środki ochrony zasobów, gromadzonych w systemach informatycznych. Jego główne zadania to ochrona dostępu do zasobów oraz szeroko pojęta reakcja na incydenty: od działań zapobiegawczych po zabezpieczanie materiału dowodowego w przypadku wystąpienia incydentu.

Do podstawowych obowiązków ABI należą:

1. Zarządzanie kontami użytkowników, a w tym implementowanie w systemie zaleceń dotyczących m.in. tworzenia konta, przekazywania hasła (i, w razie potrzeby, jego odtwarzania), zawieszanie uprawnień, usuwanie konta. Zarządzanie narzędziami uwierzytelnienia tj. nadzór nad wydawaniem i rejestracja urządzeń uwierzytelniających oraz implementacja wytycznych w kwestii haseł tj. ich składu i daty ważności.
3. Zarządzanie fizycznym dostępem do pomieszczeń, w których przetwarzane są dane osobowe.
4. Zapewnienie ciągłości pracy bazy danych (stosowanie awaryjnego zasilania oraz oprogramowania, które zabezpieczy bazę danych przed błędami i umożliwi bezpieczne zamknięcie w razie awarii).
5. Zabezpieczenie dostępu do zasobów z pomocą urządzeń mobilnych (zaopatrzenie w hasło, zapewnienie dostępu do urządzeń wyłącznie uprawnionych, przeszkolonych osób).
6. Nadzór nad prawidłowością wykonywanych operacji na fizycznych nośnikach (naprawy, konserwacje, utylizacja nośników), zawierających dane osobowe.

[195] Tamże, art. 35.
[196] Tamże, art. 36.
[197] Tamże, art. 38.
[198] Tamże, art. 39.

7. Zapewnienie ochrony antywirusowej, a także wszelkich konserwacji i aktualizacji oraz poprawnością działania sieci transmisji danych.
8. Nadzór nad dokumentami tworzonymi z wykorzystaniem systemów informatycznych, a w tym, zapewnienie dostępu do niszczarki.
9. W sytuacji wystąpienia lub podejrzenia wystąpienia incydentu naruszenia bezpieczeństwa natychmiastowe podjęcie działań zmierzających do: zabezpieczenia przed skutkami incydentu, określenie jego zasięgu, przyczyn i osoby, która jest odpowiedzialna za jego wystąpienie, oraz, w razie potrzeby, wystąpienie z wnioskiem o ukazanie winnych zaniedbań lub działań intencjonalnych.
10. Analiza skuteczności zabezpieczeń i wprowadzanie udoskonaleń, aktualizacji do instrukcji zarządzania systemem informatycznym, w szczególności po naruszeniu bezpieczeństwa systemu i przeanalizowaniu jego przyczyn i zaistniałych luk bezpieczeństwa.

ASI natomiast bezpośrednio zarządza systemem informatycznym, czyli dba o sprzęt i oprogramowanie tak, by zapewnić bezpieczeństwo zasobów na poziomie określonym przez ADO i ABI. Do jego podstawowych obowiązków związanych z zapewnieniem bezpieczeństwa systemowi informatycznemu przedsiębiorstwa, którymi zarządza zalicza się m.in.:

1. Tworzy i zrządza kontem użytkownika tj. m.in. przydziela identyfikator i hasło, prawa dostępu, nadzoruje mechanizmy uwierzytelniania.
2. Określa strategię i potrzeby w obszarze zabezpieczenia systemu, a także wdraża przyjęte rozwiązania, monitoruje i kontroluje ich skuteczność i wprowadza niezbędne poprawki.
3. Określa obowiązki oraz odpowiedzialność osób, które mają dostęp do chronionych zasobów.
4. Identyfikuje ryzyko związane z przetwarzaniem danych osobowych.
5. Odpowiada za instalację i konfigurację sprzętu oraz oprogramowania zabezpieczającego przed wyciekiem danych (np. programy antywirusowe, rozwiązania ukrywające hasło podczas wprowadzania).
6. Nadzoruje bezpieczeństwo danych przetwarzanych zarówno w urządzeniach stacjonarnych (w siedzibie firmy i poza), jak i przenośnych.
7. Prowadzi ewidencje: systemów przetwarzających dane osobowe, osób, które mają do nich dostęp oraz lokalizację chronionych zasobów.

3.4.1.4. Zalecenia dotyczące stosowania narzędzi uwierzytelnienia

Konieczność stosowania uwierzytelnienia wiąże się z wymogami prawnymi. Na mocy rozporządzenia MSWiA z dnia 29 kwietnia 2004 r dotyczącego urządzeń i systemów informatycznych służących do przetwarzania danych

osobowych, jeśli w systemie są przetwarzane dane osobowe, konieczne jest stosowanie mechanizmów kontroli dostępu tj. każdy użytkownik powinien mieć swój identyfikator w systemie, a dostęp do danych powinien odbywać się tylko po pomyślnie zakończonym procesie uwierzytelnienia[199].

Na wybór dotyczący narzędzia uwierzytelnienia wpływa poziom poufności, która powinna być zapewniona danym zasobom. Im bardziej newralgiczne dane przetwarzane są w systemie, im cięższe konsekwencje błędnego uwierzytelnienia i nadużycia zaufania, tym większa powinna być pewność, co do tożsamości osoby mającej dostęp do zasobów[200].

Kwestie poziomu zabezpieczeń regulowane są np. przez normę ISO/IEC 29115 (*Information Technology – Security techniques – Entity authentication assurance framework*), która dotyczy oceny jakości elektronicznego uwierzytelnienia i wytycza standardy związane z adekwatnością zabezpieczeń w stosunku do potrzeb. W normie wyróżniono 4 poziomy wiarygodności (*Level of Assurance*, LoA), która powinna charakteryzować dany proces dostępu i przetwarzania zasobów: od 1 (najmniejsza wymagana wiarygodność) do 4 (wymagana największa wiarygodność). Kryteriami zaszeregowania do danego poziomu powinny być skutki kompromitacji danych oraz prawdopodobieństwo ich wystąpienia (tabela 3.2.).

Tabela 3.2. Potencjalny wpływ błędnego uwierzytelnienia (skala: niski, umiarkowany, znaczący, wysoki)

Potencjalny wpływ błędnego uwierzytelnienia	Poziom wiarygodności (LoA)			
	1	2	3	4
Niewygoda, dolegliwość lub uszczerbek na reputacji lub pozycji	Niski	Umiarkowany	Znaczący	Wysoki
Strata finansowa lub odpowiedzialność podmiotu	Niski	Umiarkowany	Znaczący	Wysoki
Szkoda dla podmiotu, jego planów lub publicznych interesów	–	Niski	Umiarkowany	Wysoki
Wyciek informacji wrażliwych lub nieuprawniony dostęp do nich	–	Umiarkowany	Znaczący	Wysoki
Bezpieczeństwo osobowe	–	–	Niski Umiarkowany	Znaczący Wysoki

[199] *Rozporządzenia m.in. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.*

[200] *Electronic Authentication Guideline. NIST Special Publication 800-63-1* (2011). NIST. Online: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-63-1.pdf, dostęp: 2017.06.04.

Naruszenie prawa cywilnego lub karnego	–	Niski	Znaczący	Wysoki

Źródło: *Mielnicki, T. i inni red. (2013) Identyfikacja i uwierzytelnienie w usługach elektronicznych. Forum Technologii Bankowych przy Związku Banków Polskich. Warszawa. Online: https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf s. 53.*

Przypisanie danego procesu do poziomu pozwala na określenie właściwego sposobu zabezpieczenia: im wyższy poziom, tym mocniejsze uwierzytelnienie powinno być użyte (tabela 3.3.).

Tabela 3.3. Dozwolone narzędzia uwierzytelnienia w zależności od wymaganego poziomu wiarygodności

Rodzaje dozwolonych tokenów	**Poziom wiarygodności (LoA)**			
	1	2	3	4
Token sprzętowy	x	x	x	x
Token programowy lub urządzenie do generowania haseł jednorazowych	x	x	x	
Hasło losowe, kod PIN lub lista haseł (niegenerowane przez użytkownika)	x	x		
Hasło lub kod PIN generowane przez użytkownika	x			

Źródło: *Mielnicki, T. i inni red. (2013) Identyfikacja i uwierzytelnienie w usługach elektronicznych. Forum Technologii Bankowych przy Związku Banków Polskich. Warszawa. Online: https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf s. 41*

Każda z metod uwierzytelnienia może być stosowana w różny sposób. Zakres decyzji leżących w gestii zarówno przedstawiciela przedsiębiorstwa jak i pracownika, posługującego się daną tożsamością cyfrową, przedstawiono w tabeli 3.4.

Tabela 3.4. Przykładowe decyzje, które leżą w gestii osób zawiadujących narzędziem uwierzytelnienia tożsamości cyfrowej pracownika

Metoda uwierzytelnienia	**Pracodawca**	**Pracownik**
Login i hasło	• Minimalna wymagana długość hasła • Minimalny wymagany skład jakościowy hasła (typy znaków stosowanych w haśle) • Maksymalny termin ważności hasła • Ukrywanie hasła podczas wprowadzania	• Treść hasła • Przechowywanie hasła • Udostępnianie hasła innym osobom • Korzystanie bądź nie z jednego hasła w różnych aplikacjach • Ochrona hasła

Metoda uwierzytelnienia	Pracodawca	Pracownik
	• Stosowanie ograniczenia liczby prób wprowadzania hasła	
Przedmiot	• Typ rozwiązania • Dodatkowe zabezpieczenia • Dodatkowe uprawnienia • Okres pracy urządzenia	• Przechowywanie przedmiotu • Udostępnianie przedmiotu innym osobom • Ochrona przedmiotu
Biometria	• Wybór cechy biometrycznej • Wybór konkretnego rozwiązania • Sposób przechowywania wzorców • Ustawienie progu żądanego podobieństwa wzorca i próbki • Dodatkowe zabezpieczenia	*(brak)*

Źródło: opracowanie własne.

Istnieje szereg zaleceń dotyczących tego, jak powinno być skonstruowane hasło. Większość organizacji związanych z branżą bezpieczeństwa IT, takie jak producenci oprogramowania antywirusowego, organizacje monitorujące rynek i propagujące bezpieczeństwo w sieci czy banki, zalecają podobny sposób tworzenia i zabezpieczania hasła.

Firma Kaspersky Lab zaleca tworzenie haseł min. 6 znakowych, złożonych z trzech grup znaków (duże i małe litery oraz cyfry). Odradza hasła słownikowe, sekwencje znaków (np. 123456), korzystanie w treści hasła z danych osobowych (np. data urodzenia czy imię) i stosowanie jednego hasła do różnych aplikacji[201].

Z kolei jeden z banków (Getin Bank) oprócz sugerowanej minimalnej długości hasła (co najmniej 8 znaków), posiadania w składzie hasła wszystkich czterech typów znaków (małe, duże litery, cyfry i znaki specjalne) oraz unikania haseł słownikowych i tworzonych z danych osobowych, wskazuje na konieczność zmiany hasła co kilka miesięcy oraz konieczność zachowania go w tajemnicy i bezwzględne nie dzielenie się nim z innymi pod rygorem utraty prawa do dochodzenia utraconych z konta środków[202].

[201] *Zalecenia przy tworzeniu silnego hasła* (2013). Kaspersky. Online: http://support.kaspersky.com/pl/viruses/general/3730, 2013.11.26.

[202] *Zasady bezpieczeństwa i wymogi techniczne*. GET IN Bank. Online: https://www.getinbank.pl/dokument/Zasady-bezpieczenstwa-i-wymogi-techniczne--internetowe-kanaly-dostepu.pdf, dostęp: 2107.06.04.

Inna firma zajmująca się wsparciem przedsiębiorstw w obszarze bezpieczeństwa Norton publikuje „*10 złotych zasad*" tworzenia bezpiecznych haseł: długość hasła min. 12 znaków, skład: po co najmniej jednej małej, dużej literze, cyfrze i znaku specjalnym, unikanie wyrazów słownikowych i prostych do odgadnięcia, zalecenie tworzenia akronimów dobrze sobie znanego ciągu wyrazów, unikanie przechowywania haseł w jednym miejscu i zapamiętywania ich w przeglądarce, zmiana hasła co 10 tygodni i nieudostępnianie go innym.

Do niedawna zauważalny był trend zwiększania obostrzeń związanych z budową haseł i częstotliwością ich zmiany. Fakt ten był spowodowany postępem technologicznym, także w możliwościach i czasie łamania haseł, oraz rosnącym zagrożeniem związanym z kompromitacją hasła[203].

Jednak w odpowiedzi na zaostrzanie zasad i zwiększanie wymagań, połączone ze wzrostem liczby urządzeń i aplikacji zabezpieczanych hasłem, nasiliło się zjawisko obchodzenia zasad. Wśród najczęstszych „ułatwień" Kaspersky podaje[204]: stosowanie tego samego hasła do różnych kont, stosowanie słabych i łatwych do złamania haseł oraz przechowywanie haseł w niebezpieczny sposób. Na dwa z trzech podanych procederów przedsiębiorca nie ma właściwie wpływu. Złożone hasło może być stosowane przez pracownika nie tylko do konta w zakładzie pracy, ale też prywatnego konta bankowego, maila i wszędzie tam, gdzie wymagane jest hasło bezpieczne. Niestety z uwagi na możliwości ludzkiego mózgu, hasła długie, losowe są trudne do zapamiętania, szczególnie, gdy mają być zmienianie stosunkowo często.

Użytkownicy haseł przedkładają często wygodę nad bezpieczeństwo chronionych zasobów i nie jest to kwestia wyłącznie braku wiedzy. Osoby, korzystające z haseł mają świadomość potrzeby stosowania silnych haseł, ale tego nie robią[205]. Stąd tak ważne jest określenie jakie działania powodują, że pracownicy stosują hasła w sposób bezpieczny. Słabe lub słabo chronione hasło jest bezużyteczne w sytuacji cyberataku.

W 2017 r. amerykański Narodowy Instytut Standardów i Technologii (National Institute of Standards and Technology, NIST)[206] wydał nowe wytyczne dotyczące zabezpieczenia tożsamości cyfrowych, które zawierają rewolucyjne w stosunku do dotychczasowej praktyki zapisy, takie jak: rezygnacja z cyklicznej

---

[203] Stanisławski, P. (2017). *Wreszcie nowe wytyczne w sprawie haseł! Koniec z ciągłymi zmianami i dziwnymi znakami.* Online: http://www.crazynauka.pl/wreszcie-nowe-wytyczne-w-sprawie-hasel-koniec-z-ciaglymi-zmianami-i-dziwnymi-znakami/, 2017.04.25.

[204] Gawrych, K. (2017). *A Ty jak dbasz o swoje hasła? Zadbaj o bezpieczeństwo w sieci!* Portal ODO. Online: https://portalodo.com/a-ty-jak-dbasz-o-swoje-hasla-zadbaj-o-bezpieczenstwo-w-sieci/, 2017.03.21.

[205] Tamże.

[206] Grassi, P.A. *Draft NIST Special Publication 800-63B. Digital Identity Guidelines. Authentication and Lifecycle Management*. NIST. Online: https://pages.nist.gov/800-63-3/sp800-63b.html#sec4, dostęp: 2017.06.04.

zmiany hasła (ma ona nastąpić na życzenie użytkownika lub w przypadku podejrzenia naruszenia bezpieczeństwa) i rezygnacja z określania z jakich znaków powinno składać się hasło (jednak utrzymane zostały wytyczne związane z zakazem haseł słownikowych). Jest to związane z upowszechnianiem się w Stanach Zjednoczonych uwierzytelnienia dwuskładnikowego[207]. Wpływ nowych wytycznych na bezpieczeństwo nowych zaleceń będzie można ocenić po jakiś czasie. W przypadku systemów przetwarzających dane osobowe pracodawca musi trzymać się przepisów prawa, ale w przypadku innych systemów przygotowując politykę bezpieczeństwa może powoływać się na stare („opresyjne") wytyczne lub nowe zalecenia uwzględniające komfort użytkownika.

Wybierając konkretne rozwiązanie, opierające się o metodę posiadania przedmiotu uwierzytelniającego należy rozpatrywać kwestie wygody użytkownika oraz zapewniany poziom bezpieczeństwa. Generalnie kradzież przedmiotu oznacza narażenie zasobów na dostęp osób nieuprawnionych. Stąd kluczowe jest zapewnienie fizycznej ochrony urządzenia przez użytkownika. Jednak pieczołowite przechowywanie przedmiotu nie zapewnia stuprocentowej pewności co do bezpieczeństwa zasobów.

Stosunkowo wygodne są tokeny USB. Od użytkownika wymagają jedynie wpięcia przedmiotu w gniazdo USB. Nie ma problemu pomyłek przy wprowadzaniu wygenerowanego hasła a przez to uwierzytelnienie jest szybkie. Jednak wygoda ma swoją cenę. Komunikacja przedmiot – komputer naraża prywatny klucz szyfrujący urządzenia na złamanie. W 2012 r. francuskim naukowcom udało się złamać klucz w 13 minut. Ciekawostką jest, że na zhakowanie estońskiego dowodu osobistego, chronionego kluczem szyfrującym o długości 1024 bitów wystarczyło 11,5 godziny, a wersji nowszej, chronionej kluczem o długości 2048 bitów 27 godzin[208]. Oznacza to, że w przypadku zainstalowanego złośliwego oprogramowania, napastnicy mogą uzyskać prywatny klucz jeśli token USB będzie podpięty do zainfekowanego urządzenia przez stosunkowo niedługi czas, co oznacza poznanie kolejnych, generowanych haseł. Urządzenie może także być przechwycone przez napastników na czas potrzebny do złamania zabezpieczeń, a potem niepostrzeżenie zwrócone.

W przypadku wyboru przedmiotu uwierzytelniającego, który generuje hasła jednorazowe, zaleca się, by był on zgodny z normą PN ISO/IEC 18031 „*Technika informatyczna – Techniki bezpieczeństwa – Generowanie bitów losowych*", co zapewnia stabilne działanie urządzenia w różnych warunkach i taki sposób

[207] Stanisławski, P. (2017). *Wreszcie nowe wytyczne w sprawie haseł! Koniec z ciągłymi zmianami i dziwnymi znakami*. Online: http://www.crazynauka.pl/wreszcie-nowe-wytyczne-w-sprawie-hasel-koniec-z-ciaglymi-zmianami-i-dziwnymi-znakami, 2017.04.25.

[208] *Bezpieczeństwo tokenu RSA SecurID 800 złamane w kwadrans* (2012). Online: https://zaufanatrzeciastrona.pl/post/bezpieczenstwo-tokenu-rsa-securid-800-zlamane-w-kwadrans/, 2012. 06.25.

generowania hasła (w przypadku deterministycznych generatorów haseł jednorazowych, które opierają się na przekształceniu kryptograficznym), który utrudnia jego złamanie[209].

Lista losowo wygenerowanych haseł jednorazowych w postaci karty może mieć dodatkowe zabezpieczenia, które utrudnią podejrzenie wszystkich haseł lub pozwolą na wykrycie takiej próby. Dość skuteczną metodą jest stosowanie haseł zdrapek, które są odporne na skanowanie czy wykorzystanie haseł w innej niż podana kolejności. W przypadku, gdy hasła są generowane w przedsiębiorstwie zaleca się ochronę całego procesu tworzenia i dystrybucji haseł np. poprzez stały nadzór dwóch osób, co mniejsza ryzyko korupcji lub szantażu[210].

Dojrzałość poszczególnych metod biometrycznych jest różna, podobnie jak ich akceptacja czy powszechność użycia. Każdy z tych aspektów należy rozważyć decydując się na wybór konkretnego zastosowania. W tabeli 3.5. zawarto parametry najpopularniejszych rozwiązań biometrycznych.

Tabela 3.5. Wskaźniki niezawodności biometrycznej identyfikacji

	Twarz	Odcisk palca	Tęczówka
FRR *False Rejection Rate*	3,3%–70%	0,2%–30%	1,9%–6%
FAR *False Acceptation Rate*	0,3%–5%	0%–8%	<1%
FER *Failure to Enroll Rate*	0%	2%–5%	0,5%

Źródło: Mielnicki, T. i inni red. (2013) Identyfikacja i uwierzytelnienie w usługach elektronicznych. Forum Technologii Bankowych przy Związku Banków Polskich. Warszawa. Online: https://zbp.pl /public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_I dentyfikacja_i_uwierzytelnianie_strona_FTB.pdf s. 78.

W przypadku haseł i przedmiotów zgodność musi być pełna, w przypadku biometrii zgodność pełna jest niemal niemożliwa. Możliwe jest zatem udzielenie dostępu osobie podobnej (FAR). Z tego względu warto rozważyć uwierzytelnienie biometryczne jako element uwierzytelnienia wieloskładnikowego np. w połączeniu z przedmiotem uwierzytelniającym[211]. Rozwiązania biometryczne są stosunkowo drogie, choć ceny spadają wraz z postępem technologicznym. W razie przechowywania wzorców biometrycznych w systemach informatycznych przedsiębiorstwa, należy zabezpieczyć je tak, jak dane osobowe.

[209] Mielnicki, T. i inni red. (2013). *Identyfikacja i uwierzytelnienie w usługach elektronicznych*. Forum Technologii Bankowych przy Związku Banków Polskich. Warszawa, s. 63. Online: https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf.

[210] Tamże s. 63–64.

[211] Wasilewska-Śpioch, A. (2015). *Czas na hasło głosowe? Eksperci są sceptyczni*. Dziennik internautów Bezpieczeństwo. Online: http://di.com.pl/czas-na-haslo-glosowe-eksperci-sa-sceptyczni-51365, 2015.01.24.

3.4.2. Aspekty aktywności pracowników

O poziomie bezpieczeństwa informacyjnego świadczy nie tylko sam fakt posiadania polityki bezpieczeństwa, ale także to, czy pracownicy znają procedury, zakresy swoich odpowiedzialności, posiadają wiedzę dotyczącą zagrożeń związanych z korzystaniem z komputera, urządzenia mobilnego czy Internetu i, przede wszystkim, stosują się do zaleceń[212].

Sama wiedza jest jednak niewystarczająca, konieczne jest motywowanie pracowników, ponieważ bezpieczne stosowanie tożsamości cyfrowej zwykle wiąże się z nakładem czasu i wysiłkiem, czyli pogarsza efektywność pracy pracownika. Stąd może pojawić się chęć by kosztem bezpieczeństwa zwiększyć sobie komfort korzystania z tożsamości cyfrowych tym bardziej, że są pewne działania ryzykowne, które trudno wykryć np. stosowanie tych samych haseł do celów prywatnych i służbowych czy dzielenie się nimi z innymi osobami.

Aby uniknąć podobnych zagrożeń, pracownicy powinni zostać poddani oddziaływaniom, kształtującym ich zachowanie[213]. Oddziaływania na pracownika mogą być rozpatrywane na trzech poziomach; mogą być związane:

- z całym przedsiębiorstwem, jego strategią, procesami i kompetencjami kadry menedżerskiej (oddziaływanie pracownik – przedsiębiorstwo);
- szeregiem działań podejmowanych przez przełożonych względem swoich pracowników, z uwzględnieniem zarówno organizowania zasobów, szkoleń, kar i nagród a także włączenia pracowników w proces decyzyjny (oddziaływanie pracownik – przełożony).
- źródłem motywacji, tj. wewnętrznej lub od zewnątrz (autooddziaływanie)[214].

3.4.2.1. Analiza motywacji bezpiecznego stosowania tożsamości cyfrowej w oparciu o klasyczne koncepcje

Klasycznie wyróżnić można trzy podejścia (koncepcje) psychologiczne: behawioralne, psychodynamiczne, poznawcze. [215]

W ujęciu koncepcji behawiorystycznej, użytkownik jest zewnątrzsterowny, czyli jego zachowanie jest kształtowane całkowicie przez zewnętrzne czynniki,

---

[212] Khan, A., Woosley, J.M. (2011). *Comparison of Contemporary Technology Acceptance Models and Evaluation of the Best Fit for Health Industry Organizations*. IJCSET, December 2011, Vol. 1, Issue 11, s. 709–717.

[213] Siponen, M., Mahmood, A.M., Pahnila, S. (2010). *Compliance with Information Security Policies: An Empirical Investigatio*n. Computer, Vol. 43, Issue 11, s. 64–71.

[214] Mroczkowska, D. (2013). *Rola przywództwa w kształtowaniu motywacji.* Organizacja i Zarządzanie, Nr 2(22), Gliwice: Wydawnictwo Politechniki Śląskiej, s. 97–112.

[215] Kostera, M., Kownacki, S., Szumski, A. (2009). *Zachowania organizacyjne: motywacja, przywództwo, kultura organizacyjna*. W: Koźmiński, A.K. red., Zarządzanie, teoria i praktyka. s. 316–317.

stąd należy mu zapewnić „doskonałe środowisko", obejmujące zarówno aspekt techniczny, organizacyjny, jak i kulturę organizacyjną zorientowaną na bezpieczeństwo. Pracownik powinien poznać akceptowane wzorce zachowań, których utrwalanie odbywałoby się za pomocą odpowiednio stosowanych wzmocnień: pozytywnych (nagrody) i negatywnych (kary). Historycznym przykładem teorii formułowanych w ramach podejścia behawioralnego jest teoria X i Y Douglasa McGregora[216]. Zastosowana w dzisiejszych realiach warunkowałyby dwa różne systemy bezpieczeństwa:

1. Zogniskowany na kontroli użytkownika (teoria X) – jest wynikiem postrzegania pracownika jako osoby leniwej i niedbającej o bezpieczeństwo oraz uchylającej się od odpowiedzialności. Głównym „motywatorem" do bezpiecznego stosowania tożsamości cyfrowych są kary oraz ścisła kontrola zachowań użytkowników.
2. Dostrojony do użytkowników (teoria Y) – jest wynikiem postrzegania pracownika jako osoby, która będzie stosować tożsamości cyfrowe w sposób bezpieczny o ile zapewni się jej swobodę działania w osiągnięciu tego celu. Narzędziami, które mogą być stosowane są szkolenia, wzmocnienia pozytywne (nagrody), włączenie pracownika w proces decyzyjny (np. związany z wyborem narzędzia uwierzytelnienia).

Działania motywacyjne podejmowane przez kierownika w ujęciu behawiorystycznym mogłyby wyglądać następująco:

1. Szkolenia dotyczące zasad bezpiecznego korzystania z systemów informatycznych.
2. Wyznaczanie i komunikowanie zasad dot. bezpiecznego korzystania z systemów informatycznych.
3. Ocena pracy pracownika w aspekcie bezpiecznego użytkowania systemów informatycznych.
4. Bieżąca kontrola i reagowanie na nieprzestrzeganie zasad.
5. Motywacja finansowa.

W tej koncepcji człowiek jest traktowany poniekąd jak czarna skrzynka, czyli na zasadzie przymusu kształtowany jest wyłącznie wynik i nawyk działania, bez zagłębiania się w wewnętrzne procesy. Stąd koncepcją poniekąd komplementarną jest podejście psychodynamiczne, które koncentruje się na wewnętrznych pobudkach działań człowieka. Działanie użytkownika nie jest zatem prostą reakcją na bodziec, tylko wynika z wewnętrznych sił motywacyjnych, z których często pracownik nie zdaje sobie sprawy. Oznacza to, że ten sam bodziec może wywołać różne skutki u różnych osób w zależności od układu wewnętrznych sił. Szczególną rolę odgrywają obawy np. zbieranie wzorców biometrycznych przez

[216] Ramesh K.M.H.M. (2013). *The Relationship between McGregor's X–Y Theory Management Style and Fulfillment of Psychological Contract: A Literature Review*. International Journal of Academic Research in Business and Social Sciences, No 5, s. 715–720.

zakład pracy, zagrożenie osobiste przy próbie dotarcia do zasobów chronionych cechami biometrycznymi, przedmiotem lub hasłem, ryzyko zgubienia przedmiotu, utraty czy zapomnienia hasła.

Jednym z założeń tej koncepcji jest możliwość występowania pobudek, często będących ze sobą w sprzeczności, dlatego ważna jest ich identyfikacja i odpowiednie tłumienie bądź wzmacnianie tak, by osiągnąć pożądany skutek.

Podejście poznawcze neguje koncepcje, że działania człowieka są determinowane wyłącznie przez czynniki zewnętrzne czy popędy i wskazuje na istotną rolę woli i świadomości człowieka. W przypadku zapewnienia bezpieczeństwa systemom informatycznym można wyróżnić dwie podstawowe przyczyny postępowania pracownika w sposób bezpieczny:

1. Chęć ochrony własnej osoby (redukcja ryzyka odpowiedzialności np. karnej, świadomość dopełnienia obowiązków, uniknięcie problemów w pracy).
2. Chęć ochrony interesu przedsiębiorstwa (zapewnienie bezpieczeństwa danych czy procesowi komunikacji).

3.4.2.2. Współczesne badania i koncepcje

Studia związane z motywowaniem prowadzone są w dwóch nurtach, czyli: badanie różnicujące (tworzenie typów, grup i dopasowanych do nich czynników, narzędzi itp.) oraz badanie uogólniające (szukanie elementów uniwersalnych dla „przeciętnego człowieka"). W ramach pierwszego nurtu zakłada się, że przygotowanie, wdrażanie czy eksploatacja systemu bezpieczeństwa, musi uwzględnić fakt zróżnicowania ludzi, ich pobudek, sposobów działania i reakcji oraz sposobu motywacji do pożądanych zachowań.

Przykładem są badania z 2016 r., których celem było zróżnicowanie użytkowników urządzeń mobilnych. W raporcie z badań[217], autorzy zidentyfikowali cztery typy użytkowników tych urządzeń (tabela 3.6.).

[217] Wodo, W., Ławniczak, K. (2016). *Bezpieczeństwo i biometria urządzeń mobilnych w Polsce. Badanie użytkowników 2016*. Wrocław: Wydawnictwo Politechniki Wrocławskiej, s. 9. Online: http://wwodo.mokop.co/uploads/docs/raport-bezpieczenstwo-urzadzenia-mobilne-polska-2016.pdf.

Tabela 3.6. Typy użytkowników urządzeń mobilnych

Typ użytkownika	Charakterystyka użytkownika
Wygodnicka Wanda	• nie zważa na kwestie bezpieczeństwa • ceni przede wszystkim wygodę użytkowania • nie obawia się utraty lub kradzieży danych
Nieufna Natalia	• nie wierzy w skuteczność zabezpieczeń • posiada płytką wiedzę, cudze przekonania przyjmuje jako swoje • obawia się inwigilacji w ingerencji z zewnątrz
Zagubiony Zbig	• nie rozumie problemu bezpieczeństwa • ma niskie kompetencje informatyczne • nie orientuje się w sposobie funkcjonowania nowoczesnych technologii
Obawiający się Olek	• posiada rozległą wiedzę w dziedzinie IT i bezpieczeństwa • obawia się utraty lub kradzieży danych • stosuje adekwatne, silne zabezpieczenia

Źródło: Opracowano na podstawie Wodo, W., Ławniczak, K. (2016) Bezpieczeństwo i biometria urządzeń mobilnych w Polsce. Badanie użytkowników 2016. Wrocław: Wydawnictwo Politechniki Wrocławskiej, s. 9. Online: http://wwodo.mokop.co/uploads/docs/raport-bezpieczenstwo-urzadzenia-mobilne-polska-2016.pdf , dostęp: 2017.06.04.

Autorzy określili główne problemy i potrzeby przedstawicieli każdej z grup (tabela 3.7.). Pokazuje to, jak różne są uwarunkowania związane z pracownikami, ich motywacje, a co za tym idzie racjonalny system zapewnienia bezpieczeństwa, odpowiadający ich potrzebom.

Tabela 3.7. Problemy i potrzeby użytkowników

Typ użytkownika	Problem	Potrzeba
Wygodnicka Wanda	Rozwiązania, które wymagając ciągłego wprowadzania danych uwierzytelniających	Niezakłócone użytkownie urządzenia
Nieufna Natalia	Brak wiary i chęci edukacji w obszarze zabezpieczeń	Nabycie rzetelnej wiedzy dotyczącej systemów zabezpieczeń oraz zapewnienie nieskomplikowanego systemu zabezpieczeń, zapewniającego personalną ochronę i poczucie bezpieczeństwa
Zagubiony Zbig	Brak wiedzy i poczucie zagubienia	Pomoc osoby, która nauczy go korzystania z urządzeń, wyjaśni zagrożenia i kwestie dotyczące

Typ użytkownika	Problem	Potrzeba
		bezpieczeństwa oraz nauczy jak sobie z nimi radzić
Obawiający się Olek	Obawa przed niedostatecznym zabezpieczeniem danych i ich wyciekiem oraz świadomość szerokiej gamy możliwości ataku	Najlepsze możliwe zabezpieczenia

Źródło: Opracowano na podstawie Wodo, W., Ławniczak, K. (2016) Bezpieczeństwo i biometria urządzeń mobilnych w Polsce. Badanie użytkowników 2016. Wrocław: Wydawnictwo Politechniki Wrocławskiej. Online: http://wwodo.mokop.co/uploads/docs/raport-bezpieczenstwo-urzadzenia-mobilne-polska-2016.pdf , dostęp: 2017.06.04, s. 9.

Analiza materiału badawczego pozwoliła autorom na wyciągnięcie wniosków dotyczących[218]:

1. Braku edukacji użytkowników w obszarze bezpieczeństwa, ryzykownych zachowań (zdecydowana większość respondentów).
2. Braku stosowania zabezpieczeń urządzeń mobilnych (zdecydowana większość respondentów).
3. Bazowania na stereotypach w kwestii technologii biometrycznych i duża nieufność do tej metody (spora grupa respondentów).
4. Obaw w kwestii biometrii dotyczących: utraty prywatności, inwigilacji, wejścia w posiadanie zbyt osobistych danych, obaw dotyczących pozyskania organów celem uzyskania dostępu do zasobów chronionych np. odciskiem palca (spora grupa respondentów).
5. Potrzeby autorytetu i rekomendacji danych funkcjonalności.
6. Faktu, że użytkownicy czują się za mało ważni, aby stać się ofiarami cyberataków (spora grupa respondentów).
7. Sprzeczności oczekiwań: jednej strony najlepszą opcją byłaby sytuacja, gdyby urządzenie samo rozpoznawało użytkownika (wszyscy respondenci), co przemawia na korzyść technologii biometrycznych, ale z drugiej silne obawy przed biometrią (spora część respondentów).
8. Zapewnienia bezpieczeństwa osiąganego poprzez podejmowanie działań, których celem jest z jednej strony zminimalizowanie gromadzonych danych i pozostawianych w Internecie śladów (np. stosowanie tzw. lurkingu), a z drugiej stosowanie szeregu zabezpieczeń, by uchronić dane przed kompromitacją (bardziej świadomi respondenci).
9. Braku zaufania do przechowywania danych w sieci (tzw. chmurze).

Wysnuto wnioski i zalecenia dotyczące kierunków działań, związanych z dopasowaniem systemu bezpieczeństwa do użytkowników[219]:

[218] Tamże, s. 9.
[219] Tamże, s. 6, 8, 9, 15.

1. Istnieje luka w aspekcie bezpieczeństwa urządzeń. Dotyczy ona zarówno świadomości zagrożeń, ryzyka związanego z własnym postępowaniem, jak i wiedzy na temat zagrożeń.
2. Potrzebna jest edukacja, szczególnie w przypadku osób należących do grup Wygodnicka Wanda i Zagubiony Zbig, dotycząca zarówno celu, jak i sposobu stosowania urządzeń w sposób bezpieczny.
3. Potrzebny jest autorytet – osoba, posiadająca wiedzę, która przeprowadzi szkolenie praktyczne i tym samym zachęci do efektywniejszego wykorzystania urządzeń. Kluczowa jest wiarygodność autorytetu.
4. Wykazywane przez respondentów poczucie bezpieczeństwa podczas korzystania z urządzeń wynikać może zarówno z podjęcia działań zabezpieczających, jak i braku świadomości o narażeniu na atak.
5. Biometrię najlepiej postrzegają osoby o wyższych kompetencjach.
6. Nie ma jednego, uniwersalnego rozwiązania, odpowiadającego na oczekiwania i potrzeby wszystkich typów użytkowników.
7. W adaptacji nowych technologii kluczowe jest zidentyfikowanie i wyeliminowanie obaw związanych z daną technologią oraz właściwa edukacja.

Wprawdzie badanie dotyczyło technologii mobilnych, stanowi ono istotną przesłankę do zachowania się użytkowników systemów informatycznych. Cennym wnioskiem ogólnym jest określenie typów użytkowników, którzy są powodowani rożnymi pobudkami i mają różne potrzeby.

Przykładem czynnika różnicującego postawy względem technologii, może być wiek pracowników[220]. Osoby do 30 roku życia wykazują bardziej pozytywne postawy niż osoby starsze. Także według innych badań wiek jest istotnym czynnikiem w przypadku korzystania z usług wirtualnych[221].

W ramach drugiego nurtu, badacze poszukują uniwersalnych czynników, wpływających na postępowanie człowieka. Wynikiem jest sformułowanie oraz wykorzystanie szeregu teorii na gruncie badań związanych z zachowaniem użytkowników systemów informatycznych. Należą do ich m.in.: teoria unikania zagrożenia technologicznego (*Technology Threat Avoidance Theory*, TTAT)[222],

[220] Rosiński, J. (2012). *Postawy pracowników branży IT wobec zatrudniających organizacji jako wyzwanie dla rozwoju firm informatycznych*. Problemy Zarządzania, Vol. 10, Nr 3 (38), Uwarunkowania zastosowań systemów informatycznych w gospodarce, Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania UW, s. 230.

[221] Szyjewski, G., Niemcewicz, P. (2016). *Zdalna realizacja usług w Internecie z uwzględnieniem profilu użytkownika*. Studia Informatica Pomerania, Nr 3 (41), s. 79–89.

[222] Liang, H., Xue, Y. (2009). *Avoidance of Information Technology Threats: a Theoretical Perspective*. MIS Quarterly, Vol. 33 No. 1, s. 71–90, oraz Liang, H., Xue, Y. (2010). *Understanding Security Behaviors in Personal. Computer Usage: A Threat Avoidance Perspective.* Journal of the Association for Information Systems, Vol. 11, Issue 7, s. 394–413.

teoria motywacji ochronnej, (*Protection Motivation Theory*, PMT)[223], teoria samo-stanowienia (*Self-Determianation Theory*, SDT), teoria planowego działania (*Theory of Planned Behaviour*, TPB), Teoria uzasadnionego działania (*Theory of Reasoned Action*, TRA)[224], teoria kognitywnego rozwoju moralnego (*Theory of Cognitive Moral Development*, TCMD) i teoria motywacyjnych typów wartości (*Theory of Motivational Types of Values*, TMTV).[225]

Temat bezpiecznego korzystania z technologii, a w szczególności motywy przestrzegania bezpieczeństwa informacji i postępowanie zgodnie z wytycznymi polityki bezpieczeństwa, jest przedmiotem licznych badań, które prowadzi m.in. zespół badaczy, którego trzon stanowią Mikko Siponen i Seppo Pahnila. Ich badania koncentrują się na zagadnieniach motywacji wewnętrznej[226], intencjach[227], kształtowaniu nawyków[228] i narzędzi[229] w obszarze zapewnienia zgodności postępowania pracowników z regulacjami w kwestii bezpieczeństwa. Badacze tacy jak Pervaiz Ahmed zajmują się również czynnikami wpływającymi na wystąpienie incydentów bezpieczeństwa[230].

Dynamicznie rozwijającym się naukowych dociekań jest uwierzytelnienie biometryczne. Obecne kierunki badań dotyczą technicznych aspektów biomet-

---

[223] Ifinedo, P. (2012). *Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory*. Computers & Security 31 (2012), s. 83–95, oraz Vance, A. Sipponen, M., Pahnila, S. (2012). *Motivating IS security compliance: Insights from Habit and Protection Motivation Theory*. Information & Management 49 (3–4), s. 190–198.

[224] Siponen, M., Mahmood, A.M, Pahnila, S. (2014). *Employees' adherence to information security policies: An exploratory field study.* Information & Management March 2014 51(2), s. 217–224.

[225] Myyry, L. i inni (2009). *What levels of moral reasoning and values explain adherence to information security rules? An empirical study*. European Journal of Information Systems, Vol. 18, Issue 2, s. 126–139.

[226] Siponen, M., Mahmood, A.M, Pahnila, S. (2014). *Employees' adherence to information security policies: An exploratory field study*. Information & Management March 2014 51(2), s. 217–224.

[227] Siponen, M., Mahmood, A.M, Pahnila, S. (2006). *Factors Influencing Protection Motivation and IS Security Policy Compliance.* Materiały konferencyjne: Innovations in Information Technology 2006, 19–21.12.2006, Dubaj, s. 1–5.

[228] Vance, A., Siponen, M., Pahnila, S. (2012). *Motivating IS security compliance: Insights from Habit and Protection Motivation Theory.* Information & Management 49(3–4), s. 190–198.

[229] Pahnila, S., Siponen, M., Mahmood, A.M. (2007). *Employees' Behavior towards IS Security Policy Compliance.* 40th Annual Hawaii International Conference on System Sciences (HICSS'07) System Sciences, s. 156b–156b.

[230] Pei-Lee, T., Ahmed, P.K., D'Arcy, J. (2015). *What Drives Information Security Policy Violations among Banking Employees? Insights from Neutralization and Social Exchange Theory*. Journal of Global Information Management, Vol. 23, Issue 1, s. 44–64.

rii[231], jej zastosowań[232], ale też i postrzegania przez użytkowników związanego z niezawodnością metody[233], jej bezpieczeństwem[234] i akceptowalnością społeczną[235].

Analiza literatury, a także praktyka pokazują, że przyjęcie polityki bezpieczeństwa w postaci skodyfikowanych reguł, nie oznacza automatycznego spełnienia wytycznych przez pracowników[236]. Według Shih i inn., działania mające na celu wypracowanie określonych zachowań pracowników mogą być dwojakie: promujące określone zachowania (wzmacniające) i prewencyjne (zapo-

[231] Ross, A., Jain, A. (2007). *Human recognition using biometrics: an overview*. Annals of Telecommunications Vol. 62, Issue 1/2, s. 11–35, oraz Kapczyński, A. (2005). *Problematyka baz danych w biometrycznych systemach uwierzytelniania.* W: Kozielski, S. i inni red. Bazy Danych: Modele, Technologie, Narzędzia, Warszawa: Wydawnictwa Komunikacji i Łączności, s. 355–359, oraz Dass, S.C. (2013). *Fingerprint-Based Recognition*. International Statistical Review, Vol. 81, Issue 2, s. 175–187.

[232] Khan, A., Woosley, J.M. (2011). *Comparison of Contemporary Technology Acceptance Models and Evaluation of the Best Fit for Health Industry Organizations*. IJCSET, December 2011, Vol. 1, Issue 11, s. 709–717, oraz Amoore, L. (2005). *Biometric borders: Governing mobilities in the war on terror*. Political Geography 25(3), s. 336–351.

[233] Szczepanik, M., Jóźwik, I.J. (2014). *Metody wykrywania człowieczeństwa w systemach biometrycznych.* Organizacja i Zarządzanie z. 68, Nr kol. 1905, s. 403–411.

[234] Mielnicki, T. i inni red. *(2013) Identyfikacja i uwierzytelnienie w usługach elektronicznych.* Forum Technologii Bankowych przy Związku Banków Polskich. Warszawa, s. 77–79. Online: https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf.

[235] Plucińska, M., Wójtowicz, J. (2014). *Analiza technik biometrycznych do uwierzytelniania osób.* Elektronika 4/2014, s. 64–66.

[236] Guo, K.H. i inni (2011). *Understanding nonmalicious security violations in the workplace: a composite behavior model.* Journal of Management Information Systems, 28 (2), s. 203–236, oraz Ifinedo, P. (2012). *Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory.* Computer & Security, 31 (1), s. 83–95, oraz Pahnila, S., Siponen, M., Mahmood, A.M. (2007). *Employees' behavior towards IS security policy compliance.* Proceedings of the 40th Hawaii International Conference on System Sciences, January 3–6, Los Alamitos, oraz Vance, A., Siponen, M., Pahnila, S. (2012). *Motivating IS security compliance: insights from habit and protection motivation theory.* Information & Management, 49 (3–4), s. 190–198.

biegające)[237]. Z uwagi na dwa rodzaje osobowości pracowników[238]: powodowanych wzmocnieniami (*promotion-focused*) oraz skupionych na unikaniu zagrożeń (*prevention-focused*) wydaje się, że system oddziaływań na pracowników powinien obejmować oba te kierunki. Innymi słowy zachowania zgodne z wizją kierownictwa powinny być nagradzane, a niezgodne karane.

Realizacja idei zapewnienia bezpieczeństwa zasobom w systemach informatycznych powinna odbywać się nie tylko w wymiarze kary za niewłaściwe zachowanie, ale także we współpracy z pracownikiem[239].

Hung-Pin Shih i inn. wyróżniają 4 mechanizmy implementacji zasad, których celem jest zminimalizowanie ryzykownych działań pracowników w systemach informatycznych. Są to[240]:

1. motywacja za pomocą nagród (*promotion-approach mechanism*),
2. wprowadzenie zachęt do bezpiecznego korzystania z systemów informatycznych (*promotion-avoidance mechanism*),
3. wprowadzenie mechanizmów zabezpieczających przed naruszeniami bezpieczeństwa (*prevention-approach mechanism*),
4. motywacja za pomocą kar (*prevention-avoidance mechanism*).

3.4.2.3. Model akceptacji technologii (TAM)

Badacze wykorzystując różne podejścia badają czynniki wpływające na sposób użytkowania technologii przez jej końcowych odbiorców (użytkowników). Jednym z najszerzej stosowanych narzędzi do oceny systemów informatycznych jest Model akceptacji technologii (*Technology Acceptance Model*, TAM)[241]. Model ten, został zaproponowany przez Freda Daviesa w 1986 r.

[237] Shih, H.-P. i inni (2016). *Taking Promotion and Prevention Mechanisms Matter for Information Systems Security Policy in Chinese SMEs.* Proceedings of 2nd International Conference on Information Management (ICIM), 7–8 may 2016. London.

[238] Lockwood, P., Jordan, e.H., Kunda, Z. (2002). *Motivation by positive or negative role models: Regulatory focus determinants who will best inspire us*. Journal of Personality and Social Psychology, 83 (4), s. 854–864.

[239] Shih, H.-P. i inni (2016). *Taking Promotion and Prevention Mechanisms Matter for Information Systems Security Policy in Chinese SMEs.* Proceedings of 2nd International Conference on Information Management (ICIM), 7–8 may 2016. London.

[240] Tamże.

[241] Mortenson, M.J., Vidgen, R. (2016). *A computational literature review of the technology acceptance model*. International Journal of Information Management Vol. 36, Issue 6, Part B, s. 1248–1259.

w jego rozprawie doktorskiej[242] i opublikowany trzy lata później[243]. Koncepcja modelu z 1985 r. opisywała wpływ charakterystyki technologii na motywację jej użycia przez użytkownika, co przekładać się miało na rzeczywiste użycie. Davies rozbudował moduł motywacji wewnętrznej wydzielając: postrzeganą użyteczność, postrzeganą łatwość użycia oraz postawę wobec danej technologii. W kolejnej wersji modelu, przygotowanej trzy lata później wraz z Richardem Bagozzim i Paulem R. Warshawem pojawiły się intencje behawioralne.

TAM powstał na bazie teorii uzasadnionego działania TRA[244] oraz teorii planowanego działania TPB[245] opracowanych przez Icka Ajzena i Martina Fishbeina. Teorie te zakładały, że konkretne zachowanie użytkownika jest powodowane przez intencje, na które wpływ mają: postawa (względnie trwała ocena ludzka), subiektywne normy (przekonania co do reakcji innych ludzi na zachowanie innych) oraz, w przypadku TPB, postrzeganą kontrolę zachowań i czynniki zewnętrzne. W modelu TAM, podobnie jak w modelach TRA i TPB, wykorzystanie danej technologii (*Use*, U) jest poprzedzone przez intencję użycia (*Behavioral Intention To Use*, BI), rozumianą jako świadomy zamiar, która z kolei determinowana jest postawą. W socjologii najczęściej przyjmuje się, że na postawę składają się trzy komponenty[246]: behawioralne (działania), poznawczy (myśli, przekonania) i afektywny (odczucie), z czego ten związany z emocjami przyjmuje się jako najważniejszy. Davies w swoim modelu definiuje postawę właśnie w oparciu o komponent afektywny, tak jak zrobili to twórcy teorii TRA i TPB. Nowością są dwa czynniki, które wpływają na zaakceptowanie lub odrzucenie technologii (postawę pozytywną lub negatywną), czyli postrzegana użyteczność (*Perceived Usefulness*, PU) oraz postrzegana łatwość użycia danej technologii (*Perceived Ease Of Use*, PEOU), które mogą być kształtowane przez różne czynniki związane z technologią, samym użytkownikiem czy jego otoczeniem (rysunek 3.1.).

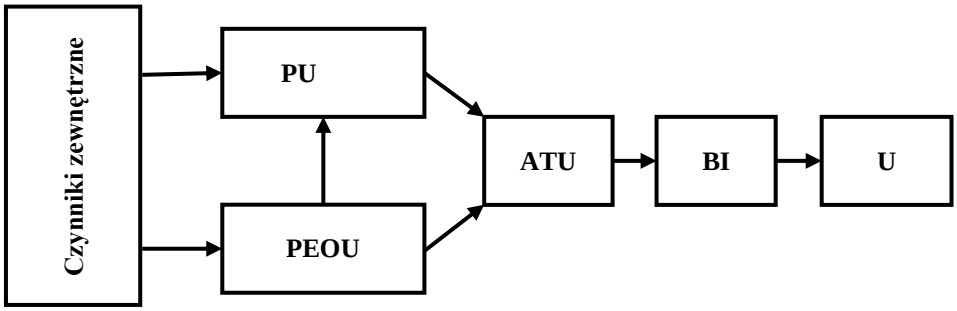
[242] Davis, F.D. (1986). *Technology Acceptance Model for Empirically Testing New End-user Information Systems Theory and Results.* Unpublished Doctoral Dissertation, MIT.

[243] Davis, F.D. (1989). *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*. MIS Quarterly 13(3), s. 319–340.

[244] Ajzen, I., and M. Fishbein (1980). *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs; NJ: Prentice Hall.

[245] Ajzen, J.: (1991). *The theory of planned behaviour*. Organisational Behaviour and Human Decision Processes, Vol. 50, s. 179–211.

[246] Aronson, E., Akert, R.M., Wilson, D.T. (2012). *Psychologia społeczna*. Serce i umysł. Zysk i S-ka., s. 313.



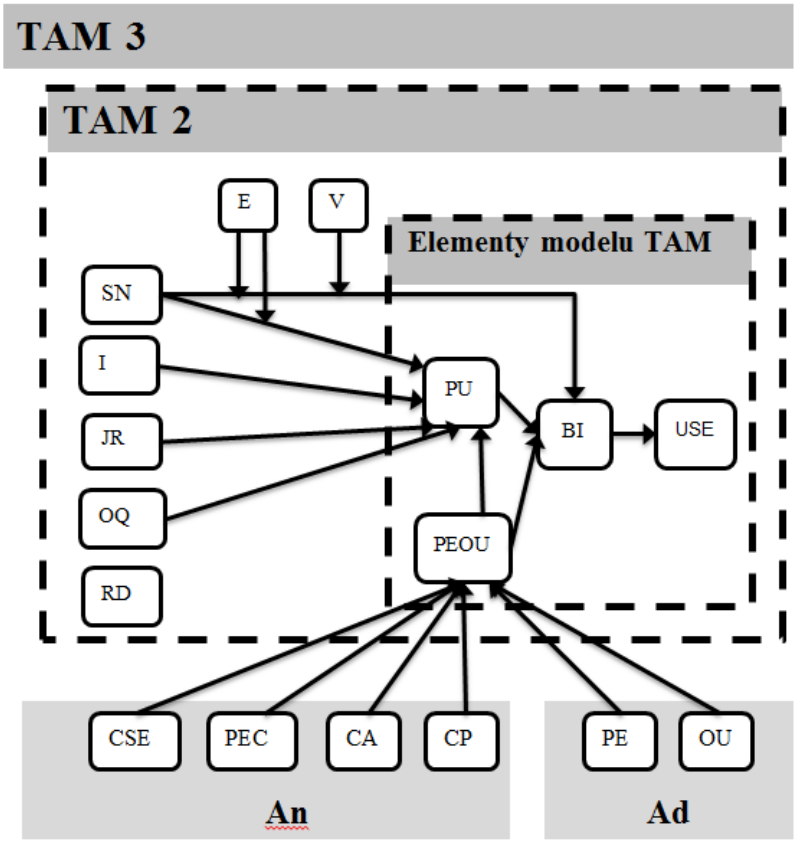
Rysunek 3.1. Ostateczna wersja modelu TAM

Źródło: Venkatesh, V., Davis, F. D. (1996). A model of the antecedents of perceived ease of use: development and test. Decision Sciences, 27 (3) s. 453.

Model TAM został zatem stworzony w celu określenia wpływu zewnętrznych czynników na wewnętrzne przekonania, postawy i intencje i może być wykorzystany m.in. do zrozumienia jak dany sposób motywowania człowieka wpłynie na jego zachowanie, a przez to może posłużyć jako narzędzie do kształtowania pożądanego sposobu działania. Dodatkowo, oprócz przewidywania zachowania użytkowników, model objaśnia przyczyny, dla których dana technologia jest nieakceptowana, co pozwoli na jej dostosowanie do potrzeb użytkowników końcowych[247].

Wyjątkowość tego modelu polega na tym, że w sposób niezwykle trafny przybliża rzeczywistość, co spowodowało jego wielką popularność. Model ten był modyfikowany wielokrotnie. Sam twórca oraz jego współpracownicy opracowali na bazie modelu TAM kolejne modele: TAM 2 i TAM 3 (rysunek 3.2.).

[247] Davis, F.D., Bagozzi, R.P., Warshaw, P.R. (1989). *User Acceptance of Computer Technology: A Comparison of Two Theoretical Models*. Management Science 35(8), s. 985.



PU – postrzegana użyteczność
PEOU – postrzegana łatwość użycia
BI – intencje użycia
USE – użycie

SN – subiektywne normy
I – wizerunek
JR – relewantność
OQ – jakość wyniku
RD – demonstrowalność wyniku
E – doświadczenie
V – dobrowolność

An – kotwica
Ad – dostosowanie
CSE – wydajność obsługi komputera
PEC – postrzeganie nadzoru
CA – niechęć do korzystania z komputera
CP – swoboda w korzystaniu z komputera
PE – postrzegana przyjemność
UO – celowość zastosowania

Rysunek 3.2. Model TAM, TAM 2, TAM 3
Źródło: Juszczyk, M. (2011). Stosowalność modelu TAM w różnych obszarach absorbcji nowych technologii IC., W: Miłosz, M. red. Techniki Informatyczne w praktyce. Lublin: Polskie Towarzystwo Informatyczne, s. 205.

W modelu TAM 2 autorzy (Fred D. Davis i Viswanath Venkatesh) zidentyfikowali czynniki wpływające na postrzeganą użyteczność (PU) jako[248]:

- Subiektywne normy (*Subjective Norm*, SN) rozumiane, jako zachowanie aprobowane przez ważne dla jednostki osoby.
- Wizerunek (*Image*, I), czyli stopień, w jakim korzystanie z technologii poprawi status jednostki w jej otoczeniu.
- Relewantność (*Job Relevance*, JR) określana, jako postrzegany stopień istotności systemu informatycznego dla wykonywanej pracy.
- Jakość wyniku pracy jednostki (*Output Quality*, OQ) uzyskiwanego przy pomocy systemu informacyjnego.
- Demonstrowalności wyniku (*Result Demonstrability*, RD) określanej, jako namacalność wyniku pracy z użyciem systemu informatycznego.

Dodatkowo wprowadzili do modelu dwa czynniki:

- Doświadczenie (*Experience*, E).
- Dobrowolność (*Voluntariness*, V).

Kolejnym rozwinięciem modelu TAM, dokonanym przez współautora modelu TAM 2 Viswanath Venkatesh jest model TAM 3, w którym określono czynniki wpływające na postrzeganą łatwość obsługi technologii, podzielone na dwie grupy: Kotwicę (*Anchor*, An) oraz Dostosowanie (*Adjustment*, Ad). Były to:

- Wydajność obsługi komputera (*Computer Self-Efficiency*, CSE), której miarą było postrzeganie własnych umiejętności do pracy z komputerem.
- Postrzeganie nadzoru (*Perception of External Control*, PEC), czyli przeświadczenie jednostki o posiadaniu wsparcia, którym jest kontrola jej pracy z systemem informatycznym.
- Niechęć do korzystania z komputera (*Computer Anxiety*, CA), która mierzona jest poziomem obawy lub lęku związanym z korzystaniem z komputera.
- Swoboda w posługiwaniu się komputerem (*Computer Playfulness*, CP) mierzona liczbą spontanicznych kognitywnych interakcji podczas pracy z komputerem.
- Postrzegana przyjemność (*Perceived Enjoyment*, PE), która mierzona jest stopniem przekonania o udanym korzystaniu z systemu, które nie jest związane z osiąganymi wynikami.
- Celowość zastosowania (Objective Usability, OU) – porównanie systemów w oparciu o rzeczywisty poziom nakładów, które są wymagane do realizacji konkretnych zadań.

[248] Venkatesh, V., Davis, F.D. (2000). *A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies*. Management Science, 46, s. 186–204.

Zwieńczeniem oryginalnych prac nad modelem TAM była ujednolicona teoria akceptacji i wykorzystania technologii (*Unified Theory of Acceptance and Use of Technology*, UTAUT) autorstwa Venkatesha i inn., która integrowała główne modele akceptacji technologii. Model TAM, jak i jego modyfikacje i rozwinięcia, z uwagi na swoją prostotę i trafność w odczytywaniu motywów użytkowników, były stosowane do badań różnych technologii takich jak[249] technologie komunikacyjne, oprogramowanie standaryzowane, specjalizowane czy biurowe, grup zdefiniowanych w oparciu o daną cechę lub badanych obszarów geograficznych. Liczbę badań wykonanych za pomocą tego modelu można mierzyć w tysiącach. Powstały też prace naukowe (Younghwa Lee, Kenneth A. Kozar i Kai R.T. Larsen, 2003; Paul Legris, John Ingham i Pierre Collerette, 2003; William R. King i Jun He, 2006; Jason H. Sharp, 2007; Mohammad Chuttur, 2009; Mark Turner, Barbara Kitchenham, Pearl Brereton, Stuart M. Charters i David Budgen, 2010; Chun-Hua Hsiao i Chyan Yang, 2011 oraz Michael J. Mortenson i Richard Vidgen, 2016)[250], których celem był przegląd literatury związanej z wykorzystaniem modelu TAM. Stał się on również bazą do tworzenia wielu nowych modeli takich jak np. Interaktywny Model Akceptacji i Satysfakcji z Technologii (Interactive Model of Technology Acceptance and Satisfaction, IMTAS) autorstwa Morteza Ghobakloo, Norzima B. Zulkifi i Faieza A. Aziza[251], który był narzędziem do badania akceptacji ICT w MSP[252]. Innym przykładem jest model badawczy zbudowany przez Jarosława Banasia i Zbigniewa Pastuszaka, który bazuje na modelach TAM i Modelu Adekwatności Zadań i Technologii (Task-

[249] Lee, Y., Kozar, K.A., Larsen, R.T. (2003). *The Technology Acceptance Model: past, present and future.* Communications of the Association for Information Systems, Vol. 12, Article 50, s. 752–780, oraz Chun, H.H., Chyan, Y. (2011). *The intellectual development of the technology acceptance model: A co-citation analysis.* International Journal of Information Management, Vol. 31, Issue 2, s. 128–136, oraz Marcinkowski, B., Wrycza, S. (2015). *CASE Tools' Acceptance in Higher Education – Assessment and Enhanced UTAUT Model.* Proceedings of the Conference on Information Systems Applied Research, Wilmington, North Carolina USA, Vol. 8, Nr 3671, s. 1–9., Wrycza, S., Marcinkowski, B., Gajda, D. (2017). *The enriched UTAUT model for the acceptance of software engineering tools in academic education.* Information Systems Management, Vol. 34, Issue 1, s. 38–49.

[250] Mortenson, M.J., Vidgen, R. (2016). *A computational literature review of the technology acceptance model.* International Journal of Information Management Vol. 36, Issue 6, Part B, s. 1248–1259.

[251] Ghobakloo M., Zulkifi, N.B., Aziza, F.A (2010). *The Interactive Model of User Information Technology Acceptance and Satisfaction in Small and Medium-sized Enterprises.* European Journal of Economics, Finance And Administrative Sciences Issue 19, s. 7–27.

[252] Wśród wniosków autorzy wymieniają szkolenia i umiejętności użytkownika jako istotne czynniki wpływające na poziom akceptacji ICT w MSP.

Technology Fit Model,TTF)[253], model bazujący na TAM opracowany w celu badań postawy wobec uczenia się w rzeczywistości rozszerzonej Rafała Wojciechowskiego i Wojciecha Cellarego[254], czy model do badania akceptacji e-learningu wyprowadzony z modelu UTAUT Stanisława Wryczy i Michała Kuciapskiego[255].

Model TAM nie jest wolny od wad. Wśród zastrzeżeń do badań z wykorzystaniem tej metody wymieniane są m.in.:[256]zbyt rzadkie badanie środowiska biznesowego jako podmiotu badań, nieprecyzyjność badań opartych na samoocenie, wskazywano także na konieczność rozszerzenia modelu o czynniki społeczne i ludzkie. Największy jednak zarzut dotyczy braku wymiernych korzyści z badań, które są powieleniem tego samego sposobu podejścia i ograniczają rozwój nowych metod i narzędzi badawczych.

[253] Banaś, J., Pastuszak, Z. (2015). *Użyteczność e-commerce w badaniach polskich użytkowników.* Problemy Zarządzania, Vol. 13, Nr 2 (52), T. 1, s. 24–36.

[254] Wojciechowski, R., Cellary, W. (2010). *Evaluation of learners' attitude toward learning in ARIES augmented reality environments.* Computers & Education, Vol. 68, s. 570–585.

[255] Wrycza, S., Kuciapski, M. (2014). *A model of faculty e-learning acceptance.* Conference proceedings,15th Annual Global Information Technology Management Association (GITMA) World Conference 2014. June 22–24, 2014, s. 2–12.

[256] Khan, A., Woosley, J.M. (2011). *Comparison of Contemporary Technology Acceptance Models and Evaluation of the Best Fit for Health Industry Organizations.* IJCSET, December 2011, Vol. 1, Issue 11, s. 709–717.

4. Modelowanie Akceptacji Tożsamości Cyfrowej

4.1. Wprowadzenie do badań

4.1.1. Badanie pilotażowe dotyczące użytkowników kont

Pierwsze z badań, których wyniki przyczyniły się do opracowania modelu DIAM, przeprowadzono podczas stażu badawczego Autorki współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Społecznego. Staż badawczy odbywał się w lubelskim przedsiębiorstwie produkującym oprogramowanie dla firm od początku maja do końca października 2011 r.

Celem głównym stażu badawczego była identyfikacja czynników Modelu Akceptacji Tożsamości Cyfrowej w sektorze MMSP oraz pogłębienie wiedzy na temat specyfiki mikro, małych i średnich przedsiębiorstw w zakresie korzystania z tożsamości cyfrowej.

W ramach badań analizowano wpływ wybranych czynników na postrzeganą użyteczność, łatwość użycia oraz postawę pracowników przedsiębiorstw sektora MMSP w obszarze tożsamości cyfrowej i jej stosowania. Przedmiotem badań były konta, rozumiane jako „*każdy zabezpieczony (np. loginem i hasłem) dostęp do funkcjonalności lub danych np. konto e-mail, konto pracownika w systemie informatycznym firmy, systemie Windows czy każdym programie, konto na Naszej Klasie, Facebooku, Allegro lub forum internetowym.*”[257]

Przyjęto rozumienie postawy jako „*względnie stałej i zgodnej organizacji poznawczej, uczuciowo-motywacyjnej i behawioralnej podmiotu, związanej z określonym przedmiotem czy klasą przedmiotów”*, na którą składają się 3 komponenty: poznawczy, emocjonalno-oceniający oraz behawioralny, który nie został uwzględniony w badaniu[258].

Postrzegana użyteczność kont w kontekście bezpieczeństwa została określona jako dobrowolny wybór rozwiązania, które chciałby stosować respondent. W przypadku uznania kont za przydatne użytkownik decydował, które konto jest dla niego optymalne: indywidualne (zapewniające większe bezpieczeństwo) czy grupowe (charakteryzujące się mniejszym bezpieczeństwem). Brak postrzeganej użyteczności kont skutkował wyborem opcji: brak kont.

Postrzegana łatwość użycia została oparta o dwa czynniki: łatwość użycia i czasochłonność.

---

[257] Juszczyk, M. (2011). *Akceptacja tożsamości cyfrowej w przedsiębiorstwach Lubelszczyzny*. W: Nauka-Biznes: zbiór raportów badawczych opracowanych przez pracowników naukowych i naukowo-dydaktycznych – przedstawicieli lubelskiego środowiska naukowego, Chełm: Chełmskie Stowarzyszenie Rozwoju Społeczno-Gospodarczego CIVIS, s. 337–363.

[258] Mądrzycki, T. (1977). *Psychologiczne prawidłowości kształtowania się postaw*, Warszawa: PWN, s. 16–18.

W badaniu postawiono następujące hipotezy[259]:

H1. Postrzegana łatwość użycia tożsamości cyfrowej jest skorelowana negatywnie z liczbą używanych w pracy kont, długością i złożonością stosowanego hasła, a pozytywnie z przebyciem szkolenia.

H2. Postawa wobec tożsamości cyfrowej jest skorelowana dodatnio z postrzeganą łatwością użycia konta.

H3. Postrzegana użyteczność jest pozytywnie skorelowana z wiedzą i doświadczeniem.

H4. Postawa wobec tożsamości cyfrowej jest pozytywnie skorelowana z postrzeganą użytecznością.

H5. Sposób użycia kont zależy od postawy wobec kont.

Respondentami byli pracownicy przedsiębiorstw Lubelszczyzny, którzy wykorzystywali komputer w pracy zawodowej, a wśród nich: 30 pracowników mikroprzedsiębiorstw, 17 osób zatrudnionych w małych i 22 osoby w średnich przedsiębiorstwach (w sumie 69 osób).

Analizując wyniki ankiet, wykryto zależności pomiędzy:

- postrzeganą łatwością użycia i postrzeganą użytecznością a czynnikami związanymi z użytkownikiem i jego kontami (tabela 4.1.),
- postawą a użyciem konta (tabela 4.2.).

Tabela 4.1.Zależności pomiędzy postrzeganą łatwością użycia oraz postrzeganą użytecznością a czynnikami związanymi z użytkownikiem i jego kontami

	Postrzegana łatwość użycia	**Postrzegana użyteczność**
Liczba kont	—	**X**
Liczba operacji	—	**X**
Długość hasła	brak	**X**
Rodzaj znaków haśle	brak	**X**
Wiedza ogólna	**X**	+
Wiedza szczegółowa	**X**	+
Odbycie szkolenia	brak	+

gdzie:

—	zależność ujemna
+	zależność dodatnia
brak	brak zależności
X	nie badano

Źródło: opracowanie własne.

[259] Juszczyk, M. (2011). *Akceptacja tożsamości cyfrowej w przedsiębiorstwach Lubelszczyzny*. W: Nauka-Biznes: zbiór raportów badawczych opracowanych przez pracowników naukowych i naukowo-dydaktycznych – przedstawicieli lubelskiego środowiska naukowego, Chełm: Chełmskie Stowarzyszenie Rozwoju Społeczno-Gospodarczego CIVIS, s. 337–363.

Tabela 4.2. Zależności pomiędzy postawą wobec konta a użyciem konta

		Postawa wobec kont	
		Komponent emocjonalno-oceniający	Komponent poznawczy
Użycie	Korzystanie z kont	+	+
	Przestrzeganie zasad	brak	+
	Bezpieczeństwo hasła	brak	**+/brak**

+	zależność dodatnia
+/brak	częściowa zależność
brak	brak zależności

Źródło: opracowanie własne.

Analiza wyników tego badania wytyczyła kierunek rozbudowy modelu, definiowania pojęć oraz budowy kwestionariusza badawczego. W szczególności postawiono następujące postulaty:

I. Konieczna jest redefinicja pojęcia postrzeganej użyteczności w oparciu o kryterium inne niż wpływ na efektywność pracy.
   Problem adaptacji postrzeganej użyteczności do celów tworzenia nowego modelu pojawił się na etapie tworzenia koncepcji kwestionariusza. Zapewnienie bezpieczeństwa wymaga zwykle nakładów (czasu, wysiłku, środków), co oznacza, że zmniejsza, a nie zwiększa efektywność pracy. Stąd efektywność nie może być kryterium postrzeganej użyteczności bezpiecznego użycia tożsamości cyfrowych.

II. Konieczne jest zdefiniowanie postrzeganej łatwości użycia, postawy wobec tożsamości cyfrowych, intencji użycia oraz użycia w oparciu o ustalone uprzednio standardy bezpieczeństwa.
   Problem konieczności wykorzystania standardów bezpieczeństwa pojawił się na etapie koncepcji modelu. Badane jest bezpieczne użycie, stąd, czynniki wpływające na sposób użytkowania tożsamości cyfrowej powinny uwzględniać ten aspekt. Przykładowo, inaczej może być postrzegane w kontekście łatwości użycia, stosowanie haseł słabych, a inaczej mocnych, których zapamiętanie czy bezbłędne wprowadzenia jest trudniejsze. Podobnie intencje użycia, czy postawa mogą być zależne od nałożonych na respondenta wymagań w kwestii sposobu wykorzystania przydzielonej mu tożsamości cyfrowej. Dlatego konieczne jest przyjęcie standardu bezpieczeństwa i badanie postrzeganej łatwości użycia, postawy wobec tożsamości cyfrowych, intencji użycia oraz bezpieczeństw użycia w kontekście tych standardów.

III. Konieczne jest badanie czynników motywujących do prawidłowego korzystania z tożsamości cyfrowej.
W przeprowadzonych badaniach wykazano, że duży wpływ na bezpieczne korzystanie z tożsamości cyfrowych ma kultura organizacyjna. Warto zatem zbadać, w jaki sposób kierownicy wspierają bezpieczeństwo informacji poprzez zapewnienie swoim podwładnym warunków sprzyjających bezpieczeństwu. Interesujących wniosków dostarczyła także analiza powodów stosowania tożsamości cyfrowych (motywacja wewnętrzna, zewnętrzna, przymus) i ich przełożenie na postawę wobec kont. Warto zatem potwierdzić je na większej grupie respondentów.

IV. Należy rozbudować model o czynniki związane z zarządzaniem pracownikiem w kontekście jego tożsamości cyfrowej na poziomie technicznym, organizacyjnym i społecznym.
Podczas pierwszego badania wstępnego respondenci sugerowali, że stosowanie tożsamości cyfrowych zależy od charakterystyki samego przedsiębiorstwa. Zasadnym zatem wydaje się rozbudowanie modelu o czynniki związane z macierzystym zakładem pracy.

V. Należy wprowadzić wielokryterialne mierzenie poziomu bezpieczeństwa użycia.
W pierwszym omawianym badaniu bezpieczeństwo użycia mierzono w wielu aspektach. Odpowiedzi respondentów obejmowały całą skalę możliwych odpowiedzi i dobrze określały różny stopień bezpieczeństwa zapewnionego tożsamościom cyfrowym.

VI. Dla przyjęcia lub odrzucenia danego czynnika wskazana jest weryfikacja jego wpływu na bezpieczeństwo użytkowania tożsamości cyfrowej na większej liczbie respondentów.
Niektóre wyniki omawianych badań przeprowadzonych na niewielkiej próbie badawczej stały w sprzeczności z powszechnymi sądami oraz wynikami innych badań. Konieczność zweryfikowania otrzymanych wyników na większej próbie badawczej oznacza, że te czynniki, które są powszechnie postrzegane jako wpływające na postrzeganie tożsamości cyfrowych, a których znaczenia nie wykazano w pierwszym badaniu wstępnym, powinny zostać ponownie rozpatrzone w modelu.

4.1.2. Badanie pilotażowe dotyczące narzędzi uwierzytelnienia

Pod koniec roku 2012 przeprowadzono drugie badanie[260], którego celem była ocena wpływu metody uwierzytelnienia na postrzeganie tożsamości cyfrowej przez użytkownika oraz głębsze zbadanie motywacji pracowników do bezpiecznego korzystania z tożsamości cyfrowych.

Badane było postrzeganie wad i zalet poszczególnych metody uwierzytelnienia, obawy związane z korzystaniem z tożsamości cyfrowych, preferencje użytkowników i ich motywy oraz ocena obecnie stosowanych rozwiązań.

Respondentami badania byli pracownicy Lubelszczyzny zatrudnienie w mikro, małych i średnich przedsiębiorstwach w liczbie 65 osób, które wykorzystywały komputer w pracy zawodowej, a wśród nich: 26 pracowników mikroprzedsiębiorstw, 22 osoby zatrudnione w małych i 10 osób w średnich przedsiębiorstwach.

Według *Raportu o stanie sektora małych i średnich przedsiębiorstw w Polsce*[261], w 2010 roku w systemie REGON zarejestrowanych było 173 616 podmiotów, włączając m.in. podmioty niebędące przedsiębiorstwami (np. fundacje) oraz podmioty o zawieszonej bądź zakończonej działalności. Stąd szacowany błąd pomiaru przy tej liczbie respondentów wyniósł maksymalnie 7% przy 95% poziomie ufności.

Główne wnioski z analizy wyników badania dotyczącego narzędzi uwierzytelnienia, były następujące[262]:

1. Wyniki badań potwierdziły przypuszczenie, że stosunek do tożsamości cyfrowej zależy od metody uwierzytelnienia.
2. Metody biometryczne generują największy opór użytkowników, są też najbardziej skrajnie postrzegane (największy odsetek osób nastawionych entuzjastycznie, ale i negatywnie).
3. Osoby zawodowo związane z technologiami IT (praca w branży IT lub wykształcenie informatyczne) preferują bezpieczniejsze metody uwierzytelnienia.
4. Respondenci generalnie zdają sobie sprawę z poziomu bezpieczeństwa zapewnianego przez poszczególne metody, a metody wykorzystywane w macierzystych przedsiębiorstwach postrzegane są przez większość z nich jako mało bezpieczne.

---

[260] Juszczyk, M., Miłosz, M., Miłosz, E. (2015). *Various methods for employees' authentication at SMEs*. Actual Problems of Economics – 2015, Nr 2, Vol. 164, s. 474–481.

[261] Polska Agencja Rozwoju Przedsiębiorczości (2011). *Raport o Stanie Sektora Małych i Średnich Przedsiębiorstw w Polsce,* Rozdział 8, PARP: Warszawa, s. 8. Online: https://badania.parp.gov.pl/files/74/81/469/12555.pdf, dostęp: 2017.05.03.

[262] Juszczyk, M., Miłosz, M., Miłosz, E. (2015). *Various methods for employees' authentication at SMEs*. Actual Problems of Economics – 2015, Nr 2, Vol. 164, s. 474–481.

Analiza wyników drugiego badania wstępnego pozwoliła na ulepszenie budowanego Modelu Akceptacji Tożsamości Cyfrowej poprzez określenie czynników wpływających na motywację użytkowników oraz wprowadzenie dodatkowych zagadnień do kwestionariusza badawczego.

W szczególności postawiono kolejne postulaty:

VII. Konieczne jest badanie metody uwierzytelnienia jako czynnika wpływającego na postrzeganie tożsamości cyfrowych.

Podczas analizy drugiego badania wstępnego wykazano znaczne zróżnicowanie stosunku do poszczególnych metod uwierzytelnienia. Przekładał się on m.in. na chęć stosowania tożsamości cyfrowych w sposób bezpieczny. Stąd konieczność uwzględnienia tego aspektu w modelu.

VIII. Konieczne jest badanie postrzeganych korzyści i strat z tytułu wykorzystywania uwierzytelnienia.

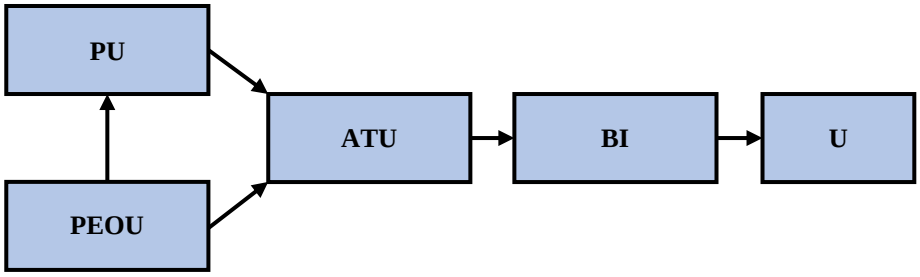
W omawianym badaniu określano jakie czynniki (za i przeciw) decydowały o wyborze metody uwierzytelnienia, którego dokonałby respondent dla swojego przedsiębiorstwa, gdyby było to w jego gestii. Respondenci określali zarówno zalety, jak i wady wybranych przez nich rozwiązań. To zestawienie umożliwiło sformułowanie ważnego wniosku z badania, czyli zdiagnozowanie dwóch grup użytkowników: tych, którzy kierują się wysokim poziomem bezpieczeństwa, zapewnianym przez daną metodę (kosztem własnej wygody), oraz tych, dla których liczy się komfort stosowania narzędzia (kosztem bezpieczeństwa zasobów systemów informatycznych). Warto zatem zastosować podobne podejście by zdefiniować czym kierują się respondenci określając użyteczność tożsamości cyfrowej.

IX. Należy poszerzyć charakterystykę użytkownika o kwestie związane z kontaktem z branżą IT.

Wyniki omawianego badania wskazują na duże różnice w postrzeganiu poszczególnych metod uwierzytelniających przez osoby związane z branżą IT oraz osoby, które nie są z nią związane.

4.2. Model Akceptacji Tożsamości Cyfrowej DIAM

Za podstawę Modelu Akceptacji Tożsamości Cyfrowej DIAM (*Digital Identity Acceptation Model*) przyjęto elementy modelu TAM (rysunek 4.1.): postrzeganą użyteczność (PU), postrzeganą łatwość użycia (PEOU), postawę (ATU), intencję użycia (BI) oraz użycie (U).



Rysunek 4.1. Model TAM
Źródło: Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), s. 319–340.

Zgodnie z postulatem I postawionym po analizie wyników badań poprzedzających badanie właściwe, dokonano redefinicji postrzeganej użyteczności. W modelu TAM postrzegana użyteczność jest definiowana jako *„stopień, do którego osoba wierzy, że wykorzystanie określonego systemu może podnieść wyniki jej pracy"*[263]. Jednak zapewnienie bezpieczeństwa zasobów w systemach informatycznych wymaga nakładów czasu i wysiłku, co skutkuje zwykle zmniejszeniem efektywności pracownika. Stąd, w modelu DIAM:

> **Postrzegana użyteczność (*Perceived Usefulness*, PU)** oznaczać będzie *stopień przekonania użytkownika, że bezpieczny sposób korzystania z tożsamości cyfrowych będzie dla niego korzystny*.

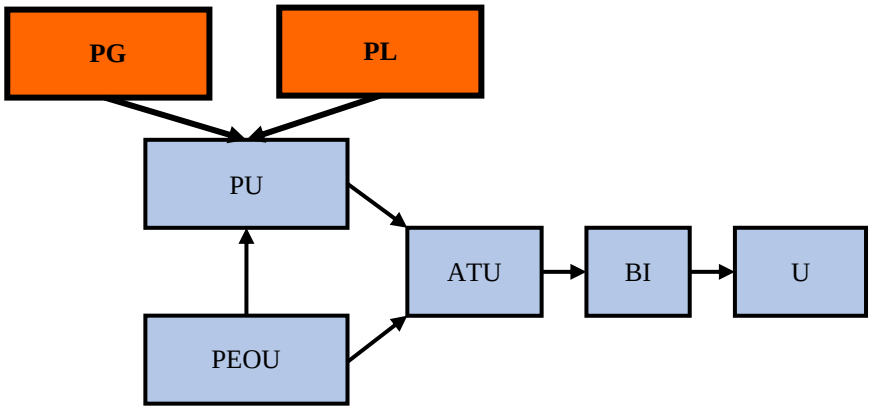
Pozostałe elementy oryginalnego modelu TAM zdefiniowano zgodnie z postulatem II:

> **Postrzegana łatwość użycia (*Perceived Easy Of Use*, PEOU)** rozumiana będzie jako *stopień przekonania użytkownika, że korzystnie z tożsamości cyfrowych w sposób bezpieczny jest łatwe*.
>
> **Postawa wobec tożsamości cyfrowych (*Attitude Towards Use*, ATU)** rozumiana będzie jako *emocjonalny (negatywny bądź pozytywny) stosunek do tożsamości cyfrowych*.
>
> **Intencja użycia (*Behavioral Intentions*, BI)** rozumiana będzie jako *gotowość do korzystania z tożsamości cyfrowych w sposób bezpieczny*.

[263] Pastuszak Z. (2007). *Implementacja zaawansowanych rozwiązań biznesu elektronicznego w przedsiębiorstwie*, Warszawa: Placet, s. 164–165.

Użycie tożsamości cyfrowej (*Use*, U) rozumiane będzie jako *użycie tożsamości cyfrowej w sposób bezpieczny, czyli bezpieczeństwo użycia mierzone bezpieczeństwem obecnie podejmowanych działań z użyciem tożsamości cyfrowej*.

Zgodnie z postulatem VIII postawionym po analizie wyników badań wstępnych założono, że na postrzeganie zdefiniowanej uprzednio użyteczności, wpływ mają **postrzegane korzyści (*Perceived Gains*, PG)** i **postrzegane straty (*Perceived Loss*, PL)** z tytułu bezpiecznego posługiwania się tożsamością cyfrową (rysunek 4.2.).

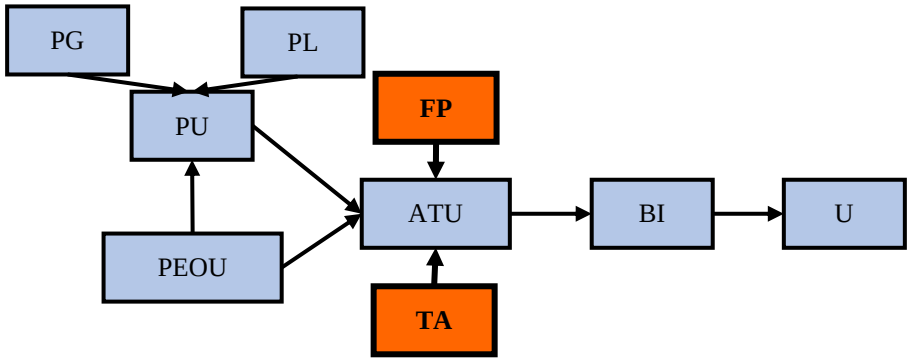


Rysunek 4.2. Budowa modelu DIAM – etap I
Źródło: opracowanie własne.

Zgodnie z postulatem III, wprowadzono dwa czynniki potencjalnie kształtujące postawę użytkownika (rysunek 4.3.):

Świadomość zagrożeń (*Threat Awareness*, TA) – stopień, w jakim jednostka postrzega, że bezpieczne stosowanie tożsamości cyfrowej przekłada się na bezpieczeństwo zakładu pracy.

Postrzeganie wymuszenia (*Force Perception*, FP) – stopień, w jakim jednostka postrzega, że jej działania związane z korzystaniem z tożsamości cyfrowej są wynikiem działań innych osób.

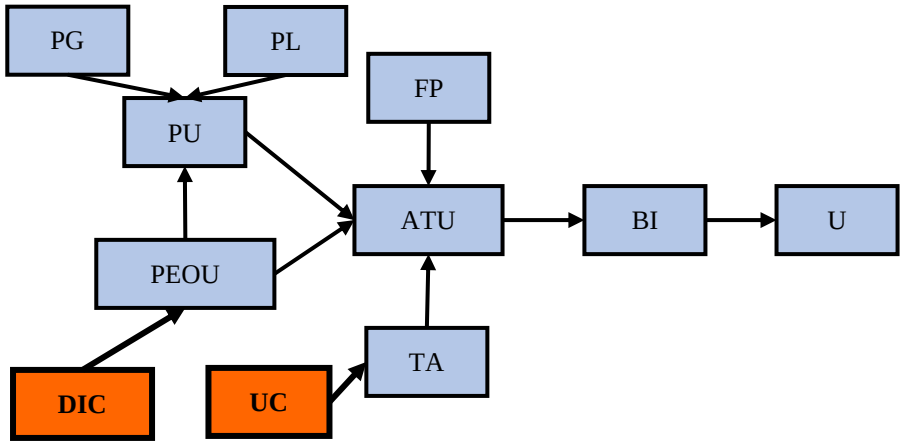


Rysunek 4.3. Budowa modelu DIAM – etap II
Źródło: opracowanie własne.

Zgodnie z postulatami VI, VII i IX, rozszerzono model (rysunek 4.4.) o **charakterystykę użytkownika** (postulat IX) i **stosowanych narzędzi uwierzytelnienia** (postulat VII). Mimo niewykrycia w pierwszym badaniu wstępnym zależności pomiędzy niektórymi parametrami narzędzi uwierzytelniających, włączono je do badanego modelu na podstawie badań literaturowych (postulat VI). Stąd:

Charakterystyka tożsamości cyfrowej (*Digital Identity Characteristic*, DIC) – obejmuje czynniki opisujące sposób korzystania z tożsamości cyfrowych w przedsiębiorstwie (wykorzystanie różnych narzędzi uwierzytelnienia, liczba haseł, ich skład, czasochłonność itp.).

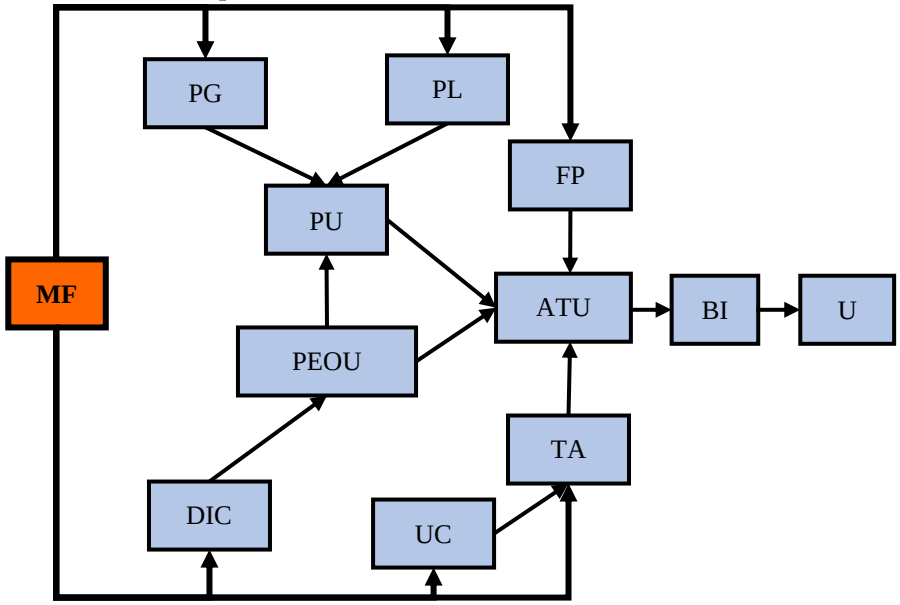
Charakterystyka użytkownika (*User Characteristic*, UC) – obejmuje czynniki związane z przymiotami pracownika (związek z branżą IT, samoocena wiedzy dotyczącej bezpiecznego wykorzystania uwierzytelnienia).



Rysunek 4.4. Budowa modelu DIAM – etap III
Źródło: opracowanie własne.

W związku z utylitarnym celem budowy modelu oraz postulatem IV, do modelu wprowadzono czynniki zarządcze (rysunek 4.5.).

Czynniki zarządcze (*Management Factors*, MF) to *czynniki związane z przedsiębiorstwem, organizacją ochrony zasobów systemów informatycznych oraz zarządzaniem kapitałem ludzkim*.



PU – Postrzegana użyteczność
PEOU – Postrzegana łatwość użycia
ATU – Postawa wobec tożsamości
BI – Intencja użycia
U – Użycie
TA – Świadomość zagrożeń
PG – Postrzegane korzyści
PL – Postrzegane straty
FP – Postrzeganie wymuszenia
DIC – Charakterystyka tożsamości cyfrowej
UC – Charakterystyka użytkownika
MF – Czynniki zarządcze

Rysunek 4.5. Budowa modelu DIAM – etap IV
Źródło: opracowanie własne.

4.3. Narzędzie badawcze

Zaproponowany model DIAM powinien zostać skwantyfikowany. Stąd potrzeba przeprowadzenia badania ilościowego. Kwestionariusz zaprojektowano tak, by pozwolił na zbadanie, jak stosowane są tożsamości cyfrowe w małych i średnich przedsiębiorstwach z perspektywy pracownika korzystającego z zasobów systemów informatycznych (perspektywa użytkowników uprzywilejowanych – administratorów systemów, nie jest przedmiotem tych rozważań), oraz umożliwił określenie siły relacji między elementami modelu DIAM. Podczas

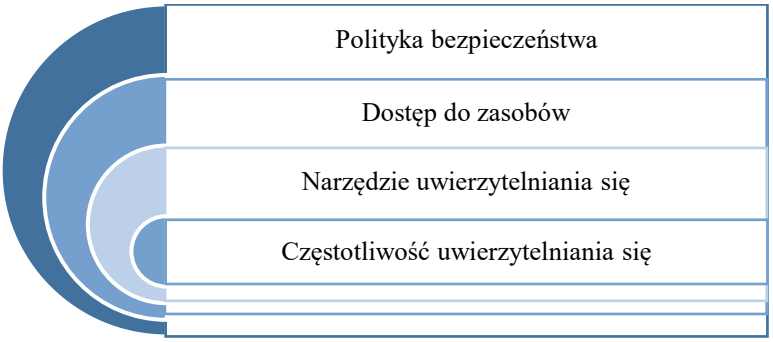
budowy kwestionariusza uwzględniono wskazówki metodologiczne dla badań małych i średnich przedsiębiorstw[264].

4.3.1. Konstrukcja pytań dotyczących zastosowania tożsamości cyfrowych

W celu pogłębionej analizy sytuacji przedsiębiorstw sektora małych i średnich przedsiębiorstw w obszarze tożsamości cyfrowych, wybrano następujące obszary do zbadania:

1. Organizacja procesu dostępu do zasobów systemów informatycznych w przedsiębiorstwach.
2. Działania użytkownika w kontekście bezpieczeństwa narzędzi uwierzytelnienia.
3. Ocena rozwiązań obecnie stosowanych przez pracowników.
4. Preferencje pracowników w kwestii organizacji dostępu do zasobów systemów informatycznych.

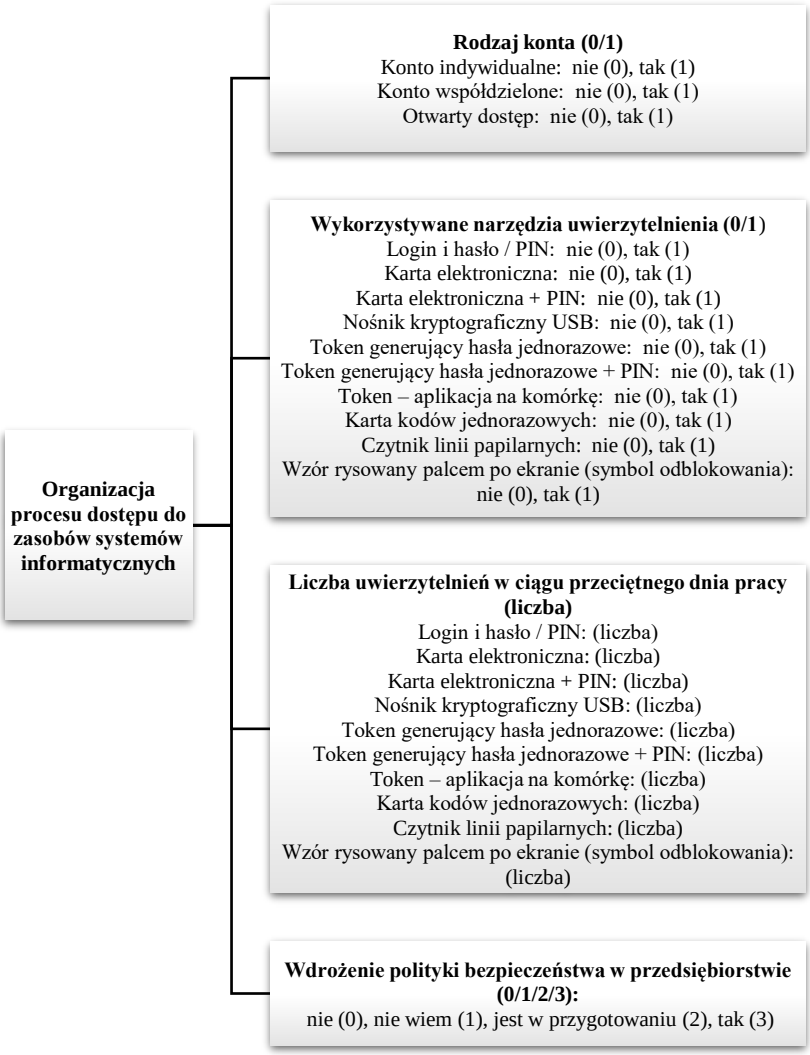
Ad. 1. Zbadano organizację dostępu do zasobów systemów informatycznych na czterech poziomach szczegółowości (rysunek 4.6.). Na ogólną organizację dostępu składają się zatem: wdrożenie polityki bezpieczeństwa, jako podstawy działań zapewniających bezpieczeństwo, jej implementację w obszarze sposobu przyznania dostępu do zasobów, stosowanych narzędzi uwierzytelnienia i częstotliwości ich używania.



Rysunek 4.6. Organizacja dostępu do zasobów systemów informatycznych – struktura
Źródło: opracowanie własne.

Aby ustalić w jaki sposób jest organizowany dostęp do zasobów systemów informatycznych w MSP, opracowane zostały badane zagadnienia wraz z wariantami odpowiedzi i sposobem ich oznaczenia – rysunek 4.7.

[264] Michna, A. (2008). *Specyfika przeprowadzania badań kwestionariuszowych w sektorze małych i średnich przedsiębiorstw*. Organizacja i Zarządzanie, Kwartalnik Naukowy Nr 3, Gliwice: Wydawnictwo Politechniki Śląskiej, s. 83–96.



Rysunek 4.7. Organizacja dostępu do zasobów systemów informatycznych – badane zagadnienia
Źródło: opracowanie własne.

Ad. 2. Działania użytkownika w kontekście bezpieczeństwa narzędzi uwierzytelnienia dotyczą tylko dwóch metod uwierzytelnienia (opartych o wiedzę i przedmiot), ponieważ przyjęto, że w przypadku metod biometrycznych, ciężar zapewnienia bezpieczeństwa leży wyłącznie po stronie przedsiębiorstwa.

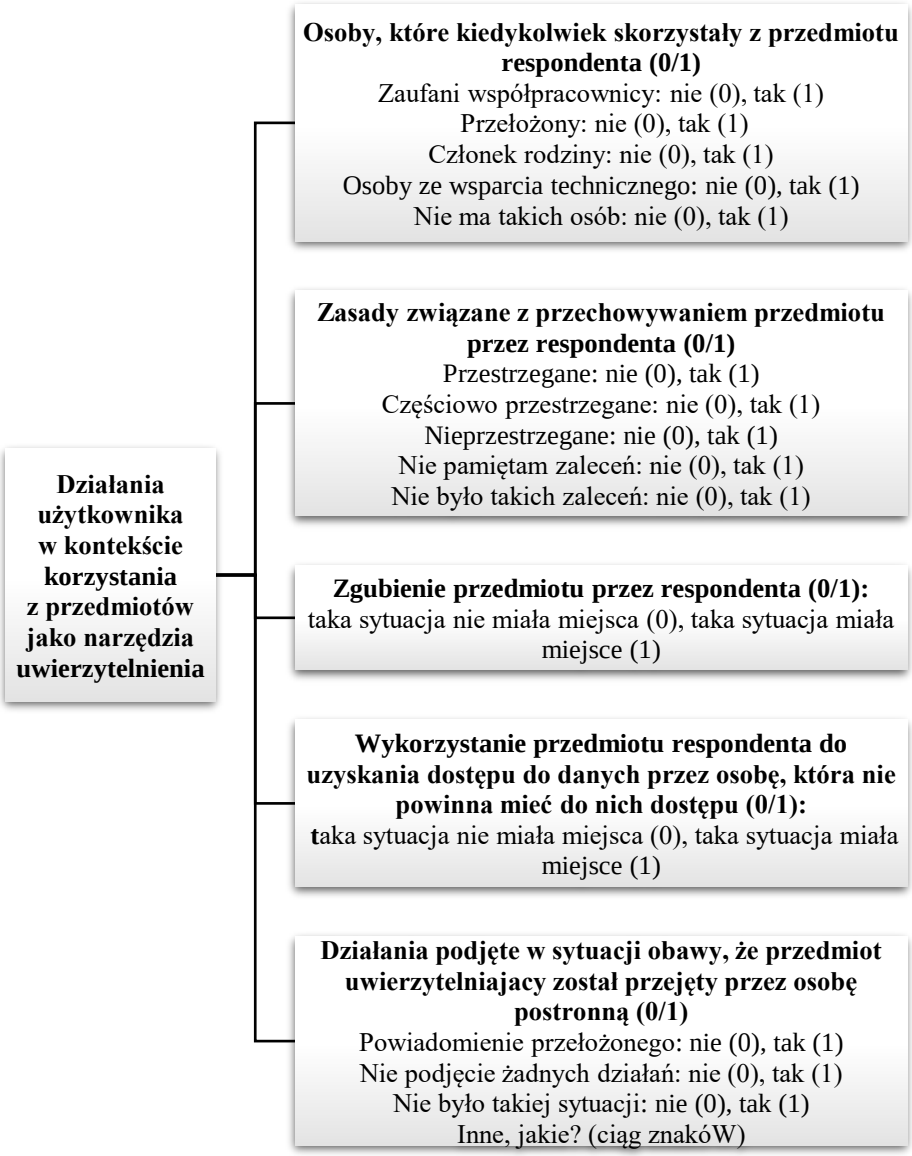
Wyszczególniono trzy obszary zapewnienia bezpieczeństwa zasobów w kontekście wykorzystywanego narzędzia uwierzytelniania. Poszczególne pytania przygotowano z uwzględnieniem specyfiki obydwóch narzędzi uwierzytelnienia (tabela 4.3.).

Tabela 4.3. Działania użytkownika w kontekście bezpieczeństwa narzędzi uwierzytelnienia - struktura

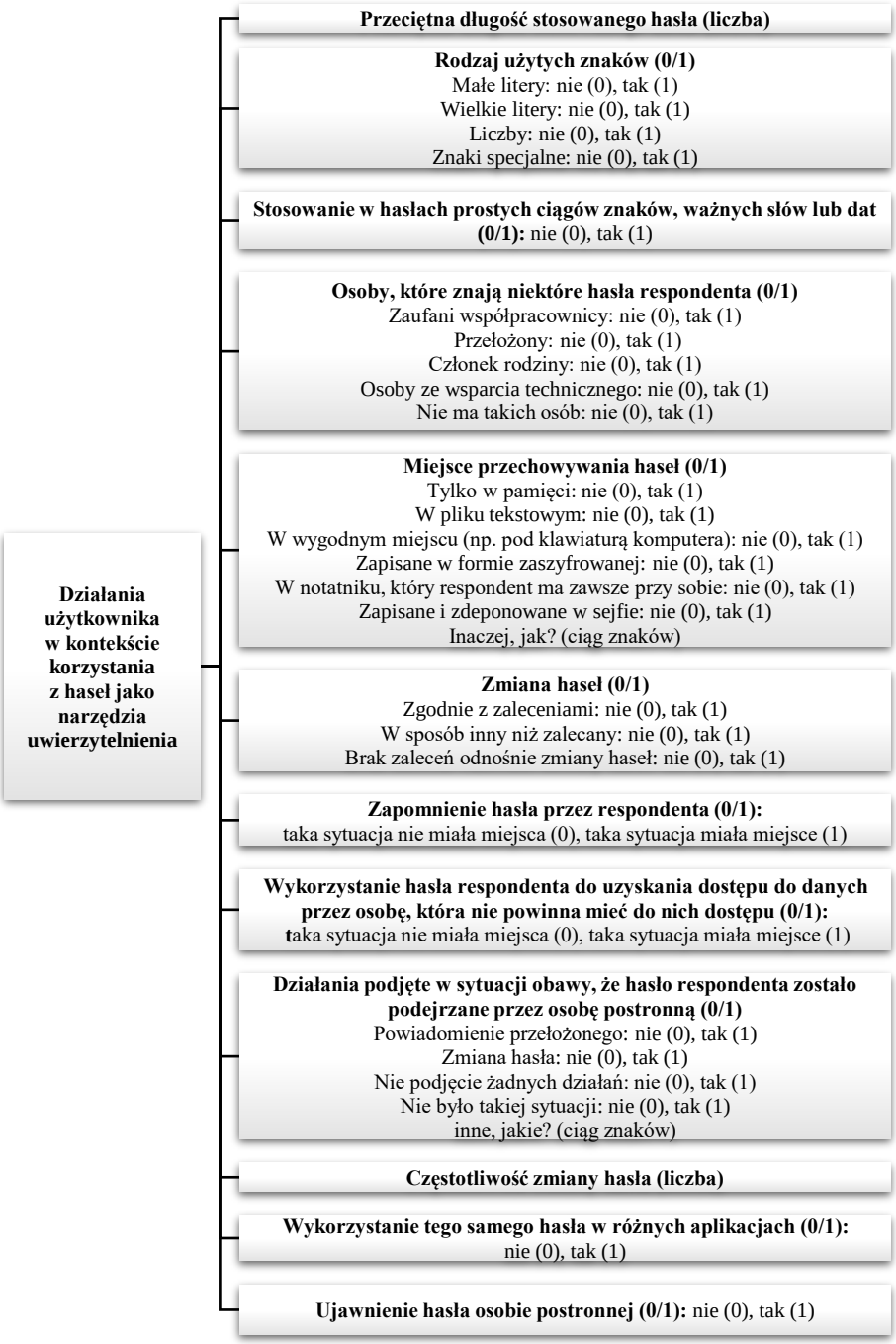
	Hasła	Przedmioty
Budowa	• długość • rodzaj użytych znaków • ryzykowna treść	
Ochrona narzędzia	• osoby, które znają hasła respondenta • sposób przechowywania	• osoby, które skorzystały z przedmiotu respondenta
Sposób użytkowania	• postępowanie zgodnie z zasadami • utrata hasła • nieautoryzowany dostęp z użyciem hasła • działanie podjęte w przypadku wystąpienia incydentu naruszenia bezpieczeństwa • częstotliwość zmiany • wykorzystanie w różnych aplikacjach tego samego hasła • ujawnienie osobie postronnej	• postępowanie zgodnie z zasadami • utrata przedmiotu • nieautoryzowany dostęp z użyciem przedmiotu • działanie podjęte w przypadku wystąpienia incydentu naruszenia bezpieczeństwa

Źródło: opracowanie własne.

Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich oznaczenia przedstawiono na rysunku 4.8. oraz na rysunku 4.9.



Rysunek 4.8. Działania użytkownika w kontekście bezpieczeństwa przedmiotów jako narzędzi uwierzytelnienia – badane zagadnienia
Źródło: opracowanie własne.



Rysunek 4.9. Działania użytkownika w kontekście bezpieczeństwa haseł jako narzędzi uwierzytelnienia – badane zagadnienia
Źródło: opracowanie własne.

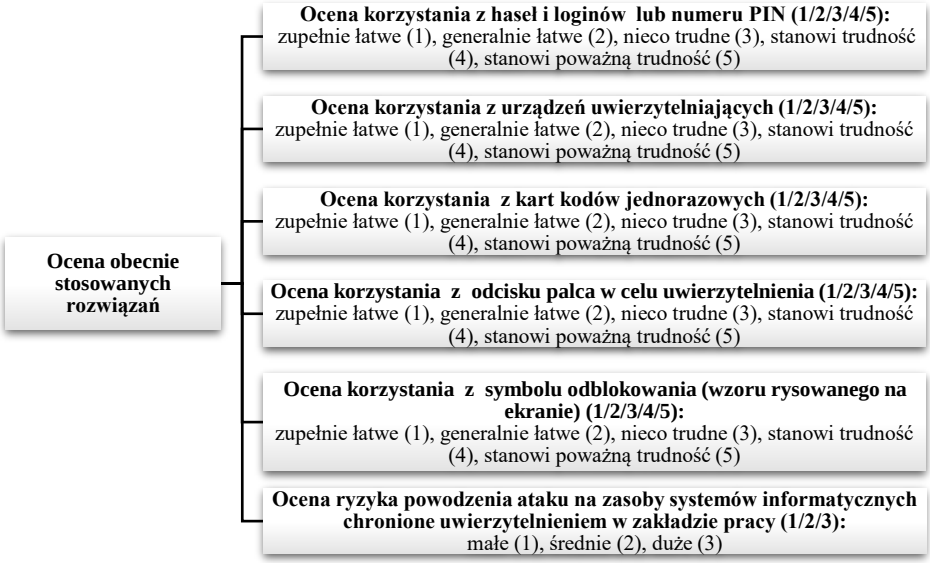
Ad. 3. W ocenie obecnie stosowanych rozwiązań przez pracowników MSP uwzględniono dwa aspekty:

- na ile stosowane uwierzytelnienia są postrzegane przez pracownika jako łatwe w użyciu,
- na ile stosowane uwierzytelnienia są postrzegane przez pracownika jako spełniające swoje zadanie ochrony zasobów przedsiębiorstwa.

Z uwagi na fakt, że respondent może korzystać z różnych narzędzi uwierzytelnienia, pogrupowano zidentyfikowane wcześniej narzędzia według podobieństwa użycia na:

1. Loginy i hasła lub numer PIN – jako bazujące na wiedzy (konieczność pamiętania lub przechowywania hasła).
2. Urządzenia uwierzytelniające – czyli karty elektroniczne z i bez numeru PIN , nośniki USB, tokeny, jako wymagające użycia przedmiotu elektronicznego.
3. Karty kodów jednorazowych – czyli przedmiotu, który wymaga dodatkowych działań manualnych i nie posiada cech urządzenia elektronicznego (np. baterii).
4. Czytniki palca – jako najbardziej rozpowszechnionej metody biometrycznej.
5. Symbol odblokowania – czyli metody łączącej metodę opartej na wiedzy użytkownika z koniecznością działań manualnych.

Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.10.



Rysunek 4.10. Ocena stosowanych przez respondentów narzędzi uwierzytelnienia – badane zagadnienia
Źródło: opracowanie własne.

Ad. 4. Preferencje pracowników w kwestii organizacji dostępu do zasobów systemów informatycznych zbadano w następujących obszarach:

1. Preferowane narzędzie uwierzytelnienia.
2. Preferowana liczba stosowanych narzędzi uwierzytelnienia.
3. Preferowane zasady dotyczące haseł (jeśli hasło byłoby preferowanym narzędziem).

Preferencje respondentów były badane tak, by wcześniej respondent mógł wyrobić sobie zdanie na temat poszczególnych narzędzi uwierzytelnienia, a potem wyrazić swoją opinię na ich temat.

Jako, że celem tego pytania jest poznanie, jaki poziom bezpieczeństwa respondenci byliby skłonni zaakceptować, uwzględniając konieczność poświęcania własnych sił i czasu, narzędzia uwierzytelnienia pogrupowano według poziomu zapewnianego bezpieczeństwa na:

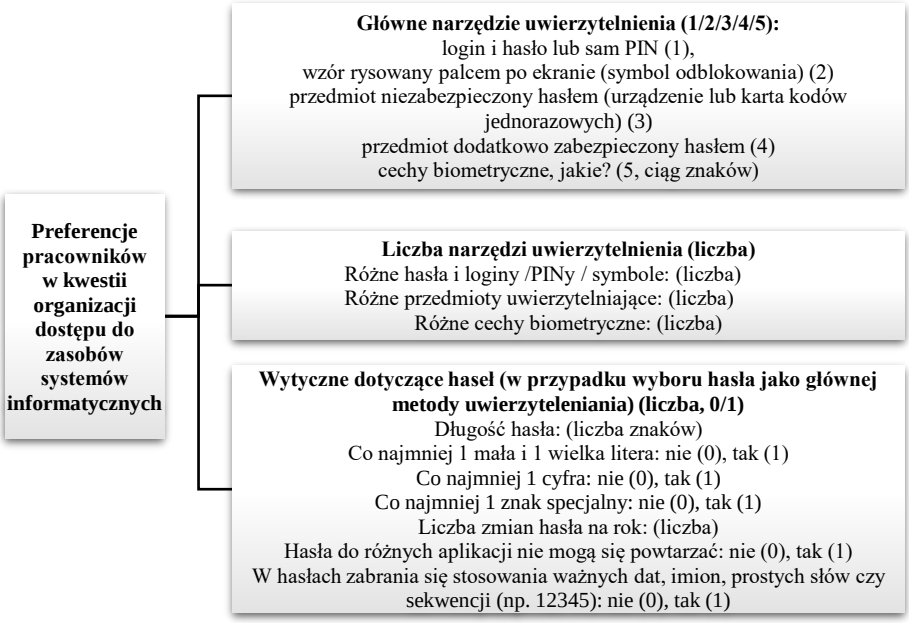
- wzór rysowany palcem po ekranie (symbol odblokowania),
- login i hasło lub numer PIN,
- przedmiot niezabezpieczony hasłem (urządzenie lub karta kodów jednorazowych),
- przedmiot dodatkowo zabezpieczony hasłem,
- cechę biometryczną.

Dla uproszczenia określenia preferowanej liczby narzędzi uwierzytelniających, co z założenia ma być tylko pewnym szkicem sposobu zabezpieczenia dostępu do zasobów systemów informatycznych, narzędzia podzielono na podstawowe grupy: bazujące na wiedzy, posiadanym przedmiocie, cesze osobistej.

Z uwagi na fakt szerokiego zakresu możliwej implementacji wytycznych dotyczących haseł, oraz w celu porównania z obecnie stosowanymi zasadami, zasady dotyczące haseł pogrupowano na:

- charakterystykę ilościową (minimalna długość, minimalna liczba różnych typów znaków),
- charakterystykę jakościową (niepowtarzanie haseł w różnych aplikacjach, zakaz haseł słownikowych, prostych ciągów znaków, ważnych dat, słów itp.),
- częstotliwość zmiany hasła.

Opracowane zagadnienia wraz z odpowiedziami i sposobem ich zapisu przedstawiono na rysunku 4.11.



Rysunek 4.11. Preferencje użytkowników dotyczące haseł – badane zagadnienia
Źródło: opracowanie własne.

4.3.2. Konstrukcja pytań umożliwiających kwantyfikację modelu DIAM

W celu określenia znaczenia poszczególnych czynników modelu w zarządzaniu akceptacją tożsamości cyfrowych pracowników, opracowano pytania mierzące każdy element modelu.

4.3.2.1. PEOU – Postrzegana łatwość użycia tożsamości w sposób bezpieczny

Z uwagi na fakt, że respondenci mogą inaczej interpretować pojęcie „bezpieczne użycie", konieczne jest zdefiniowanie bezpiecznego korzystania z danego narzędzia. Stąd, pytanie dotyczące postrzeganej łatwości korzystania z poszczególnych narzędzi uwierzytelnienia powinno zostać poprzedzone opisem zawierającym informacje, które pozwolą respondentowi na udzielenie odpowiedzi.

Na podstawie analizy zaleceń dotyczących bezpieczeństwa haseł określono stosowanie hasła w sposób bezpieczny jako:

- długość hasła min. 14 znaków;
- w składzie ma co najmniej jedną wielką i małą literę, cyfrę i znak specjalny;
- nie może zawierać dat ani imion ważnych dla użytkownika;
- wszystkie hasła do kluczowych aplikacji muszą być różne;

- hasło musi być zmieniane minimum co miesiąc;
- hasło nie może być przechowywane w postaci niezaszyfrowanej lub w miejscu, gdzie jest łatwo dostępne;
- hasło nie może być znane nikomu w miejscu pracy ani poza nim.

Bezpieczeństwo urządzenia uwierzytelniającego, które może zapewnić pracownik, opisano w następujący sposób:

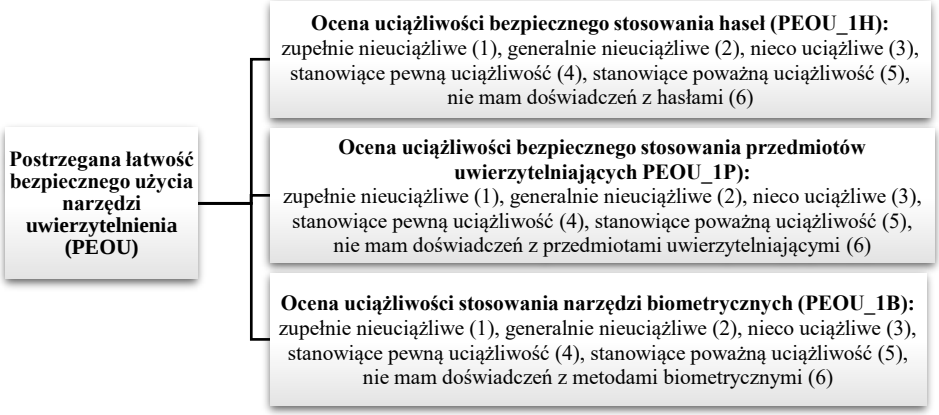
- urządzenie/karta byłaby pieczołowicie przechowywana (np. stale noszona przy sobie, ew. złożona w sejfie lub bardzo bezpiecznym miejscu) i nieprzekazywana nikomu innemu;
- ewentualne dodatkowe zabezpieczenie (PIN) nie byłoby nigdzie zapisane, ani nikomu przekazywane.

W przypadku uwierzytelnienia biometrycznego pracownik nie ma właściwie wpływu na poziom bezpieczeństwa zasobów systemów informatycznych i czynnikiem wpływającym na postrzeganą łatwość użycia są potencjalne błędy odczytu danych biometrycznych. Stąd, dla celów estymacji obciążenia przez użytkownika, wskazano następujące czynniki wpływające na komfort użytkowanie narzędzi opartych o cechy osobiste:

- wrażliwość na tymczasowe zmiany cech fizycznych / behawioralnych tj. otarcia naskórka / skaleczenia (odcisk palca), chrypka / przeziębienie (głos), spuchnięcie twarzy (geometria twarzy);
- wrażliwość na zmiany warunków odczytu np. oświetlenia (geometria twarzy).

Założono, że ocena łatwości użycia danego narzędzia może być dokonywana tylko przez osoby, które mają doświadczenie z daną metodą. Stąd do zestawu odpowiedzi dodano odpowiedź *Nie mam doświadczeń…*

Badane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.12.



Rysunek 4.12. Ocena łatwości użycia poszczególnych narzędzi uwierzytelnienia (PEOU) – badane zagadnienia
Źródło: opracowanie własne.

4.3.2.2. PG – Postrzegane korzyści z bezpiecznego korzystania z tożsamości cyfrowych

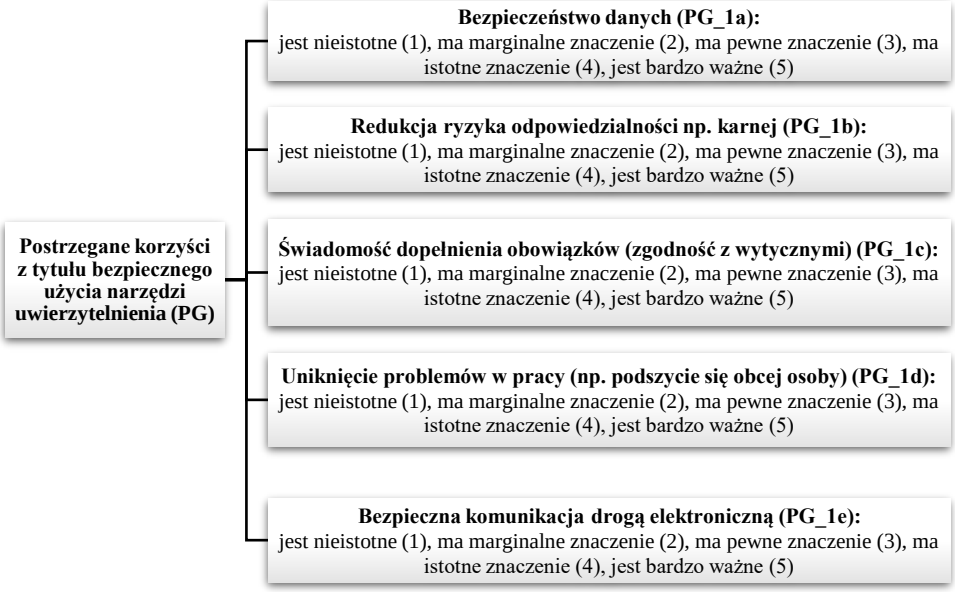
Postrzegane korzyści z tytułu bezpiecznego korzystania z tożsamości cyfrowej wyznaczono w ramach dwóch grup (tabela 4.4.): korzyści dla przedsiębiorstwa (w ramach dwóch podstawowych zastosowań tożsamości cyfrowej), oraz korzyści dla respondenta jako pracownika (rozpatrywane z punktu widzenia pozytywnej i negatywnej motywacji).

Tabela 4.4. Postrzegane korzyści z tytułu bezpiecznego stosowania tożsamości cyfrowych – struktura

Korzyści dla przedsiębiorstwa	Korzyści dla pracownika
• Bezpieczeństwo danych • Bezpieczna komunikacji	• Uniknięcie następstw niewłaściwego użycia tożsamości cyfrowej • Świadomość dopełnienia obowiązków

Źródło: opracowanie własne.

Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.13.



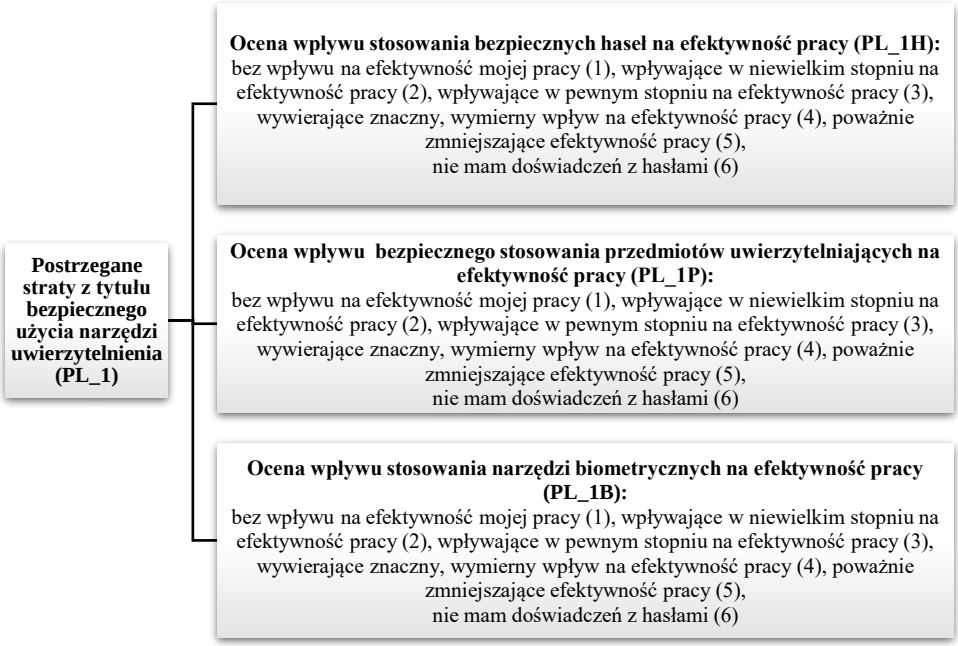
Rysunek 4.13. Postrzegane korzyści z tytułu bezpiecznego użycia narzędzi uwierzytelnienia (PG) – badane zagadnienia
Źródło: opracowanie własne.

W celu uproszczenia utworzono wskaźnik PG – poziom postrzegania korzyści – jako średnią arytmetyczną wartości PG_1a do PG_1e. Im wyższa wartość tego wskaźnika, tym wyższy jest poziom postrzeganych korzyści.

4.3.2.3. PL – Postrzegane straty z tytułu bezpiecznego korzystania z tożsamości cyfrowej

Postrzegane straty z tytułu bezpiecznego korzystania z tożsamości cyfrowych określono w oparciu o definicje bezpiecznego użycia, zawarte w konstrukcji pytań dotyczących postrzeganej łatwości użycia. Straty mierzono poziomem wpływu na efektywność pracy osobno dla każdej metody uwierzytelnienia.

Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.14.



Rysunek 4.14. Postrzegane straty z bezpiecznego użycia narzędzi uwierzytelnienia (PL_1) – badane zagadnienia
Źródło: opracowanie własne.

W celu zbadania jak są postrzegane czynniki ryzyka, wynikające ze stosowania tożsamości cyfrowych w ogóle, opracowano pytania, zawierające potencjalne ryzyka dla respondenta, związane z utratą tożsamości, specyficzne dla poszczególnych metod. Wyszczególniono dwie grupy zagrożeń związanych z ryzykiem utraty tożsamości cyfrowej: intencjonalne – związane z bezpośrednim atakiem na respondenta oraz nieintencjonalne – związane z ryzykiem kompro-

mitacji lub utraty dostępu do tożsamości cyfrowej (tabela 4.5.). Nie uwzględniano zagrożeń, na które wpływ mają inne czynniki np. techniczne.

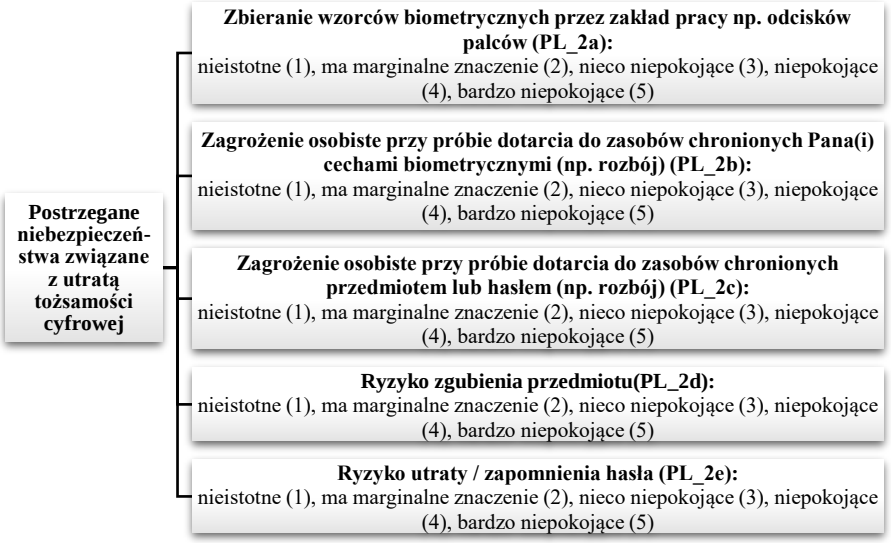
Tabela 4.5. Postrzegane zagrożenia z tytułu korzystania z narzędzi uwierzytelnienia (PL) – struktura

	Hasla	Przedmioty	Biometria
Ryzyka intencjonalne	Zagrożenie osobiste przy próbie dotarcia do zasobów chronionych hasłem (np. rozbój)	Zagrożenie osobiste przy próbie dotarcia do zasobów chronionych z użyciem przedmiotu (np. rozbój)	Zagrożenie osobiste przy próbie dotarcia do zasobów chronionych cechami biometrycznymi (np. rozbój)
Ryzyka nieintencjonalne	Ryzyko utraty lub zapomnienia hasła	Ryzyko zgubienia przedmiotu	Zbieranie wzorców biometrycznych przez zakład pracy np. odcisków palców

Źródło: opracowanie własne.

Z uwagi na podobieństwa (podobne skutki dla respondenta), pytanie dotyczące ryzyka utraty lub zapomnienia hasła zostało połączone z pytaniem dotyczącym ryzyka zagubienia przedmiotu.

Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.15.



Rysunek 4.15. Postrzegane zagrożenia z tytułu korzystania z narzędzi uwierzytelnienia (PL_2) – badane zagadnienia
Źródło: opracowanie własne.

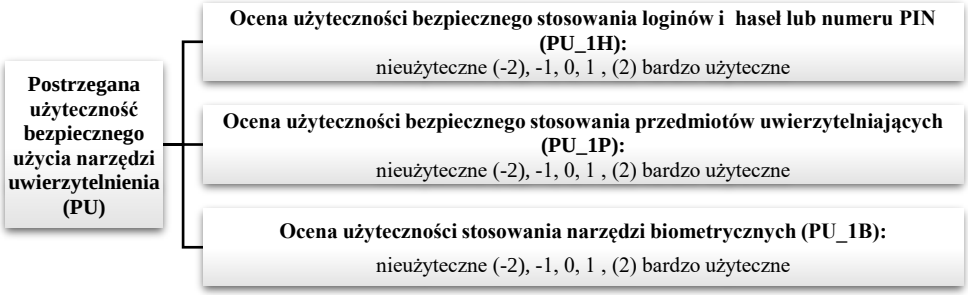
4.3.2.4. PU – Postrzegana użyteczność bezpiecznego korzystania z tożsamości cyfrowych

By umożliwić respondentowi dokonanie wyważonej oceny użyteczności bezpiecznego korzystania z tożsamości cyfrowych:

1. w kwestionariuszu badawczym przedstawiono pojęcie bezpiecznego korzystania z tożsamości cyfrowych (vide 4.3.2.1.),
2. przeprowadzono dyskusję wad i zalet bezpiecznego sposobu uwierzytelnienia (vide 4.3.2.2., 4.3.2.3.),
3. w treści pytania podkreślono konieczność rozważenia korzyści i obciążeń związanych z zapewnieniem bezpieczeństwa tożsamości cyfrowych.

Wykorzystano skalę semantyczną Osgooda od -2 do +2, gdzie -2 (nieużyteczny), +2 (bardzo użyteczny). Z uwagi na zróżnicowane korzyści i straty wynikające ze stosowania poszczególnych metod uwierzytelnienia, ocenę przeprowadzono dla każdej metody osobno.

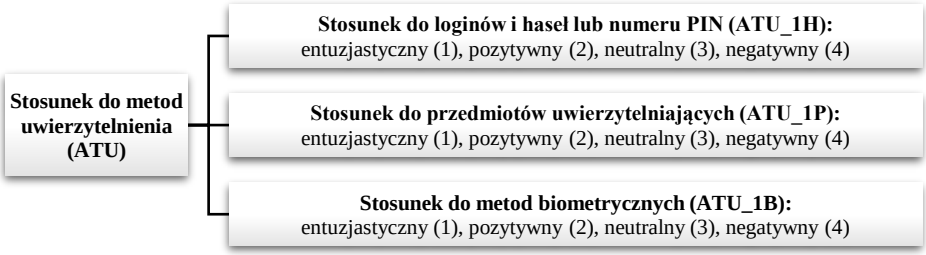
Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.16.



Rysunek 4.16. Postrzegana użyteczność bezpiecznego użycia narzędzi uwierzytelnienia (PU) – badane zagadnienia
Źródło: opracowanie własne.

4.3.2.5. ATU – Postawa wobec tożsamości cyfrowej

Do oceny postawy wobec tożsamości cyfrowej wybrano jej najistotniejszy komponent (emocjonalno-oceniający). Oceniano każdą z metod uwierzytelniających osobno. Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.17.



Rysunek 4.17. Postawa wobec tożsamości cyfrowej (ATU) – badane zagadnienia
Źródło: opracowanie własne.

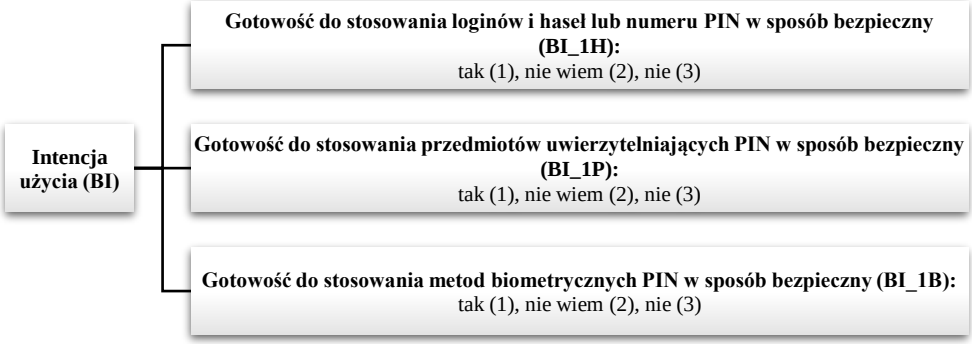
4.3.2.6. BI – Intencje użycia

By umożliwić respondentowi świadome określenie intencji użycia tożsamości cyfrowych w sposób bezpieczny:

1. w kwestionariuszu badawczym przedstawiono pojęcie bezpiecznego korzystania z tożsamości cyfrowych (vide 4.3.2.1.),
2. przeprowadzono dyskusję wad i zalet bezpiecznego sposobu uwierzytelnienia (vide 4.3.2.2., 4.3.2.3.),
3. wykrystalizowano nastawienie respondenta do poszczególnych narzędzi uwierzytelnienia (vide 4.3.2.4).

Zbadano osobno intencję użycia każdej z metod uwierzytelniających. Oprócz odpowiedzi jednoznacznie potwierdzającej („tak") i przeczącej („nie"), zastosowano odpowiedź unikową („nie wiem") w celu zapewnienia rzetelności odpowiedzi.

Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.18.



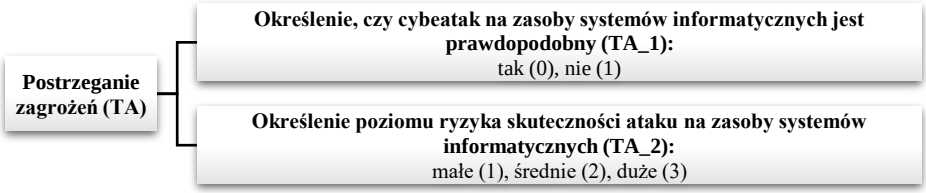
Rysunek 4.18. Intencje użycia (BI) – badane zagadnienia
Źródło: opracowanie własne.

4.3.2.7. TA – Świadomość zagrożeń

W celu określenia świadomości zagrożeń respondentów zbadano dwa elementy kluczowe:

1. świadomość, że zasoby systemów informatycznych zakładu pracy mogą stać się przedmiotem ataku,
2. świadomość, że działania respondenta przekładają się na bezpieczeństwo zasobów systemów informatycznych.

W tym celu przygotowano pytania dotyczące oceny prawdopodobieństwa ataku na zasoby systemów informatycznych przedsiębiorstwa oraz oceny prawdopodobieństwa tego ataku (rysunek 4.19.).



Rysunek 4.19. Postrzeganie zagrożeń (TA) – badane zagadnienia
Źródło: opracowanie własne.

Porównanie poziomu bezpieczeństwa, uzyskanego dzięki obecnemu sposobowi korzystania z tożsamości cyfrowej przez respondenta, z oceną ryzyka powodzenia cyberataku na zasoby informatyczne, pozwoli na określenie postrzegania przez respondenta swojej roli w zabezpieczaniu zasobów.

Wynik porównania może być następujący (patrz: tabela 4.6.):

- OK – gdy widoczna jest zgodność między postrzeganym ryzykiem powodzenia cyberataku na zasoby systemów informatycznych, a poziomem bezpieczeństwa obecnego stosowania tożsamości cyfrowej.
- W – wynik wątpliwy.
- NOK1 – wynik nieprawidłowy, który oznacza, że respondent nie ma świadomości, że naraża zasoby systemów informatycznych.
- NOK2 – wynik, który może sugerować bardzo wysoką świadomość w obszarze bezpieczeństwa zasobów lub istnienie dodatkowego czynnika, wpływającego na ocenę respondenta.

Tabela 4.6. Ocena świadomości respondenta dotyczącej jego roli w ochronie zasobów systemów informatycznych

		Ryzyko powodzenia cyberataku na zasoby informatyczne		
		Małe	**Średnie**	**Duże**
Bezpieczeństwo aktualnego użycia tożsamości cyfrowych	**Niskie**	NOK1	W	OK
	Średnie	W	OK	W
	Wysokie	OK	W	NOK2

Źródło: opracowanie własne.

Stąd, podczas analizy wyniki zapisywane będą w sposób następujący:

- 1 – zgodność (OK),
- 2 – wynik nieokreślony (w tym: wynik W oraz NOK2),
- 3 – niezgodność (NOK1).

W celu oceny bezpieczeństwa aktualnego użycia tożsamości cyfrowych, określono czynniki, które wpływają na bezpieczeństwo uwierzytelnienia oraz leżą, lub mogą leżeć w gestii respondenta. Rozpatrzono sytuację, gdy respondent posługiwał się hasłem oraz przedmiotem. Przyjęto, że bezpieczeństwo uwierzytelnienia biometrycznego nie zależy od użytkownika.

Czynniki wpływające na bezpieczeństwo użycia zostały podzielone na dwie kategorie, które pozwalają na określenie poziomu bezpieczeństwa uwierzytelnienia respondenta:

- Czynniki krytyczne – stanowią trzon i określają wyjściowy poziom bezpieczeństwa. Aby zakwalifikować sposób uwierzytelnia się danego respondenta do określonego poziomu bezpieczeństwa, muszą być spełnione wszystkie czynniki krytyczne.
- Czynniki dopełniające – czyli obniżające poziom bezpieczeństwa określony przez czynniki krytyczne. Przyjęto, że każdy z czynników posiada tę samą wagę tj. 1 punkt, przy czym -1 oznacza obniżenie, a 1 podwyższenie bezpieczeństwa, 0 natomiast brak wpływu na poziom bezpieczeństwa. Czynniki te mogą się kompensować tj. liczona jest wypadkowa liczba punktów, która powinna wynieść nie mniej niż 0. Jeśli jest niższa, poziom bezpieczeństwa ulega zmniejszeniu (z wysokiego na średni lub ze średniego na niski). W przypadku czynników dopełniających, nie jest wymagane udzielenie wszystkich odpowiedzi przez respondenta.

Za pomocą metody delfickiej oraz analizy zaleceń dotyczących bezpieczeństwa haseł określono poszczególne poziomy bezpieczeństwa: wysoki (tabela 4.7.) i średni (tabela 4.8.). Poziom niski oznacza niespełnienie wymogów poziomu średniego.

Tabela 4.7. Poziom bezpieczeństwa wysoki – wymogi minimalne (czynniki krytyczne) i dodatkowe (czynniki dopełniające)

Czynniki krytyczne		Czynniki dopełniające		
Czynnik	**Wartość wymagana**	**Czynnik**	**Wartość pożądana**	**Punktacja**
Długość hasła	Min. 8 znaków	Dodatkowe narzędzie uwierzytelnienia	Tak	0 / 1
Częstotliwość zmiany hasła	Min. co 60 dni	Posiadanie indywidualnego konta	Tak	-1 / 1
Skład hasła	Min. 3 grupy znaków	Nie stosowanie sekwencji, ważnych dat itp. w haśle	Tak	-1 / 1
Sposób przechowywania hasła	Niejawny	Sposób przechowywania hasła	W sposób zaszyfrowany	-1 / 0 / 1
		Ujawnienie hasła lub przekazanie przedmiotu innym osobom	Nie	-1 / 1
		Stosowanie jednego hasła do różnych celów	Nie	-1 / 1

Źródło: opracowanie własne.

Tabela 4.8. Poziom bezpieczeństwa średni – wymogi minimalne (czynniki krytyczne) i dodatkowe (czynniki dopełniające)

Czynniki krytyczne		Czynniki dopełniające		
Czynnik	**Wartość wymagana**	**Czynnik**	**Wartość pożądana**	**Punktacja**
Długość hasła	Min. 8 znaków	Dodatkowe narzędzie uwierzytelnienia	Tak	0 / 1
Częstotliwość zmiany hasła	Min. raz na rok	Posiadanie indywidualnego konta	Tak	-1 / 1
Skład hasła	Min. 2 grupy znaków	Nie stosowanie sekwencji, ważnych dat itp. w haśle	Tak	-1 / 1
Sposób przechowywania hasła	Niejawny	Sposób przechowywania hasła	W sposób zaszyfrowany	-1 / 0 / 1
		Ujawnienie hasła innym osobom	Nie	-1 / 1
		Stosowanie jednego hasła do różnych celów	Nie	-1 / 1

Źródło: opracowanie własne.

4.3.2.8. FP – Postrzeganie wymuszenia

Postrzeganie wymuszenia zdecydowano określać w oparciu o pobudki, jakimi kieruje się respondent korzystając z kont. Pobudki podzielono na:

- przymus (konieczność), gdy brak uwierzytelnienia oznacza brak dostępu do danych i niemożność wykonania obowiązków;
- motywację wewnętrzną, czyli przekonanie, że korzystanie z tożsamości cyfrowej przynosi korzyść dla respondenta lub jego zakładu pracy;
- motywację zewnętrzną, czyli ogół działań podejmowanych przez przełożonych.

Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.20.

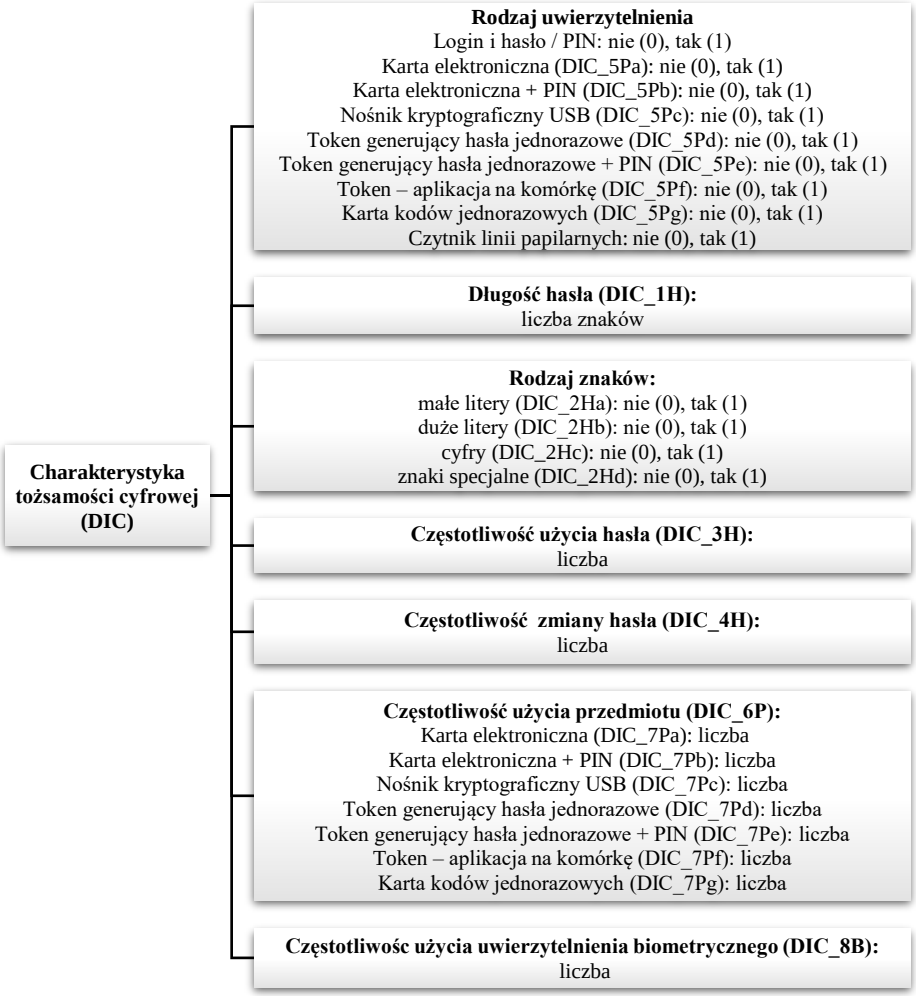
Rysunek 4.20. Postrzeganie wymuszenia – badane zagadnienia
Źródło: opracowanie własne.

4.3.2.9. DIC – Charakterystyka tożsamości cyfrowej

Charakterystyka tożsamości cyfrowej to czynniki opisujące wybrane parametry charakterystyczne dla poszczególnych narzędzi: loginów i haseł lub numerów PIN, przedmiotów służących uwierzytelnieniu oraz narzędzi biometrycznych.

Wybrano elementy, które mogą mieć wpływ na łatwość użytkowania i efektywność pracy respondenta. Z uwagi na konsekwentne pomijanie aspektów czysto technicznych (np. parametry tokena lub skanera wykorzystywanego przez respondenta), pełna charakterystyka tożsamości cyfrowej będzie odnosić się tylko do loginów i haseł lub numerów PIN (tj. częstotliwość użycia, długość hasła oraz liczba grup znaków, z których składa się hasło). Uwierzytelnienie z użyciem przedmiotów i biometrii charakteryzowane będzie przez jeden parametr – częstotliwość użycia.

Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.21.



Rysunek 4.21. Charakterystyka tożsamości cyfrowej (DIC) – badane zagadnienia
Źródło: opracowanie własne.

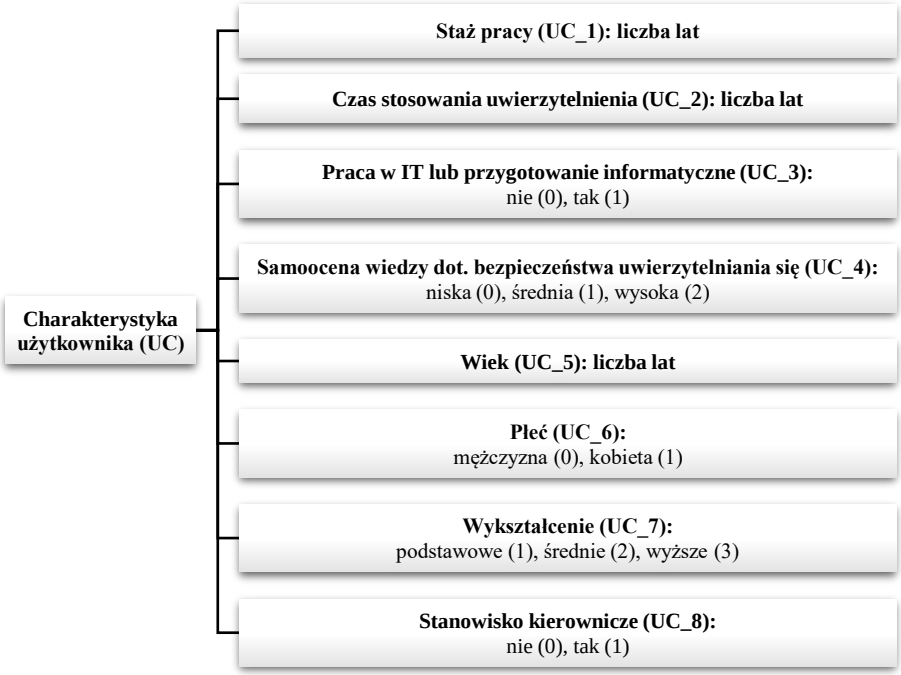
4.3.2.10. UC – Charakterystyka użytkownika

W ramach charakterystyki użytkownika, która może wpływać na sposób wykorzystania tożsamości cyfrowej wyodrębniono czynniki:

- demograficzne (płeć, wiek),
- związane z poziomem wiedzy (wykształcenie, samoocena wiedzy dotyczącej bezpieczeństwa uwierzytelniania się, kompetencje cyfrowe),

- związane z miejscem pracy (rodzaj stanowiska, staż pracy i czas stosowania uwierzytelnienia).

Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.22.



Rysunek 4.22. Charakterystyka użytkownika (UC) – badane zagadnienia
Źródło: opracowanie własne.

4.3.2.11. MF – Czynniki zarządcze

Czynniki zarządcze zidentyfikowano w ramach:

- zarządzania przez bezpośredniego przełożonego (MFA),
- zarządzania w ramach całej organizacji (MFB).

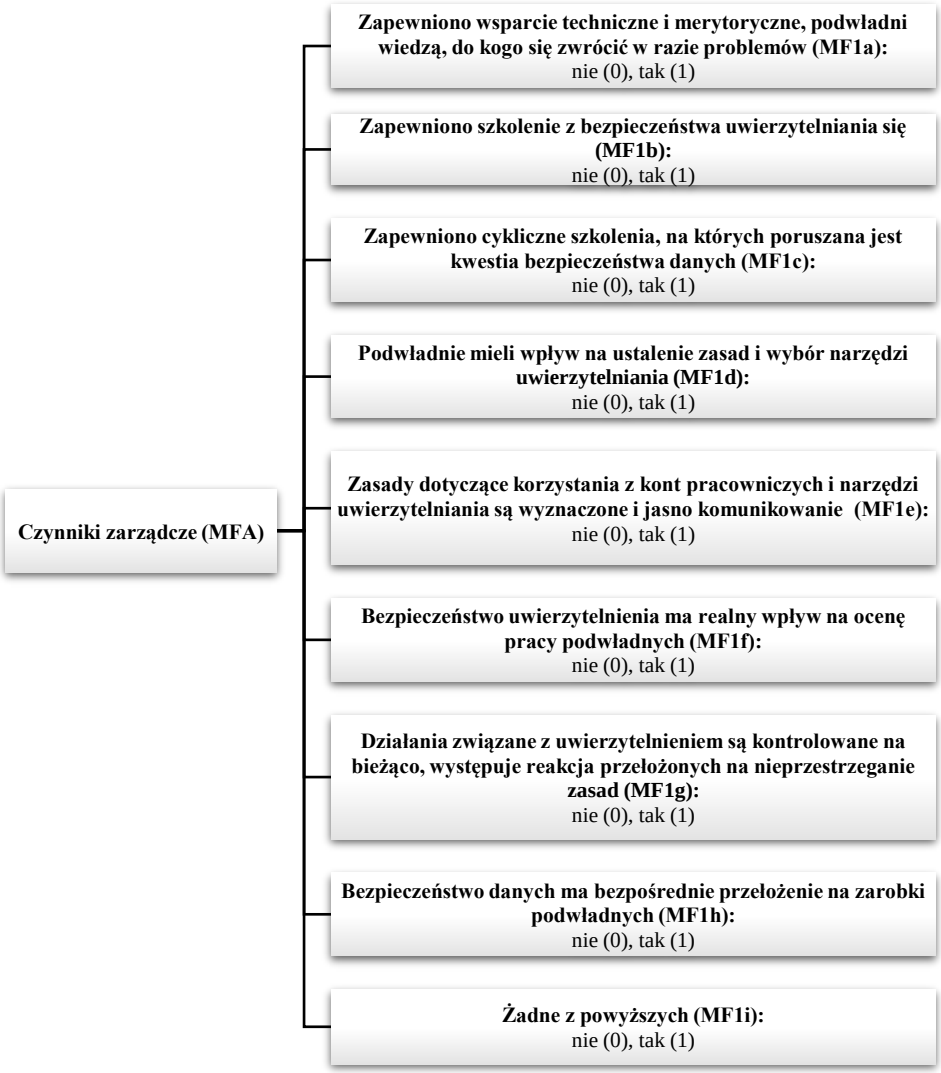
Uwzględniając funkcje zarządzania, zidentyfikowano działania, które mogą być podejmowane przez bezpośredniego przełożonego w celu zapewnienia właściwego korzystania z tożsamości cyfrowych, jako:

- zaangażowanie pracowników w proces planowania zasad i narzędzi uwierzytelniania,
- określenie zasad i ich jasne komunikowanie,
- organizowanie zasobów w celu sprawnego wypełniania powierzonych zadań w sposób określony wyznaczonymi zasadami,
- zapewnienie przygotowania merytorycznego pracowników do postępowania zgodnie z wytyczonymi zasadami z uwzględnieniem konieczności odświeżania wiedzy,

- finansowe i poza finansowe motywowanie pracowników,
- kontrolowanie przestrzegania zasad i reagowanie na ich łamanie.

Zarządzanie w ramach całego przedsiębiorstwa zbadano w trzech aspektach: przywództwa, stylu zarządzania oraz kompetencji. Z uwagi na większą trudność estymacji, do oceny wprowadzono skalę Likerta.

Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunkach: 4.23. i 4.24.



Rysunek 4.23. Czynniki zarządcze MFA – badane zagadnienia
Źródło: opracowanie własne.

Rysunek 4.24. Czynniki zarządcze MFB – badane zagadnienia
Źródło: opracowanie własne.

W celu uproszczenia analiz utworzono następujące wskaźniki:

1. MF_5 – poziom przywództwa – jako średnią arytmetyczną MF_2a do MF_2e.
2. MF_6 – poziom stylu zarządzania – jako średnią arytmetyczną MF_3a do MF_3e.
3. MF_7 – poziom kompetencji – jako średnią arytmetyczną MF_4a do MF_4c.
4. MF – poziom czynników zarządczych na poziomie organizacji – jako średnią arytmetyczną MF_2a do MF_4c. Im wyższa wartość MF tym lepiej zarządzana organizacja.

4.3.2.12. U – Bezpieczeństwo użycia tożsamości cyfrowej

Wyodrębniono trzy grupy czynników, które wpływają na bezpieczeństwo użycia tożsamości cyfrowych: parametry narzędzia uwierzytelniającego, zachowania użytkownika oraz rozwiązania organizacyjne (tabela 4.9.).

Z uwagi na fakt, że przeciętny użytkownik może nie być świadomy parametrów technicznych urządzeń uwierzytelniających oraz skanerów do odczytu danych biometrycznych, badając parametry techniczne narzędzia uwierzytelniającego, uwzględniono te elementy, które są użytkownikowi znane. Skupiono się zatem na parametrach haseł.

Zachowanie użytkownika, jako czynnik wpływający na bezpieczeństwo danych, rozważano w kontekście użytkowania loginów i haseł oraz przedmiotów uwierzytelniających, gdyż konsekwentnie przyjęto, że osoba posługująca się uwierzytelnieniem biometrycznym nie ma właściwie wpływu na bezpieczeństwo tożsamości cyfrowych.

Tabela 4.9. Bezpieczeństwo użycia tożsamości cyfrowej (U) ─struktura

Parametry haseł	Zachowanie użytkownika	Rozwiązania organizacyjne
• długość • skład • częstotliwość zmiany	• ochrona dostępu do hasła lub przedmiotu • wykorzystywanie jednego hasła do różnych celów • spełnianie wytycznych odnośnie bezpiecznego stosowania narzędzi uwierzytelnienia • postępowanie podczas wystąpienia incydentu naruszenia bezpieczeństwa	• indywidualizacja przyznanego dostępu • narzędzie uwierzytelnienia • dodatkowe zabezpieczenia systemu • wytyczne odnośnie bezpiecznego stosowania narzędzi uwierzytelnienia

Źródło: opracowanie własne.

Wyszczególnione elementy wpływające na bezpieczeństwo stosowania tożsamości cyfrowych podzielono na dwie grupy: te dotyczące haseł (tabela 4.10.) oraz te, które dotyczą korzystania z przedmiotów uwierzytelniających (tabela 4.11.).

Opracowane zagadnienia wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.25., rysunku 4.26. i rysunku 4.27.

Tabela 4.10. Elementy wpływające na bezpieczeństwo stosowania haseł

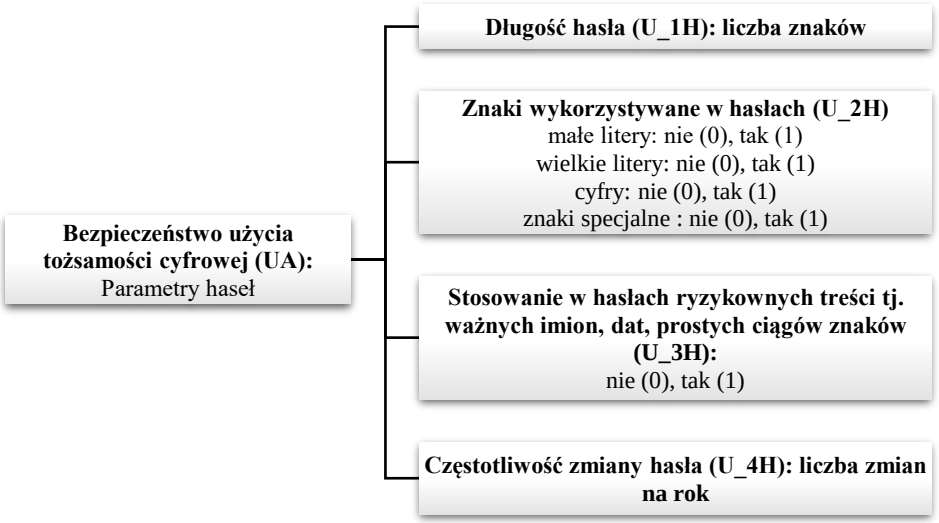
	Element	Wpływ na bezpieczeństwo użycia	
		Pozytywny	**Negatywny**
Parametry haseł	• długość hasła	• 8 znaków i więcej	• poniżej 8 znaków
	• liczba grup znaków wykorzystywanych w haśle	• 3 i więcej	• 1 lub 2
	• stosowanie w haśle ważnych dat, imion, sekwencji itp.	• Nie	• tak
	• częstotliwość zmiany hasła na rok	• 2 razy lub częściej	• rzadziej niż 2 razy rocznie
Zachowanie użytkownika	• przechowywanie hasła	• tylko w pamięci • zaszyfrowany plik • zapisane na kartce przechowywanej w sejfie	• w wygodnym miejscu np. pod klawiaturą komputera
	• udostępnianie hasła innym osobom	• nie	• tak
	• wykorzystywanie jednego hasła do różnych aplikacji	• nie	• tak
	• zmiana hasła zgodnie z zaleceniami	• tak	• nie
	• reakcja na sytuację, gdy mogła nastąpić kompromitacja hasła	• powiadomienie przełożonego • zmiana hasła	• brak reakcji
Rozwiązania organizacyjne	• sposób uzyskiwania dostępu do zasobów systemów informatycznych	• konto pracownicze indywidualne	• wyłącznie konto grupowe lub otwarty dostęp
	• zabezpieczenie przed podejrzeniem wprowadzanego hasła	• tak	• nie

Źródło: opracowanie własne.

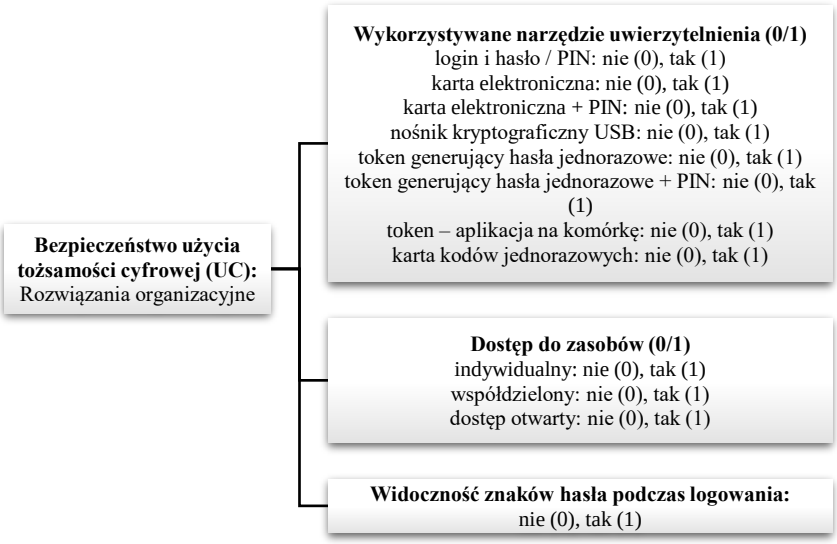
Tabela 4.11. Elementy wpływające na bezpieczeństwo stosowania przedmiotów uwierzytelniających

	Element	Wpływ na bezpieczeństwo użycia	
		Pozytywny	Negatywny
Zachowanie użytkownika	• Udostępnianie przedmiotu innym osobom	• Nie	• Tak
	• Przestrzeganie zasad związanych z przechowywaniem przedmiotu	• Tak • Częściowo tak	• Nie
	• Reakcja na sytuację, gdy mogło nastąpić przejęcie przedmiotu przez osobę postronną	• Powiadomienie przełożonego	• Brak reakcji
Rozwiązania	• Sposób uzyskiwania dostępu do zasobów systemów informatycznych	• Konto pracownicze indywidualne	• Wyłącznie konto grupowe lub otwarty dostęp

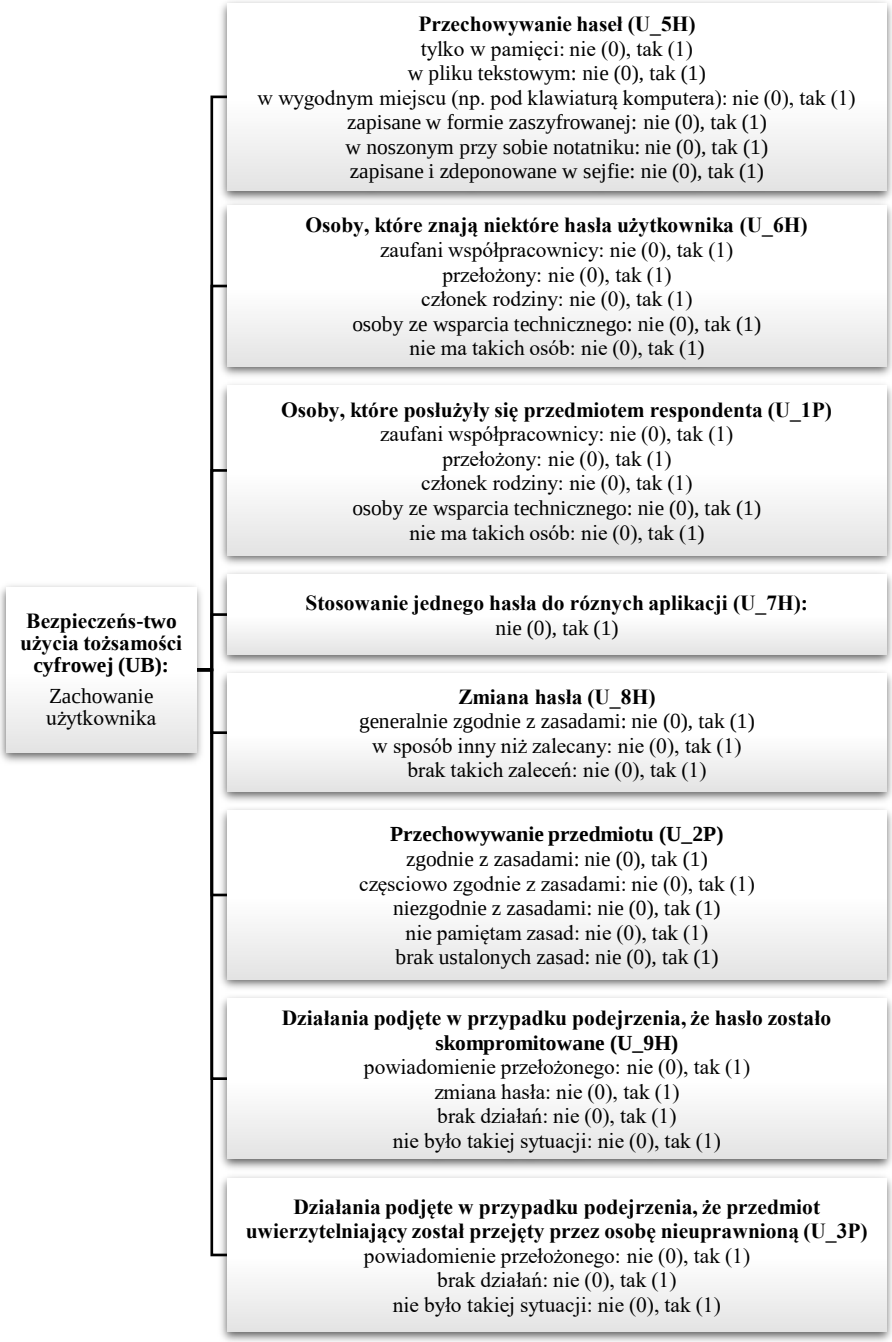
Źródło: opracowanie własne.



Rysunek 4.25. Bezpieczeństwo użycia tożsamości cyfrowej (UA): Parametry haseł – badane zagadnienia
Źródło: opracowanie własne.



Rysunek 4.26. Bezpieczeństwo użycia tożsamości cyfrowej (UC): Rozwiązania organizacyjne – badane zagadnienia
Źródło: opracowanie własne.



Rysunek 4.27. Bezpieczeństwo użycia tożsamości cyfrowej (UB): Zachowanie użytkownika – badane zagadnienia
Źródło: opracowanie własne.

4.3.3. Konstrukcja pytań umożliwiających zbadanie podejścia pracowników na stanowiskach kierowniczych i wykonawczych do kwestii bezpieczeństwa użycia tożsamości cyfrowych

W celu porównania jak kwestie bezpieczeństwa tożsamości cyfrowej postrzegają osoby pracujące na stanowiskach kierowniczych oraz wykonawczych, postawiono pytania badawcze:

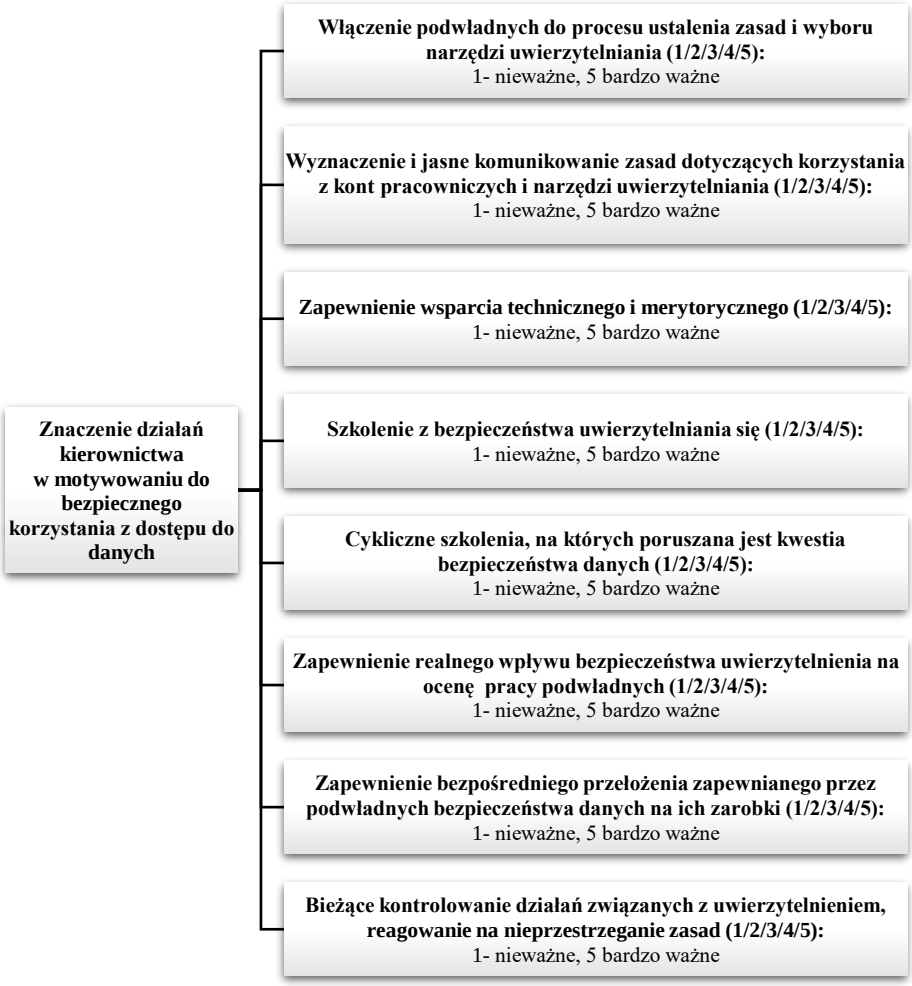
1. Czy poziom bezpieczeństwa użycia tożsamości cyfrowych przez respondentów z obu tych grup jest taki sam?
2. Czy są różnice w postrzeganiu znaczenia motywacji przełożonych do bezpiecznego korzystania z tożsamości cyfrowych między pracownikami na stanowiskach kierowniczych i wykonawczych?
3. Czy przynależność do grupy kierowników lub pracowników wykonawczych wpływa na postrzeganie optymalnego sposobu na zabezpieczenie dostępu do zasobów przedsiębiorstwa?

Aby udzielić odpowiedzi na postawione pytania zaplanowano następujące działania:

Ad. 1. Porównanie poziomu bezpieczeństwa haseł oraz przedmiotów, zapewnianego przez respondentów (kierowników i pracowników wykonawczych) według kryteriów zdefiniowanych w tabeli 4.10. oraz tabeli 4.11.
W celu dokonania porównań wykorzystano pytania przedstawione na rysunkach: 4.25., 4.26. i 4.27.

Ad. 2. Porównanie oceny siły wpływu działań przełożonych na motywację podwładnych do bezpiecznego korzystania z dostępu do danych, dokonanej przez kierowników i pracowników wykonawczych.

W tym celu skonstruowano pytanie badające jakie znaczenie mają wybrane działania przełożonych w motywowaniu do bezpiecznego korzystania z dostępu do danych (w skali od 1 – nieważne do 5 – bardzo ważne). Za podstawę przyjęto czynności zidentyfikowane w ramach konstruowania czynnika MFA (rysunek 4.23.), czyli te działania, które mogą być podejmowane przez bezpośredniego przełożonego. Opracowane zagadnienie wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.28.



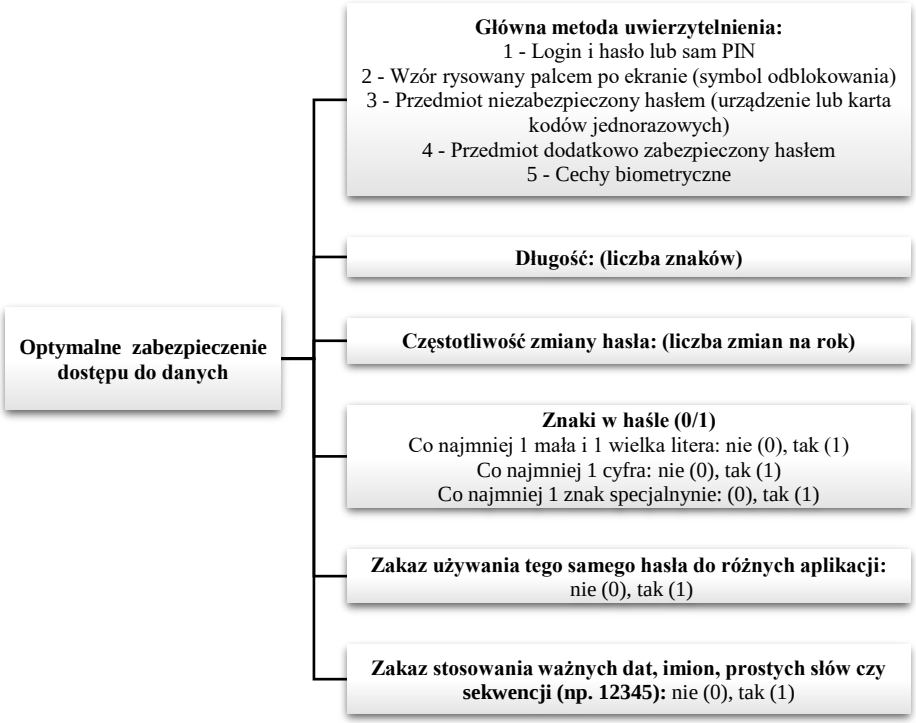
Rysunek 4.28. Ocena znaczenia działań kierownictwa w motywowaniu do bezpiecznego korzystania z dostępu do danych
Źródło: opracowanie własne.

Ad. 3. Porównanie optymalnych rozwiązań dla macierzystych przedsiębiorstw, wybranych przez kierowników i pracowników wykonawczych.

Optymalność rozwiązania została zdefiniowana jako zbalansowanie bezpieczeństwa danych, jak i wygody pracowników, w oparciu o doświadczenie i znajomość specyfiki macierzystych zakładów pracy respondentów. Wybrano następujące elementy:

1. Główną metodę uwierzytelnienia
2. Wytyczne do stosowania haseł

Opracowane zagadnienie wraz z wariantami odpowiedzi i sposobem ich zapisu przedstawiono na rysunku 4.29.



Rysunek 4.29. Optymalne zabezpieczenie danych według respondentów
Źródło: opracowanie własne.

4.3.4. Charakterystyka kwestionariusza badawczego

Z uwagi na obszerność kwestionariusza (7 stron, ponad 17.000 znaków i ponad 200 wariantów odpowiedzi) konieczne było umieszczenie pytań w określonej kolejności.

W pierwszej grupie pytań umieszczono zamknięte pytania o fakty i wprowadzające w temat. Mały one na celu zidentyfikowanie stosowanych przez respondentów narzędzi uwierzytelnień i sposobu ich wykorzystania.

Druga grupa pytań (głównie pytania sondujące i o motywy) dotyczyła odczuć respondentów w stosunku do poszczególnych narzędzi uwierzytelnienia. W przypadku niektórych pytań konieczne było uściślenie pojęć, by zapobiec dowolnej ich interpretacji. Na przykład określono, co można rozumieć pod pojęciem bezpiecznego hasła, by respondent mógł ocenić jego uciążliwość czy wpływ na efektywność pracy. Z początku, pytania pozwalały respondentom na określenie swojego zdania w kwestiach związanych z różnymi (pozytywnymi i negatywnymi) aspektami stosowanej przez nich tożsamości cyfrowej, co było

później podstawą do udzielenia wyważonej odpowiedzi na kolejne, złożone pytania. Na końcu postawiono trzy proste w formie pytania, dotyczące faktów, ale dotykające newralgicznych kwestii (m.in. określenie poziomu bezpieczeństwa informatycznego zakładu pracy).

Trzecia grupa pytań dotyczyła czynników związanych z przedsiębiorstwem. Zaczynała się pytaniami o motywy i opinie użytkownika, po których następowała dość obciążająca respondenta (monotonna) seria jednolitych w formie (skala Likerta) pytań, dotyczących różnych aspektów funkcjonowania macierzystego zakładu pracy.

Czwarta grupa złożona była z pytań hipotetycznych. Na bazie uświadomionego sposobu korzystania z uwierzytelnienia (pierwsza grupa pytań), dyskusji jego wad i zalet, wyrażonego stosunku wobec poszczególnych metod (druga grupa pytań) oraz rozważań związanych ze specyfiką macierzystego zakładu pracy, respondent został poproszony o nakreślenie zasad dotyczących uwierzytelnienia, które zapewniałyby akceptowalny poziom bezpieczeństwa, jednocześnie uwzględniający możliwie dużą wygodę użytkownika.

Piątą grupę stanowiły pytania metryczkowe dotyczące respondenta i jego zakładu pracy.

Kwestionariusz podzielono na cztery części, obejmujące wcześniej utworzone grupy pytań:

Część 1. Tożsamość cyfrowa pracowników i narzędzia uwierzytelnienia (I gr.)
Część 2. Postawa pracowników wobec tożsamości cyfrowej (II gr.)
Część 3. Zarządzanie postawą pracowników wobec tożsamości cyfrowej (II, IV gr.)
Część 4. Metryczka (V gr.)

Ostateczną postać kwestionariusza do badania kwantyfikującego model przedstawiono w załączniku 1.

Zakończenie

Badania literaturowe, a w szczególności analiza trendów i zmiany funkcjonowania społeczeństwa spowodowane pandemią SARS-CoV-2 potwierdziły znaczenie tożsamości cyfrowych, jako sposobu na korzystanie z zasobów cyfrowych. Przyspieszona i nasilona informatyzacja przedsiębiorstw, wzrost popularności i upowszechnienie się usług oferowanych przez Internet, ale i zagrożeń w sieci powodują, że bezpieczne stosowanie tożsamości cyfrowych staje się niezwykle ważne.

Dbałość o bezpieczeństwo wymaga nakładu czasu i wysiłku, co przekłada się na obniżenie efektywności pracy pracownika. Okazuje się, że pracownicy zaniedbują kwestie bezpieczeństwa, co stanowi istotne zagrożenie dla zasobów informatycznych przedsiębiorstw, w których pracują.

W niniejszej pracy podjęto próbę naukowego rozwiązania tego problemu. W tym celu określono ciąg działań prowadzących do utworzenia Modelu Akceptacji Tożsamości Cyfrowej DIAM. Na podstawie badań literaturowych, ale także eksploracji tego obszaru podczas badań wstępnych, zidentyfikowano szereg czynników, które mogą mieć wpływ na postawę pracownika, a przez to na korzystanie z tożsamości cyfrowych w przedsiębiorstwie w sposób bezpieczny.

Kwestie bezpieczeństwa są trudne do badania z dwóch powodów. Po pierwsze przedsiębiorstwa niechętnie dzielą się informacjami, które potencjalnie mogą zagrozić funkcjonowaniu ich przedsiębiorstwa. Z drugiej natomiast, świadomość ujawnienia potencjalnego niedopełnienia obowiązku służbowego (korzystanie z powierzonych systemów w nieodpowiedni sposób), a przez to obawa przed narażeniem się na odpowiedzialność karną czy finansową, może prowadzić do ukrywania prawdziwych zachowań. Stąd, przygotowanie kwestionariusza do badań ilościowych, które pozwolą na skwantyfikowanie modelu, ma kluczowe znaczenie dla rzetelności otrzymanych wyników.

Praca zawiera udokumentowany ciąg myślowy, prowadzący do utworzenia kwestionariusza, wraz z zaproponowanym sposobem interpretacji wyników. Badanie jest bardzo rozległe, więc zaproponowano taką konstrukcję narzędzia, by zwiększyć szansę na uzyskanie maksymalnie prawdziwych i kompletnych wyników. Kwestionariusz został więc rozszerzony o kwestie służące lepszemu zrozumieniu obecnej organizacji dostępu do zasobów firmowych, co okazało się istotnym czynnikiem w badaniach wstępnych. Przyczyną tego zabiegu było spełnienie celu utylitarnego, którym było opracowanie narzędzia, umożliwiającego przygotowanie rekomendacji dla kadry menedżerskiej.

Zaproponowany model i kwestionariusz (załącznik 1) stanowią zestaw gotowy do wdrożenia w procesie badawczym, mającym na celu skwantyfikowanie modelu i wypracowanie rekomendacji dotyczących bezpiecznego stosowania tożsamości cyfrowych.

Bibliografia

Wydawnictwa zwarte

1. Ajzen, I., and M. Fishbein (1980). *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs; NJ: Prentice Hall, 278 s.
2. Aronson, E., Akert, R.M., Wilson, D.T. (2012). *Psychologia społeczna. Serce i umysł*. Zysk i S-ka, 544 s.
3. Bertino, E., Takahashi, K. (2011). *Identity Management, Concepts, Technologies, and Systems*. London: Artech House, 198 s.
4. Branicki, W. (2009). *Tożsamość a wirtualność*. Kraków: Nomos, 246 s.
5. Byczkowski M. (2010) *Zarządzanie bezpieczeństwem informacji i systemów*, W: Zawiła-Niedźwiecki, J., Rostek, K., Gąsiorkiewicz, A. red. Informatyka gospodarcza T.4 Warszawa: C.H.Beck, s. 369–409, 673 s.
6. Chmielarz, W., Szumski, O. (2016). *Technologie mobilne geograficznych systemów informatycznych (GIS) w turystyce*. W: Chmielarz, W. red. Mobilne aspekty technologii informacyjnych, Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, s. 65–80, 235 s.
7. Davis, F.D. (1986). *Technology Acceptance Model for Empirically Testing New End-user Information Systems Theory and Results*. Unpublished Doctoral Dissertation, MIT, 292 s.
8. *Encyklopedia socjologii* (2002). Warszawa: Oficyna Naukowa, 376 s.
9. Hewlett Packard (2005). *The HP Security Handbook. Protecting Your Business*. 176 s.
10. Juszczyk, M. (2011). *Akceptacja tożsamości cyfrowej w przedsiębiorstwach Lubelszczyzny*. W: Nauka-Biznes: zbiór raportów badawczych opracowanych przez pracowników naukowych i naukowo-dydaktycznych – przedstawicieli lubelskiego środowiska naukowego, Chełm: Chełmskie Stowarzyszenie Rozwoju Społeczno-Gospodarczego CIVIS, s. 337–363, 786 s.
11. Kamiński, W. (1996). *Człowiek dorosły w sytuacjach zagrożenia tożsamości*. W: Wujek, T., red. Wprowadzenie do andragogiki. Warszawa: Instytut Technologii Eksploatacji, 437 s.
12. Kisielnicki, J., Soroka, H. (2005). *Systemy informatyczne biznesu – informatyka dla zarządzania*. Warszawa: Placet, 389 s.
13. Kostera, M., Kownacki, S., Szumski, A. (2009). *Zachowania organizacyjne: motywacja, przywództwo, kultura organizacyjna.* W: Koźmiński, A.K. red., Zarządzanie, teoria i praktyka. s. 316–317, 789 s.

14. Lange, R., Osiecki, J. (2014). *Nastolatki wobec Internetu*. Pedagogium Wyższej Szkoły Nauk Społecznych. Warszawa: NASK, 40 s.
15. Mądrzycki, T. (1977). *Psychologiczne prawidłowości kształtowania się postaw*, Warszawa: PWN, 228 s.
16. Mitnick, K.D., Simon, W. (2003). *Sztuka podstępu. Łamałem ludzi, nie hasła*. Wyd. I. Gliwice: Wydawnictwo Helion, 400 s.
17. OECD (2002). *Small and Medium Enterprise Outlook 2002, Enterprise, Industry and Services*, 252 s.
18. Palfrey, J., Gasser, U. (2007). *Case Study. Digital Identity, Interoperability and eInnovation*. Berkman Publication Series. 50 s.
19. Pastuszak Z. (2007). *Implementacja zaawansowanych rozwiązań biznesu elektronicznego w przedsiębiorstwie*, Warszawa: Placet, 376 s.
20. Piecuch, T. (2010). *Funkcjonowanie małych i średnich przedsiębiorstw w gospodarce*. W: Matejun, M., red. Wyzwania i perspektywy zarządzania w małych i średnich przedsiębiorstwach. Warszawa: C.H. Beck, 353 s.
21. Sitarski, P. (2002). *Rozmowa z cyfrowym cieniem*. Kraków: Rabid, 186 s.
22. Szpringer, W. (2008). *Wpływ wirtualizacji przedsiębiorstw na modele e-biznesu. Ujęcie instytucjonalne*. Warszawa: Oficyna Wydawnicza SGH, 275 s.
23. Warchał, M. (2009). *Językowe (re)konstrukcje tożsamości (psycho- i etnolingwistyczna analiza chorwackich wypowiedzi narracyjnych)*. Praca doktorska. Uniwersytet Śląski w Katowicach. Wydział Filologiczny. Katowice, 193 s.
24. Windley, Ph. J. (2005). *Digital Identity*. Sebastopol: O'Reily, 254 s.
25. Wołowski, F., Zawiła-Niedźwiecki, J. (2012). *Bezpieczeństwo systemów informacyjnych: praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*. Kraków; Warszawa: edu-Libri, 395 s.
26. Zarańska, K. (2016). *Determinanty korzystania z mobilnego handlu elektronicznego*. W: Chmielarz, W. red., Mobilne aspekty technologii informacyjnych, Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, 235 s.

Czasopisma, serie wydawnicze i materiały konferencyjne

1. Ajzen, J.: (1991). *The theory of planned behaviour*. Organisational Behaviour and Human Decision Processes, Vol. 50, s. 179–211.
2. Amoore, L. (2005). *Biometric borders: Governing mobilities in the war on terror*. Political Geography 25(3), s. 336–351.
3. Beck, E.N., (2015). *The Invisible Digital Identity: Assemblages in Digital Networks*. Computers and Composition, Volume 35, March 2015, s. 125–140.
4. Chmielarz W. (2008). *Stadium rozwoju systemów e-Administracji w Polsce*. W: Gołuchowski, J., Frączkiewicz-Wronka, A. red. Technologie wiedzy w zarządzaniu publicznym, Katowice: Wydawnictwo Akademii Ekonomicznej w Katowicach, s. 115–127.
5. Chmielarz, W. (2015). *Determinanty rozwoju serwisów dystrybucji treści komercyjnych w Polsce*. Problemy Zarządzania, Vol. 13, Nr 2 (52), T. 1, s. 51–65.
6. Chodacka, B., Miłosz, M. (2008). *E-obywatel – przezwyciężanie barier*. W: E-mentor nr 2 (24). Warszawa: Szkoła Główna Handlowa. s. 27–31.
7. Chun, H.H., Chyan, Y. (2011). *The intellectual development of the technology acceptance model: A co-citation analysis*. International Journal of Information Management, Vol. 31, Issue 2, s. 128–136.
8. Czerwińska-Lubszczyk, A., Michna, A., Męczyńska, A. (2013). *Determinanty rozwoju małych i średnich przedsiębiorstw sektora budowlanego*. Zarządzanie i Finanse, Tom 4 Nr 2, s. 79–91.
9. Dass, S.C. (2013). *Fingerprint-Based Recognition*. International Statistical Review, Vol. 81, Issue 2, s. 175–187.
10. Davis, F.D. (1989). *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*. MIS Quarterly 13(3), s. 319–340.
11. Davis, F.D., Bagozzi, R.P., Warshaw, P.R. (1989). *User Acceptance of Computer Technology: A Comparison of Two Theoretical Models.* Management Science 35(8), s. 982–1003.
12. Dolot A. (2020). Wpływ pandemii COVID-19 na pracę zdalną – perspektywa pracownika. E-mentor nr 1 (83) / 2020, s. 35–43.
13. Dziedzic, K. (2013). *E-administracja w Polsce na tle państw w Unii Europejskiej*. W: Laskowski, P. red. Prace Naukowe Wałbrzyskiej Szkoły Zarządzania i Przedsiębiorczości, T. 24, Samorząd terytorialny a polityka lokalna, s. 7–16.
14. Ghobakloo M., Zulkifi, N.B., Aziza, F.A (2010). *The Interactive Model of User Information Technology Acceptance and Satisfaction in Small and Medium-sized Enterprises*. European Journal of Economics, Finance And Administrative Sciences Issue 19, s. 7–27.

15. Grodzka, D. (2009). *E-administracja w Polsce*. W: Grodzka, D. red. Społeczeństwo informacyjne. Studia BAS, 2009, Nr 3 (19), s. 57–82.
16. Gulati, H., Huang, C.-T. (2019). *Self-Sovereign Dynamic Digital Identities based on Blockchain Technology*. SoutheastCon, 2019, 1–6.
17. Guo, K.H. i inni (2011). *Understanding nonmalicious security violations in the workplace: a composite behavior model*. Journal of Management Information Systems, 28 (2), s. 203–236.
18. Gupta, S., Kim, H.-W. (2004). *Virtual Community: Concepts, Implications, and Future Research Directions.* Proceedings of the Tenth Americas Conference on Information Systems, New York, August 2004, s. 2679–2687.
19. Ifinedo, P. (2012). *Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory.* Computers & Security 31 (2012), s. 83–95.
20. Juszczyk, M. (2011). Stosowalność modelu TAM w różnych obszarach absorbcji nowych technologii IC., W: Miłosz, M. red. Techniki Informatyczne w praktyce. Lublin: Polskie Towarzystwo Informatyczne, s. 205.Juszczyk, M., Miłosz, M., Miłosz, E. (2015). *Various methods for employees' authentication at SMEs*. Actual Problems of Economics – 2015, Nr 2, Vol. 164, s. 474–481.
21. Kapczyński, A. (2005). *Problematyka baz danych w biometrycznych systemach uwierzytelniania*. W: Kozielski, S. i inni red. Bazy Danych: Modele, Technologie, Narzędzia, Warszawa: Wydawnictwa Komunikacji i Łączności, s. 355–359.
22. Khan, A., Woosley, J.M. (2011). *Comparison of Contemporary Technology Acceptance Models and Evaluation of the Best Fit for Health Industry Organizations.* IJCSET, December 2011, Vol. 1, Issue 11, s. 709–717.
23. Kisielnicki, J. (2015) *Technologia informacyjna jako narzędzie wspomagania systemu zarządzania – analiza trendów*. Problemy Zarządzania, Vol. 13, Nr 2 (52), T. 1, s. 13–23.
24. Knight, A., Saxby, S. (2014). *Identity crisis: Global challenges of identity protection in a networked world.* Computer Law & Security Review, Volume 30, Issue 6, s. 617–632.
25. Koziczak, A. (2010). *Społeczna akceptacja identyfikacji biometrycznej. Rozwój i perspektywy biometrii na świecie*. Techniki komputerowe biuletyn informacyjny XLV, Nr 1. Warszawa: Wyd. Instytut Maszyn Matematycznych, s. 41–46.
26. Król, K. (2015) *Organizacyjne aspekty zarządzania bezpieczeństwem danych z perspektywy zagrożeń phishingu*. Organizacja i Zarządzanie, Wyd. Kwartalnik naukowy 2 (30), Politechniki Śląskiej, s. 19–32.

27. Lee, Y., Kozar, K.A., Larsen, R.T. (2003). *The Technology Acceptance Model: past, present and future*. Communications of the Association for Information Systems, Vol. 12, Article 50, s. 752–780.
28. Leimeister, J.M., Balaji, R. (2014). *Virtual Communities: 2014*, Vol. 20. Advances in Management Information Systems. Armonk: M.E. Sharpe, 192 s.
29. Liang, H., Xue, Y. (2009). *Avoidance of Information Technology Threats: a Theoretical Perspective*. MIS Quarterly, Vol. 33 No. 1, s. 71–90.
30. Liang, H., Xue, Y. (2010). *Understanding Security Behaviors in Personal. Computer Usage: A Threat Avoidance Perspective*. Journal of the Association for Information Systems, Vol. 11, Issue 7, s. 394–413.
31. Liu, J., Hodges, A., Clay, L., Monarch, J. (2020). *An analysis of digital identity management systems - a two-mapping view*. 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), s. 92–96.
32. Lockwood, P., Jordan, e.H., Kunda, Z. (2002). *Motivation by positive or negative role models: Regulatory focus determinants who will best inspire us*. Journal of Personality and Social Psychology, 83 (4), s. 854–864.
33. Marcinkowski, B., Wrycza, S. (2015). *CASE Tools' Acceptance in Higher Education – Assessment and Enhanced UTAUT Model*. Proceedings of the Conference on Information Systems Applied Research, Wilmington, North Carolina USA, Vol. 8, No 3671, 9 s.
34. Michna, A. (2008). *Specyfika przeprowadzania badań kwestionariuszowych w sektorze małych i średnich przedsiębiorstw*. Organizacja i Zarządzanie, Kwartalnik Naukowy Nr 3, Gliwice: Wydawnictwo Politechniki Śląskiej, s. 83–96.
35. Michna, A., Męczyńska, A., Kmieciak, R. (2011). *Małe i średnie przedsiębiorstwa wobec wyzwań współczesnej gospodarki*. W: Knosala, R., red. Komputerowo zintegrowane zarządzanie. T. 2. Opole: Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją, s. 108–116.
36. Michna, A., Męczyńska, A., Kmieciak, R. (2011). *Niewykorzystywane źródła przewagi konkurencyjnej MSP*. Zarządzanie i Edukacja nr 78/ 2011, s. 45–59.
37. Mikołajczyk, B., Krawczyk, M. (2006). *Sektor przedsiębiorstw mikro, małych i średnich w krajach Unii Europejskiej*, Studia Europejskie / Centrum Europejskie Uniwersytetu Warszawskiego, 2006, Nr 2, Cracow University of Economics, s. 67–85.
38. Milanowicz, M. (2012). *Elektroniczna wymiana danych (EDI) jako atrybut współczesnego społeczeństwa informacyjnego*. W: Społeczeństwo informacyjne – uwarunkowania rozwoju. Zeszyty naukowe nr 680. Problemy zarządzania, finansów i marketingu Nr 21. Szczecin. Uniwersytet Szczeciński. s. 37–47.

39. Mortenson, M.J., Vidgen, R. (2016). *A computational literature review of the technology acceptance model*. International Journal of Information Management Vol. 36, Issue 6, Part B, s. 1248–1259.
40. Mroczkowska, D. (2013). *Rola przywództwa w kształtowaniu motywacji*. Organizacja i Zarządzanie, Nr 2(22), Gliwice: Wydawnictwo Politechniki Śląskiej, s. 97–112.
41. Myyry, L. i inni (2009). *What levels of moral reasoning and values explain adherence to information security rules? An empirical study*. European Journal of Information Systems, Vol. 18, Issue 2, s. 126–139.
42. Nadybski, P. (2013). *Elektroniczna administracja w Polsce – ograniczenia i bariery*. Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy nr 9, s. 31–40.
43. Ocieczek W., Łakomy K., Nowacki K. (2016). *Proces doskonalenia pracowników poprzez szkolenia w aspekcie kształtowania kultury bezpieczeństwa pracy*. Organizacja i zarządzanie nr 4(36). Gliwice: Wydawnictwo Politechniki Śląskiej, s. 53–66.
44. Olszak, C., M.; Ziemba, E. (2011). *The stage of e-Government maturity in a Polish region – Silesia* Journal of Economics & Management, Vol. 7, s. 87–103.
45. Olszak, C., Ziemba, E. (2011). *Rozwój e-administracji. Rodzaje i poziomy dojrzałości e-usług publicznych w regionie śląskim*. W: Babis, H., Czapiewski, R. Drogi dochodzenia do społeczeństwa informacyjnego. Stan obecny, perspektywy rozwoju i ograniczenia. Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 651, Ekonomiczne Problemy Usług, Nr 68, T. 2, s. 250–266.
46. Olszak, C.M., Ziemba, E. (2012). *Critical Success Factors for Implementing Business Intelligence Systems in Small and Medium Enterprises on the Example of Upper Silesia,* Poland. Interdisciplinary Journal of Information, Knowledge & Management, Vol. 7, s. 129–150.
47. Olszak, C.M. (2012). *Organizacja oparta na Business Intelligence.* W: Ziemba, E., Olszak, C.M. red., Technologie informacyjne w transformacji współczesnej gospodarki. Katowice: Wydawnictwo Uniwersytetu Ekonomicznego W Katowicach, s. 9–29.
48. Opitek, P. (2015). *Przestępstwo skimmingu.* Prokuratura i prawo nr 11, s. 66–82.
49. Pahnila, S., Siponen, M., Mahmood, A.M. (2007). *Employees' Behavior towards IS Security Policy Compliance.* Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07) System Sciences, s. 156b–156b.
50. Pal, P. (2010). *Monetyzacja e-obecności*. Marketing w praktyce, Nr 4, s. 18–20.
51. Pei-Lee, T., Ahmed, P.K., D'Arcy, J. (2015). *What Drives Information Security Policy Violations among Banking Employees? Insights from*

Neutralization and Social Exchange Theory. Journal of Global Information Management, Vol. 23, Issue 1, s. 44–64.
52. Plucińska, M., Ryżko, J. (2010). *Rozwój i perspektywy biometrii na świecie*. Techniki komputerowe biuletyn informacyjny, XLV, Nr 1. Warszawa: Wyd. Instytut Maszyn Matematycznych, s. 9–21.
53. Plucińska, M., Wójtowicz, J. (2014*). Analiza technik biometrycznych do uwierzytelniania osób*. Elektronika 4/2014, s. 64–66.
54. Poznański, R., Szacki, K. (2011). *Bezpieczne uwierzytelnianie biometryczne na przykładzie rozwiązania AXSionics Internet Passport*. Techniki komputerowe biuletyn informacyjny XLV, Nr 1. Warszawa: Wyd. Instytut Maszyn Matematycznych, s. 160–162.
55. Ramesh K.M.H.M. (2013). *The Relationship between McGregor's X–Y Theory Management Style and Fulfillment of Psychological Contract: A Literature Review*. International Journal of Academic Research in Business and Social Sciences, No 5, s. 715–720.
56. Rosiński, J. (2012). *Postawy pracowników branży IT wobec zatrudniających organizacji jako wyzwanie dla rozwoju firm informatycznych*. Problemy Zarządzania, Vol. 10, Nr 3 (38), Uwarunkowania zastosowań systemów informatycznych w gospodarce, Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania UW, s. 229–247.
57. Ross, A., Jain, A. (2007). *Human recognition using biometrics: an overview*. Annals of Telecommunications Vol. 62, Issue 1/2, s. 11–35.
58. Sarzyński, K. (2016). *Bring your own device (BYOD) – szansa czy zagrożenie dla przedsiębiorstwa?* Organizacja i Zarządzanie, Nr 4(36). Gliwice: Wydawnictwo Politechniki Śląskiej, s. 67–80.
59. Shih, H.-P. i inni (2016). *Taking Promotion and Prevention Mechanisms Matter for Information Systems Security Policy in Chinese SMEs*. Proceedings of 2nd International Conference on Information Management (ICIM), 7–8 may 2016. London, s. 6.
60. Siponen, M., Mahmood, A.M, Pahnila, S. (2006). *Factors Influencing Protection Motivation and IS Security Policy Compliance.* Materiały konferencyjne: Innovations in Information Technology 2006, 19–21.12.2006, Dubaj, s. 1–5.
61. Siponen, M., Mahmood, A.M., Pahnila, S. (2010). *Compliance with Information Security Policies: An Empirical Investigation*. Computer, Vol. 43, Issue 11, s. 64–71.
62. Siponen, M., Mahmood, A.M, Pahnila, S. (2014). *Employees' adherence to information security policies: An exploratory field study*. Information & Management March 2014 51(2), s. 217–224.
63. Sobińska, M. (2014). *Innowacyjne modele biznesu dla IT -– wyzwania i perspektywy rozwoju.* W: Informatyka ekonomiczna. Business Informatics. 1(31)/2014. Wrocław: Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, s. 126–137.

64. Sullivan, C. (2012). *Digital identity and mistake*. International Journal of Law and Information Technology, Vol. 20, No. 3, s. 223–241.
65. Szczepanik, M., Jóźwik, I.J. (2014). *Metody wykrywania człowieczeństwa w systemach biometrycznych*. Organizacja i Zarządzanie z. 68, Nr kol. 1905, s. 403–411.
66. Szplit, M. (2012). *Ekonomiczne Aspekty Działania Systemów Informatycznych w Przedsiębiorstwach.* Gospodarka elektroniczna, wyzwania rozwojowe, tom II, Uniwersytet Szczeciński. Zeszyty Naukowe nr 703. Ekonomiczne Problemy Usług nr 88. Szczecin. s. 101–108.
67. Szyjewski, G. (2011). *Wykorzystanie modeli procesów biznesowych BPMN 2.0 do identyfikacji potrzeb zdalnego uwierzytelniania*. Metody Informatyki Stosowanej Nr 3/2011 (28), s. 167–178.
68. Szyjewski, G., Niemcewicz, P. (2016). *Zdalna realizacja usług w Internecie z uwzględnieniem profilu użytkownika*. Studia Informatica Pomerania, Nr 3 (41), s. 79–89.
69. Tadeusiewicz, R. (2010). *Zagrożenia w cyberprzestrzeni*. Nauka 4.2010. s. 31–42.
70. Vance, A. Sipponen, M., Pahnila, S. (2012). *Motivating IS security compliance: Insights from Habit and Protection Motivation Theory*. Information & Management 49 (3–4), s. 190–198.
71. Venkatesh, V., Davis, F.D. (2000). *A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies*. Management Science, 46, s. 186–204.
72. Wielki, J. (2012). *Analiza wyzwań związanych z zarządzaniem przestrzenią elektroniczną przez współczesne organizacje gospodarcze.* Problemy Zarządzania, Vol. 10, Nr 3 (38), Uwarunkowania zastosowań systemów informatycznych w gospodarce, Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania UW, s. 54–66.
73. Wielki, J. (2012). *Internet rzeczy i jego wpływ na modele biznesowe współczesnych organizacji gospodarczych*. Monografie i Opracowania Uniwersytetu Ekonomicznego we Wrocławiu, Nr 211, s. 208–219.
74. Wielki, J. (2016). *Analiza szans, możliwości i wyzwań związanych z wykorzystaniem Internetu Rzeczy przez współczesne organizacje gospodarcze*. Przedsiębiorczość i Zarządzanie, Tom XVII, Zeszyt 11, Część I, s. 127–140.
75. Wojciechowski, r., Cellary, W. (2010). *Evaluation of learners' attitude toward learning in ARIES augmented reality environments*. Computers & Education, Vol. 68, s. 570–585.
76. Wolniak, R. (2015). *Ocena funkcjonowania e-administracji w Dąbrowie Górniczej z punktu widzenia osób niepełnosprawnych.* W: Zeszyty naukowe Politechniki Śląskiej Nr kol. 1940, s. 369–383.

77. Wójtowicz, A., Cellary, W. (2010). *Representing User Privileges in Object-Oriented Virtual Reality Systems.* W: Camarinha-Matos, L.M., Pereira, P., Ribeiro, L. red. Emerging Trends in Technological Innovation. Proceedings of First IFIP WG 5.5/SOCOLNET Doctoral Conference on Computing, Electrical and Industrial Systems, DoCEIS 2010 Costa de Caparica, Portugal, February 22–24, 2010, s. 53–61.
78. Wróblewska, M. (2013). *Kształtowanie tożsamości w perspektywie rozwojowej i edukacyjnej*. *Pogranicze*, Studia Społeczne. Tom XVII, s. 176–187.
79. Wrycza, S., Kuciapski, M. (2014). *A model of faculty e-learning acceptance.* Conference proceedings,15th Annual Global Information Technology Management Association (GITMA) World Conference 2014. June 22–24, 2014, s. 2–12.
80. Wrycza, S., Marcinkowski, B., Gajda, D. (2017). *The enriched UTAUT model for the acceptance of software engineering tools in academic education*. Information Systems Management, Vol. 34, Issue 1, s. 38–49.
81. Ziemba, E., Obłąk, I. (2012). *Systemy informatyczne w organizacjach zorientowanych procesowo*. Problemy Zarządzania, Vol. 10, Nr 3 (38), s. 8–2.
82. Ziemba, E. (2012). *Transformacja zarządzania relacjami z klientami w kierunku zarządzania wiedzą klienta – kanony i technologie informatyczne*. W: Ziemba, E., Olszak, C.M. red, Technologie informacyjne w transformacji współczesnej gospodarki. Katowice: Wydawnictwo Uniwersytetu Ekonomicznego W Katowicach, s. 31–43.
83. Ziemba, E., Papaj, T., Będkowski, J. (2013). *Egzemplifikacja e-government w Polsce – analiza porównawcza SEKAP i ePUAP*. W: Roczniki Kolegium Analiz Ekonomicznych Nr 29/2013. Warszawa: Szkoła Główna Handlowa, s. 427–445.

Polskie normy i materiały źródłowe

1. PN-13335-1.
2. PN-I-02000.
3. PN-ISO/IEC 2382-1:1996.
4. PN-ISO/IEC 2382-8 2001.
5. PN-ISO/IEC 27001:2007.
6. PN-ISO/IEC 27002:2013.
7. PN-ISO/IEC 27005:2011.
8. PN-ISOIIEC 2382-8.
9. PNT-02000:

Akty prawne

1. Rozporządzenie Komisji (WE) nr 70/2001 (Dz. Urz. UE L 10 z 13.01.2001, s. 33).
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych.
3. Rozporządzenia m.in. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.
5. Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych
6. Rozporządzenie Ministra Administracji i Cyfryzacji z 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji przez administratora bezpieczeństwa.
7. Rozporządzenie Ministra Administracji i Cyfryzacji z 29 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji.
8. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.
9. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych.
10. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883.
11. Ustawa o swobodzie działalności gospodarczej z dnia 2 lipca 2004 roku.
12. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Dz.U. 2010 nr 182 poz. 1228.
13. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych.
14. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym.
15. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
16. Zalecenie Komisji Nr 96/280/WE z 3.04.1996 r. dotyczące definicji małych i średnich przedsiębiorstw (Dz.U. L 107 z 30.04.1996).

17. Zalecenie Komisji z 6.05.2003 r. dotyczące definicji mikroprzedsiębiorstwa oraz małych i średnich przedsiębiorstw (Dz.U. WE Nr L. 124 z 20.05.2003).

Źródła internetowe

1. *4 edycja badania stanu bezpieczeństwa informacji w Polsce. Ochrona biznesu w cyfrowej transformacji czyli 4 kroki do bezpieczniejszej firmy*. PWC. Online: https://www.pwc.pl/pl/pdf/ochrona-biznesu-w-cyfrowej-transformacji-pwc.pdf, dostęp: 2017.06.04.
2. *Adjusting the Lens on Economic Crime Preparation brings opportunity back into focus. Global Economic Crime Survey 2016*. (2016) PWC. Online: http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf, dostęp: 2017.06.04.
3. Beata Zdańczyk-Golędzinowska (2012). *Identyfikacja biometryczna w Banku BPH, informacja prasowa*, Warszawa. Online: http://www.bph.pl/repo/bph/PR/informacje_prasowe/2012/120919.pdf, dostęp: 2012.09.20.
4. Berezowska, J., Huet, M., Kamińska, M. (2015). *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2011–2015*. Warszawa: Główny Urząd Statystyczny. Online: http://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/1/9/1/spoleczenstwo_informacyjne_w_polsce_2011-2015.pdf, dostęp: 2017.06.04.
5. *Bezpieczeństwo tokenu RSA SecurID 800 złamane w kwadrans* (2012). Online: https://zaufanatrzeciastrona.pl/post/bezpieczenstwo-tokenu-rsa-securid-800-zlamane-w-kwadrans/, 2012.06.25.
6. Bień, A. (2016). *Branża e-commerce: zobacz, jaki budżet wydaje na posty sponsorowane na Facebooku.* Online: http://socialpress.pl/2016/05/branza-e-commerce-zobacz-jaki-budzet-wydaje-na-posty-sponsorowane-na-facebooku/, dostęp: 2017.06.04.
7. Bień, A. (2016). *Jak zmieniły się media społecznościowe na przestrzeni 5 lat?* Online: http://socialpress.pl/2016/03/jak-zmienily-sie-media-spolecznosciowe-na-przestrzeni-5-lat/, dostęp: 2017.06.04.
8. Bień, A. (2016). *Raport: Internet najmocniej wpływa na sprzedaż kosmetyków.* Online: http://socialpress.pl/2016/07/raport-internet-najmocniej-wplywa-na-to-ktore-kosmetyki-kupic-warto-a-ktore-nie/, dostęp: 2017.06.04.
9. Buchner, A., Zaniewska, K. (2016). *Katalog kompetencji cyfrowych małych firm.* Warszawa: Centrum Cyfrowe Projekt Polska, 37 s., s. 16. Online: https://centrumcyfrowe.pl/wp-content/uploads/2016/03/IR-katalog-kompetencji.pdf, dostęp: 2017.06.04.

10. Cameron, K. (2005). *The Laws of Identity.* Online: http://myinstantid.com/laws.pdf, dostęp: 2017.06.04.
11. *Dane bez ochrony. NIK: samorządowe systemy informatyczne i gromadzone dane podatne na ataki hakerów* (2019). Online: https://samorzad.pap.pl/kategoria/archiwum /dane-bez-ochrony-nik-samorzadowe-systemy-informatyczne-i-gromadzone-dane-podatne, 2019.05.10.
12. *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations* (2020). W3C Working Draft 24 November 2020. Online: W3C Working Draft 24 November 2020. Online: https://www.w3.org/TR/did-core/, dostęp: 2020.11.20.
13. Dederko, J. (2015). *Czy warto lokować produkty na YouTube? Mamy raport!* Online: http://socialpress.pl/2015/10/czy-warto-lokowac-produkty-na-youtube-mamy-raport/, dostęp: 2017.06.04.
14. Dederko, J. (2015). *Internet należy do Maffashion, Jemerced i Make Life Easier*. Online: http://socialpress.pl/2015/10/internet-nalezy-do-maffashion-jemerced-i-make-life-easier/, dostęp: 2017.06.04.
15. Dederko, J. (2015). *O tym, jak ogromny wpływ na decyzje konsumenckie mają youtuberzy*. Online: http://socialpress.pl/2015/11/o-tym-jak-ogromny-wplyw-na-decyzje-konsumenckie-maja-youtuberzy/, dostęp: 2017.06.04.
16. Dederko, J. (2015). *W jakim kierunku zmierza polski content marketing?* Online: http://socialpress.pl/2015/11/w-jakim-kierunku-zmierza-polski-content-marketing/, dostęp: 2017.06.04.
17. *Digital Economy and Society Index Report 2020 – Use of Internet Services* (2020). Online: https://ec.europa.eu/digital-single-market/en/use-internet-and-online-activities, dostęp: 2020.11.30.
18. *Digital identity management. Enabling Innovation and Trust in the Internet Economy* (2011). OECD. Online: http://www.oecd.org/sti/ieconomy/49338380.pdf, dostęp: 2017.06.04.
19. *Digital, mobile i social media w Polsce w styczniu 2020 roku.* Online: https://mobirank.pl/2020/02/23/digital-mobile-i-social-media-w-polsce-w-styczniu-2020-roku/, 2020.12.14.
20. *Dokumentacja zarządzania incydentami bezpieczeństwa* (2016). 4ITSecurity. Online:http://4itsecurity.pl/blog/1-Bezpiecze%C5%84stwo-informacji/72-dokumentacja-zarzadzania-incydentami-bezpieczenstwa.html, 2016.06.06.
21. *EIDAS supported Self-Sovereign Identity* (2019). Dokumenty Komisji Europejskiej. Online: https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf, 2020.11.30.
22. *Electronic Authentication Guideline. NIST Special Publication 800-63-1* (2011). NIST. Online: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-63-1.pdf, dostęp: 2017.06.04.

23. E*lektroniczna administracja*. Online: http://www.eadministracja.pl/elektroniczna-administracja, dostęp: 2017.06.04.
24. *Elektroniczna Platforma Usług Administracji Publicznej. Instrukcja zakładania konta. Wersja 7.1.* Ministerstwo Spraw Wewnętrznych i Administracji, 61 s. Online: http://bip.zielonagora.pl/system/obj/25161_Instrukcja_zakladania_konta_71.pdf, dostęp: 2017.06.04.
25. *ePUAP2*. Online: https://epuap.gov.pl/wps/portal, dostęp: 2017.06.04.
26. Ferrari, A. (2013), tłum. Urban, K. (2016). *DIGCO MP Ramy odniesienia dla rozwoju i rozumienia kompetencji cyfrowych w Europie*, 80 s. Online: http://www.digcomp.pl/download/raport-eccc-digcomp-pl/?wpdmdl=396, dostęp: 2017.06.04.
27. Filho, F.G., (2008). *The Evolving Role of the Identity: From the Lone User to the Internet 2*. The Architecture Journal, Journal 16. Microsoft. Online: http://msdn.microsoft.com/en-us/library/cc837112.aspx, dostęp: 2015.01.06.
28. Fliciak, M., Mazurek, P., Growiec, K. (2013), Korzystanie z mediów a podziały społeczne. *Kompetencje medialne Polaków w ujęciu relacyjnym*. Warszawa: Centrum Cyfrowe. 108 s. Online: http://ngoteka.pl/bitstream/handle/item/215/korzystanie%20z%20mediow%20a%20podzialy%20spoleczne.pdf?sequence=3, dostęp: 2017.06.04.
29. Gawrych, K. (2017). *A Ty jak dbasz o swoje hasła? Zadbaj o bezpieczeństwo w sieci!* Portal ODO. Online: https://portalodo.com/a-ty-jak-dbasz-o-swoje-hasla-zadbaj-o-bezpieczenstwo-w-sieci/, 2017.03.21.
30. GIODO *Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji*. Online: www.giodo.gov.pl/plik/id_p/550/, dostęp: 2017.06.04.
31. *Globalne cyberzagrożenia związane z pandemią* (2020). Online: https://www2.deloitte.com/pl/pl/pages/technology/articles/globalne-cyberzagrozenia-zwiazane-z-epidemia.html, dostęp: 30.11.2020.
32. Góra, J. (2013). *Raport. Efektywne zarządzanie bezpieczeństwem informacji*. Online: https://www.us.edu.pl/sites/all/files/www/wiadomosci/pliki/RAPORT2013.pdf, dostęp: 2017.06.04.
33. Górczyńska, A. *Wpływ Programu Operacyjnego Polska Cyfrowa (POPC) na rozwój innowacyjnej e-administracji w Polsce.* W: Nowak, P.A. red. INNOWACJE 2015. Rozwój społeczeństwa informacyjnego w nowej perspektywie finansowej. Łódź: Urząd Marszałkowski Województwa Łódzkiego, s. 6–20. Online: http://dspace.uni.lodz.pl:8080/xmlui/bitstream/handle/11089/16518/1_%206_pdf_INNOWACJE%202015.pdf?sequence=1&isAllowed=y, dostęp: 2017.06.14.

34. Grassi, P.A. *Draft NIST Special Publication 800-63B. Digital Identity Guidelines. Authentication and Lifecycle Management*. NIST. Online: https://pages.nist.gov/800-63-3/sp800-63b.html#sec4, dostęp: 2017.06.04.
35. Greenwood, D. *Context, Terms, Models and Options for Digital Identity Management.* OECD. 3 Online: http://www.oecd.org/sti/ieconomy /38584991.pdf, dostęp: 2017.06.04.
36. Gutierrez, A. J. (2006). *Towards better Digital Identity Management. Sensitive Information in a Wired World CPSC 457b*. Online: http://zoo.cs.yale.edu/classes/cs457/spr06/info_paper.pdf, dostęp: 2017.06.04.
37. *Handel danymi osobowymi* (2016). 4ITSecurity. Online: http://4itsecurity.pl/blog/2-Dane-osobowe/87-handel-danymi-osobowymi.html, 2016.08.25.
38. *IOCTA 2020. Internet organized crime. Threat assessment* (2020). Europol. Online: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020, dostęp: 15.12.2020.
39. *Jak po cichu zhackować dowolnego smartphona (oraz inne urządzenia komunikujące się po GSM)?* (2014). Niebezpiecznik. Online: https://niebezpiecznik.pl/post/jak-zhackowac-dowolnego-smartphona-oraz-inne-urzadzenia-komunikujace-sie-po-gsm/, 2014.08.13.
40. Jasiewicz, J. i in. (201). *Ramowy katalog kompetencji cyfrowych. Warszawa: Centrum Cyfrowe, 68 s. Online: http://cppc.gov.pl/wp-*content/uploads/zal.-13-Ramowy_katalog_kompetencji_cyfrowych.pdf, dostęp: 2017.06.04.
41. Johansson, J. M. (2009). *Security Watch: Thoughts on Identity, Part 1*. TechNet Magazine, June 2009. Online: https://technet.microsoft.com/en-us/magazine/2009.06.securitywatch, dostęp: 2017.06.04.
42. Kaczmarek, S. (2016). *Bezpieczna firma w cyberprzestrzeni*. Online: http://it-filolog.pl/bezpieczna-firma-w-cyberprzestrzeni, 2016.02.15.
43. Kaczmarek, A. *Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa*. GIODO. Online: www.giodo.gov.pl/plik /id_p/10212/j/pl/, dostęp: 2017.06.04.
44. *Korzystanie z Internetu, Komunikat z badań Nr 95/2019* (2019).CBOS. Online: https://www.cbos.pl/SPISKOM.POL/2019/K_095_19.PDF, dostęp: 14.12.2020.
45. Kosior, A. (2017) *RODO – niejasne wytyczne, kary rzędu nawet 20 mln euro. Kto zyska na nowej unijnej rezolucji?* Dziennik internautów. Biznes i prawo. Online: http://di.com.pl/rodo-niejasne-wytyczne-kary-rzedu-nawet-20-mln-euro-kto-zyska-na-nowej-unijnej-rezolucji-56984, 2017.03.24.

46. Lörincz, B., i inni. (2010). *Digitizing Public Services In Europe: Putting ambition into action*, 9th Benchmark Measurement, 272 s. Online: http://ec.europa.eu/newsroom/document.cfm?action=display&doc_id=747, dostęp: 2017.06.04.
47. Łapacz, D. (2015). *Udział małych i średnich przedsiębiorstw w wytwarzaniu PKB – Polska na tle Unii Europejskiej*. Electronic Scientific Journal, 6 Issue 1, s. 43–51.
48. Maj, M. (2016). *Polska wśród państw "pozostających w tyle" jeśli chodzi o cyfryzację społeczeństwa.* Dziennik internautów Biznes i Prawo. Online: http://di.com.pl/polska-wsrod-panstw-pozostajacych-w-tyle-jesli-chodzi-o-cyfryzacje-spoleczenstwa-54512, dostęp: 2017.06.04.
49. Majchrzyk, Ł. (2016). *Mobile i digital w Polsce i na świecie w 2016 r.* Online: https://mobirank.pl/2016/01/27/mobile-digital-w-polsce-na-swiecie-2016/, 2016.01.27.
50. Mielnicki, T. i inni red. (2013). *Identyfikacja i uwierzytelnienie w usługach elektronicznych.* Forum Technologii Bankowych przy Związku Banków Polskich. Warszawa. Online: https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf, dostęp: 2017.06.04.
51. Mullins, R. i inni (2007). *A Web Based Intelligent Training System for SMEs*. Electronic Journal of e-Learning, Vol. 5, No 1, s. 39–48. Online: www.ejel.org/issue/download.html?idArticle=29.
52. *Nastolatki 3.0* (2019). Red.: Bochenek, M., Lange, M. Raport NASK Państwowy Instytut Badawczy, Warszawa 2019.
53. *NIK o wdrażaniu systemów teleinformatycznych w miastach i gminach.* (2015). NIK. Online: https://www.nik.gov.pl/aktualnosci/nik-o-wdrazaniu-systemow-teleinformatycznych-w-miastach-i-gminach.html, 2015.03.23.
54. *Nowe przepisy o ochronie danych osobowych* (2017). 4ITSecurity. Online: http://4itsecurity.pl/blog/2-Dane-osobowe/90-nowe-przepisy-o-ochronie-danych-osobowych.html, 2017.01.07.
55. OECD (2011). *Digital identity management. Enabling Innovation and Trust in the Internet Economy*, 183 s. Online: http://www.oecd.org/sti/ieconomy/49338380.pdf.
56. Pacut, A. (2012). *Nie uciekniemy już od biometrii*. Online: http://centrumpr.pl/artykul/nie-uciekniemy-juz-od-biometrii,39105.html, dostęp: 2012.09.28.
57. Paliszkiewicz, J., Gołuchowski, J., Koohang, A. (2015). *Leadership, trust, and knowledge management in relation to organizational performance: Developing an instrument*. Online Journal of Applied Knowledge Management, Vol. 3 Issue 2, s. 19–35. Online:

http://www.iiakm.org/ojakm/articles/2015/volume3_2/OJAKM_Volume3_2pp19-35.pdf.
58. Pato, J. (2003). *Identity Management: Setting Context*. Encyclopedia of Information Security, (Summer/Fall). Online: http://www.hpl.hp.com /techreports/2003/HPL-2003-72.pdf?jumpid=reg_R1002_USEN, dostęp: 2017.06.01.
59. *Polityka bezpieczeństwa informacji*. Online: https://mikroporady.pl/ zarzadzanie/item/1610-polityka-bezpieczenstwa-informacji.html, dostęp: 2017.06.04.
60. Polska Agencja Rozwoju Przedsiębiorczości (2011). *Raport o Stanie Sektora Małych i Średnich Przedsiębiorstw w Polsce, Rozdział 8*, PARP: Warszawa, s. 8. Online: https://badania.parp.gov.pl/files/ 74/81/469/12555.pdf, dostęp: 03.05.2017.
61. *Raport Interaktywnie.com "Media społecznościowe 2016"*. (2016). s. 10. Online: http://interaktywnie.com/biznes/artykuly/raporty-interaktywnie-com/raport-interaktywnie-com-media-spolecznosciowe-2016-253577, dostęp: 2017.06.04.
62. Ratajczak, M. (2015) *E-administracja w Polsce kosztowała miliardy złotych. I wciąż jest gorsza niż w Rosji i Kazachstanie*. Money.pl. Online: http://news.money.pl/artykul/e-administracja-w-polsce-kosztowala-miliardy,48,0,1755184.html, 2015.04.08.
63. Rouse, M. (2010). *Definition of user account provisioning.* TechTarget Network. Online: http://searchsecurity.techtarget.com/definition/user-account-provisioning, dostęp: 2017.06.04.
64. Sapronov, K. *Czynnik ludzki a bezpieczeństwo informatyczne*. Securelist. Online: http://securelist.pl/threats/5480,czynnik_ludzki_a_ bezpiecze nstwo _informatyczne.html dostęp: 2017.06.04.
65. *Sektor MŚP będzie coraz bardziej atrakcyjnym i zyskownym łupem dla hakerów* (2016). Online: http://interaktywnie.com/biznes/newsy/ bezpieczenstwo/sektor-msp-bedzie-coraz-bardziej-atrakcyjnym-i-zyskownym-lupem-dla-hakerow-253102, dostęp: 2016.04.22.
66. *Słownik innowacji – leksykon haseł*. Online: http://www.pi.gov.pl, dostęp: 2017.06.04.
67. *Słownik Języka Polskiego*. Online: http://sjp.pwn.pl, dostęp: 2011.09.20.
68. Stanisławski, P. (2017). *Wreszcie nowe wytyczne w sprawie haseł! Koniec z ciągłymi zmianami i dziwnymi znakami*. Online: http://www.crazynauka.pl/wreszcie-nowe-wytyczne-w-sprawie-hasel-koniec-z-ciaglymi-zmianami-i-dziwnymi-znakami/, 2017.04.25.
69. Starkowski, M. T. *Palec zamiast karty* (2012). Online: http://www.biztok.pl/Palec-zamiast-karty-a5617, dostęp: 2012.10.04.
70. Stevens, T. i inni. (2010). *Stan rynku tożsamości elektronicznej. Technologie, infrastruktura, usługi i polityki.* Ipts, Komisja Europejska,

101 s. Online: http://spiner.org.pl/biblioteka-erozwoju.html?download=135%3Asytuacja-rynku-tozsamosci-elektronicznej, dostęp: 2017.06.04.
71. *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013* (2008). Ministerstwo Spraw Wewnętrznych i Administracji, 5 s. Online: http://www.umwd.dolnyslask.pl/fileadmin/user_upload/spoleczenstwo_informacyjne/dokumenty/Streszczenie.pdf, dostęp: 2017.06.04.
72. *The role of digital identity management in the internet economy: A primer for policy makers.* (2009). OECD. Online: http://www.oecd.org/internet/ieconomy/43195291.pdf, June 2009.
73. Tomala, L. (2010). *Prof. Pacut o tym, czy można oszukać urządzenia biometryczne*. PAP Nauka w Polsce. Online: http://naukawpolsce.pap.pl/aktualnosci/news,374692,prof-pacut-o-tym-czy-mozna-oszukac-urzadzenia-biometryczne.html, dostęp: 2017.06.04.
74. Wasilewska-Śpioch, A. (2015). *Czas na hasło głosowe? Eksperci są sceptyczni*. Dziennik internautów Bezpieczeństwo. Online: http://di.com.pl/czas-na-haslo-glosowe-eksperci-sa-sceptyczni-51365, 2015.01.24.
75. Wodo, W., Ławniczak, K. (2016). *Bezpieczeństwo i biometria urządzeń mobilnych w Polsce. Badanie użytkowników 2016.* Wrocław: Wydawnictwo Politechniki Wrocławskiej. Online: http://wwodo.mokop.co/uploads/docs/raport-bezpieczenstwo-urzadzenia-mobilne-polska-2016.pdf.
76. Zadura-Lichata, P. (2012). *Małe i średnie przedsiębiorstwa a dobre zarządzanie – Raport o stanie sektora MSP w Polsce*. Warszawa: PARP. Online: http://badania.parp.gov.pl, dostęp: 2017.06.04.
77. *Zalecenia przy tworzeniu silnego hasła* (2013). Kaspersky. Online: http://support.kaspersky.com/pl/viruses/general/3730, 2013.11.26.
78. *Zasady bezpieczeństwa i wymogi techniczne*. GET IN Bank. Online: https://www.getinbank.pl/dokument/Zasady-bezpieczenstwa-i-wymogi-techniczne--internetowe-kanaly-dostepu.pdf, dostęp: 2107.06.04.
79. Zegarek, P. (2010). *Podstawowe obowiązki administratora danych osobowych*. Online: http://blog-daneosobowe.pl/ochrona-danych-osobowych-podstawowe-obowiazki-administratora-danych-osobowych, 2010.03.18.

Załącznik 1. Ankieta badawcza

CZĘŚĆ 1. TOŻSAMOŚĆ CYFROWA PRACOWNIKÓW I NARZĘDZIA UWIERZYTELNIENIA

1. W jaki sposób uzyskuje Pan(i) dostęp do zasobów systemów informatycznych w pracy? (wybór wielokrotny)
   - ☐ Mam przydzielony indywidualny dostęp (np. z indywidualnym loginem i hasłem)
   - ☐ Dzielę moje konto pracownicze z innymi współpracownikami (np. mamy jeden login i hasło)
   - ☐ Mam otwarty dostęp do zasobów (np. nie korzystamy z haseł i loginów)

2. Z ilu narzędzi uwierzytelnienia korzysta Pan(i) w pracy?

Login i hasło / PIN		szt.
Karta elektroniczna		szt.
Karta elektroniczna + PIN		szt.
Nośnik kryptograficzny USB		szt.
Token generujący hasła jednorazowe		szt.
Token generujący hasła jednorazowe + PIN		szt.
Token – aplikacja na komórkę		szt.
Karta kodów jednorazowych		szt.
Czytnik linii papilarnych		szt.
Wzór rysowany palcem po ekranie (symbol odblokowania)		szt.
Inne, jakie?.....……		szt.
Inne, jakie?…….……		szt.

3. Ile razy w ciągu przeciętnego dnia pracy musi Pan(i) korzystać z uwierzytelnienia, czyli potwierdzać uprawnienia dostępu np. przez wpisanie hasła (proszę wpisać liczbę tylko przy tych narzędziach, z których Pan(i) korzysta)?

Login i hasło / PIN		dziennie
Karta elektroniczna		dziennie
Karta elektroniczna + PIN		dziennie
Nośnik kryptograficzny USB		dziennie
Token generujący hasła jednorazowe		dziennie
Token generujący hasła jednorazowe + PIN		dziennie
Token – aplikacja na komórkę		dziennie
Karta kodów jednorazowych		dziennie
Czytnik linii papilarnych		dziennie
Wzór rysowany palcem po ekranie (symbol odblokowania)		dziennie
Inne, jakie?.....……		dziennie

Inne, jakie?……		dziennie

4. Proszę uzupełnić zdania dotyczące haseł wykorzystywanych w pracy poprzez wpisanie liczby bądź podkreślenie właściwych odpowiedzi (tekst pisany pogrubioną czcionką).

UWAGA! Jeśli nie korzysta Pan(i) z haseł w pracy – proszę pominąć kolejne pytania pt. 4.

- Moje hasła mają średnio **…….** znaków i są to: **małe litery / duże litery / cyfry / znaki specjalne.**
- Moje hasła **zawierają / nie zawierają** ważnych dla mnie dat lub imion, prostych ciągów znaków (np. 12345, qwerty).
- Przechowuję hasła**: tylko w pamięci / w pliku tekstowym / w wygodnym miejscu (np. pod klawiaturą komputera) / zapisane w formie zaszyfrowanej / w notatniku, który staram się mieć zawsze przy sobie / zapisane i zdeponowane w sejfie / inaczej, jak?**

  .....

  .....
- Osoby, które znają niektóre moje hasła to: **zaufani współpracownicy / przełożony / członek rodziny / osoby ze wsparcia technicznego / nie ma takich osób.**
- Zmieniam hasła średnio raz na **…… dni / miesięcy / lat / nie zmieniam haseł wcale**.
- Generalnie zmieniam hasła **zgodnie z zaleceniami / w sposób inny niż zalecany / nie mam żadnych zaleceń**.
- **Używam / nie używam** tego samego hasła do różnych aplikacji.
- Decyzja o użyciu hasła w celu zabezpieczenia dostępu do zasobów **była w mojej gestii / podjął ją mój przełożony / jest regulowana wewnętrznymi przepisami.**
- **Zdarzyło / nie zdarzyło** mi się zapomnieć hasła.
- **Zdarzyło mi się / nie zdarzyło mi się** ujawnić hasła osobie postronnej.
- **Zdarzyła / nie zdarzyła** mi się sytuacja, że ktoś wykorzystał moje hasło by uzyskać dostęp do danych, do których nie powinien mieć dostępu.
- Podczas logowania wpisywane przeze mnie znaki **są / nie są** widoczne.
- Opuszczając swoje miejsce pracy na dłuższą chwilę **wylogowuję / nie wylogowuję się / wylogowuję się automatycznie.**
- W sytuacji obawy, że hasło, którym się posługuję zostało podejrzane przez osobę postronną, zostały podjęte przeze mnie działania: **mój przełożony został powiadomiony / moje hasło zostało zmienione / nie było żadnych działań z mojej strony / nie było takiej sytuacji / inne, jakie?**

  .....

  .....

  .....

5. Proszę uzupełnić zdania dotyczące urządzeń uwierzytelniających (tokenów, USB, kart lub aplikacji) lub kart kodów jednorazowych wykorzystywanych w zakładzie pracy poprzez uzupełnienie wykropkowania bądź podkreślenie właściwych odpowiedzi (tekst pogrubioną czcionką).

UWAGA! Jeśli nie używa Pan(i) przedmiotów uwierzytelniających – proszę pominąć kolejne pytania pt. 5.

- Osoby, które kiedykolwiek skorzystały z mojego przedmiotu uwierzytelniającego to: **zaufani współpracownicy / przełożony / członek rodziny / osoby ze wsparcia**

technicznego / nie ma takich osób / ktoś inny, kto?

.....

- Zasady związane z przechowaniem przedmiotu uwierzytelniającego są przeze mnie: **przestrzegane / częściowo przestrzegane / nieprzestrzegane / nie pamiętam zaleceń / nie było takich zaleceń.**
- **Zdarzyło / nie zdarzyło** mi się zgubić przedmiot uwierzytelniający.
- **Zdarzyła / nie zdarzyła** mi się sytuacja, że ktoś wykorzystał mój przedmiot uwierzytelniający by uzyskać dostęp do danych, do których nie powinien mieć dostępu.
- W sytuacji obawy, że przedmiot uwierzytelniający, którym się posługuję został przejęty przez osobę postronną, zostały przeze mnie podjęte: **mój przełożony został powiadomiony / nie było żadnych działań z mojej strony / nie było takiej sytuacji / inne, jakie?**

.....

CZĘŚĆ 2. POSTAWA PRACOWNIKÓW WOBEC TOŻSAMOŚCI CYFROWEJ

6. Proszę wskazać jak ocenia Pan(i) korzystanie z poniższych sposobów uwierzytelnienia.

	Zupełnie łatwe	Generalnie łatwe	Nieco trudne	Stanowi trudność	Stanowi poważną trudność	Nie mam doświadczeń
Login i hasła lub PIN	☐	☐	☐	☐	☐	☐
Urządzenie uwierzytelniające	☐	☐	☐	☐	☐	☐
Karta kodów jednorazowych	☐	☐	☐	☐	☐	☐
Odcisk palca	☐	☐	☐	☐	☐	☐
Wzór rysowany na ekranie	☐	☐	☐	☐	☐	☐
Inne, jakie? …… ……..……	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐	☐ ☐

7. Załóżmy, że każde hasło, którego używa Pan(i) w pracy spełniałoby następujące kryteria bezpieczeństwa:
   - długość min. 14 znaków,
   - w składzie co najmniej 1: wielka i mała litera, cyfra, znak specjalny,
   - nie mogłoby zawierać dat ani imion ważnych dla Pana(i),
   - wszystkie hasła do kluczowych aplikacji byłyby różne,
   - byłoby zmieniane minimum co miesiąc,
   - nie mogłoby być przechowywane w postaci niezaszyfrowanej lub w miejscu, gdzie jest łatwo dostępne,
   - nie byłoby znane nikomu w Pana(i) miejscu pracy ani poza nim.

Gdyby tak określone *bezpieczne* hasła były główną metodą Pana(i) uwierzytelnienia, jak ocenił(a)by je Pan(i)

w obszarze uciążliwości:

☐ Zupełnie nieuciążliwe

- ☐ Generalnie nieuciążliwe
- ☐ Nieco uciążliwe
- ☐ Stanowiące pewną uciążliwość
- ☐ Stanowiące poważną uciążliwość
- ☐ Nie mam doświadczeń z hasłami

w obszarze wpływu na efektywność pracy:

- ☐ Bez wpływu na efektywność mojej pracy
- ☐ Wpływające w niewielkim stopniu na efektywność pracy
- ☐ Wpływające w pewnym stopniu na efektywność pracy
- ☐ Wywierające znaczny, wymierny wpływ na efektywność pracy
- ☐ Poważnie zmniejszające efektywność pracy
- ☐ Nie mam doświadczeń z hasłami

8. Załóżmy, że bezpieczne korzystanie z urządzenia służącego uwierzytelnieniu lub karty kodów jednorazowych oznaczałoby spełnienie następujących warunków:
   - urządzenie / karta byłaby pieczołowicie przechowywana (np. stale noszona przy sobie, ew. złożona w sejfie lub bardzo bezpiecznym miejscu) i nieprzekazywana nikomu innemu,
   - ewentualne dodatkowe zabezpieczenie (PIN) nie byłoby nigdzie zapisane, ani nikomu przekazywane.

Gdyby tak określone *bezpieczne* przedmioty uwierzytelniające były główną metodą uwierzytelnienia stosowaną w Pana(i) miejscu pracy, stosowanie tej metody ocenił(a)by Pan(i) jako…

w obszarze uciążliwości:

- ☐ Zupełnie nieuciążliwe
- ☐ Generalnie nieuciążliwe
- ☐ Nieco uciążliwe
- ☐ Stanowiące pewną uciążliwość
- ☐ Stanowiące poważną uciążliwość
- ☐ Nie mam doświadczeń z urządzeniami uwierzytelniającymi ani kartami kodów jednorazowych

w obszarze wpływu na efektywność pracy:

- ☐ Bez wpływu na efektywność mojej pracy
- ☐ Wpływające w niewielkim stopniu na efektywność pracy
- ☐ Wpływające w pewnym stopniu na efektywność pracy
- ☐ Wywierające znaczny, wymierny wpływ na efektywność pracy
- ☐ Poważnie zmniejszające efektywność pracy
- ☐ Nie mam doświadczeń z przedmiotami uwierzytelniającymi ani kartami kodów jednorazowych

9. Wadami uwierzytelnienia z użyciem cech fizycznych lub behawioralnych (np. badanie odcisku palca, geometrii twarzy czy dłoni, układu naczyń krwionośnych, głosu) są m.in. problemy z właściwym odczytem danych np.:
   - Wrażliwość na tymczasowe zmiany cech fizycznych / behawioralnych tj. otarcia naskórka / skaleczenia (odcisk palca), chrypka / przeziębienie (głos), spuchnięcie twarzy (geometria twarzy)
   - Wrażliwość na zmiany warunków odczytu np. oświetlenia (geometria twarzy)

Mając to na uwadze proszę ocenić, czy gdyby metody oparte o cechy fizyczne lub behawioralne (zwane metodami biometrycznymi) były główną metodą uwierzytelnienia w Pana(i) miejscu pracy, stosowanie tej metody uwierzytelnienia ocenia Pan(i) jako…

w obszarze uciążliwości:
- ☐ Zupełnie nieuciążliwe
- ☐ Generalnie nieuciążliwe
- ☐ Nieco uciążliwe
- ☐ Stanowiące pewną uciążliwość
- ☐ Stanowiące poważną uciążliwość
- ☐ Nie mam doświadczeń z uwierzytelnianiem opartym o biometrię

w obszarze wpływu na efektywność pracy:
- ☐ Bez wpływu na efektywność mojej pracy
- ☐ Wpływające w niewielkim stopniu na efektywność pracy
- ☐ Wpływające w pewnym stopniu na efektywność pracy
- ☐ Wywierające znaczny, wymierny wpływ na efektywność pracy
- ☐ Poważnie zmniejszające efektywność pracy
- ☐ Nie mam doświadczeń z uwierzytelnianiem opartym o biometrię

10. Jakie znaczenie mają dla Pana(i) poniższe ryzyka?

	Nieistotne	Marginalne znaczenie	Nieco niepokojące	Niepokojące	Bardzo niepokojące
Zbieranie wzorców biometrycznych przez zakład pracy np. odcisków palców	☐	☐	☐	☐	☐
Zagrożenie osobiste przy próbie dotarcia do zasobów chronionych Pana(i) cechami biometrycznymi (np. rozbój)	☐	☐	☐	☐	☐
Zagrożenie osobiste przy próbie dotarcia do zasobów chronionych przedmiotem lub hasłem (np. rozbój)	☐	☐	☐	☐	☐
Ryzyko zgubienia przedmiotu	☐	☐	☐	☐	☐
Ryzyko utraty / zapomnienia hasła	☐	☐	☐	☐	☐

11. Czy w Pana(i) zakładzie pracy wdrożona jest polityka bezpieczeństwa?
    - ☐ Tak
    - ☐ Nie
    - ☐ Jest w trakcie przygotowania
    - ☐ Nie wiem
12. Proszę ocenić na ile ważne są dla Pana(i) korzyści z bezpiecznego korzystania z dostępu do zasobów informatycznych Pana(i) zakładu pracy:

	Jest nieistotne	Ma marginalne znaczenie	Ma pewne znaczenie	Ma istotne znaczenie	Jest bardzo ważne
Bezpieczeństwo danych	☐	☐	☐	☐	☐
Redukcja ryzyka odpowiedzialności np. karnej	☐	☐	☐	☐	☐
Świadomość dopełnienia obowiązków (zgodność z wytycznymi)	☐	☐	☐	☐	☐

Uniknięcie problemów w pracy (np. podszycie się obcej osoby)	□	□	□	□	□
Bezpieczna komunikacja drogą elektroniczną	□	□	□	□	□

13. Mając na uwadze korzyści i obciążenia, jakie niesie ze sobą bezpieczne korzystanie z różnych metod uwierzytelnienia, jak ocenia Pan(i) ich przydatność w skali od -2 (nieużyteczne) do 2 (bardzo użyteczne)?

	-2	-1	0	1	2
Login i hasło lub PIN	□	□	□	□	□
Przedmiot uwierzytelniający	□	□	□	□	□
Biometria	□	□	□	□	□

14. Jaki ma Pan(i) stosunek do różnych metod uwierzytelniania?

	Entuzjastyczny	Pozytywny	Neutralny	Negatywny
Login i hasło lub PIN	□	□	□	□
Przedmiot uwierzytelniający	□	□	□	□
Biometria	□	□	□	□

15. Czy chce Pan(i) używać metod uwierzytelniania w sposób bezpieczny?

	Tak	Nie	Nie wiem
Login i hasło lub PIN	□	□	□
Przedmiot uwierzytelniający	□	□	□
Biometria	□	□	□

16. Proszę wskazać, które twierdzenia są prawdziwe w Pana(i) jednostce organizacyjnej w zakładzie pracy (wybór wielokrotny).
    - ☐ Mamy zapewnione wsparcie techniczne i merytoryczne, wiemy, do kogo się zwrócić w razie problemów
    - ☐ Przeszkolono nas z bezpieczeństwa uwierzytelniania się
    - ☐ Przechodzimy cykliczne szkolenia, na których poruszana jest kwestia bezpieczeństwa danych
    - ☐ Mieliśmy wpływ na ustalenie zasad i wybór narzędzi uwierzytelniania
    - ☐ Zasady dotyczące korzystania z kont pracowniczych i narzędzi uwierzytelniania są wyznaczone i jasno komunikowanie
    - ☐ Bezpieczeństwo uwierzytelnienia ma realny wpływ na ocenę naszej pracy
    - ☐ Działania związane z uwierzytelnieniem są kontrolowane na bieżąco, występuje reakcja przełożonych na nieprzestrzeganie zasad
    - ☐ Można powiedzieć, że bezpieczeństwo danych ma bezpośrednie przełożenie na nasze zarobki
    - ☐ Żadne z powyższych
17. Czy prawdopodobne są ataki cyberprzestępców na zasoby komputerowe chronione procesem uwierzytelnienia w zakładzie pracy takim jak Pana(i)?
    - ☐ Tak
    - ☐ Nie
18. Jakie jest ryzyko powodzenia takiego ataku na systemy informatyczne Pana(i) zakładu pracy?
    - ☐ Małe

- ☐ Średnie
- ☐ Duże

CZĘŚĆ 3. ZARZĄDZANIE POSTAWĄ PRACOWNIKÓW WOBEC TOŻSAMOŚCI CYFROWEJ

19. Co powoduje, że stosuje Pan(i) uwierzytelnienie dostępu do zasobów? (wybór wielokrotny)
    - ☐ Konieczność – brak uwierzytelnienia oznacza brak dostępu do danych i niemożność wykonania obowiązków
    - ☐ Świadomość zalet dla zakładu pracy
    - ☐ Świadomość zalet dla Pana(i)
    - ☐ Konkretne działania ze strony przełożonego
    - ☐ Żadne z powyższych
    - ☐ W moim miejscu pracy nie są stosowane uwierzytelnienia
20. Proszę ocenić w skali 1–5, na ile poniższe działania mają według Pana(i) znaczenie w motywowaniu do bezpiecznego korzystania z dostępu do danych.

Działania kierownictwa	Znaczenie (1 – nieważne, 5 – bardzo ważne)
Zapewnienie wsparcia technicznego i merytorycznego	
Szkolenie dot. zasad bezpiecznego korzystania z systemów informatycznych podczas wdrażania do pracy	
Szkolenia cykliczne (utrwalające) dot. zasad bezpiecznego korzystania z systemów informatycznych	
Konsultacje dotyczące zasad i narzędzi uwierzytelniania	
Wyznaczanie i komunikowanie zasad dot. bezpiecznego korzystania z systemów informatycznych	
Ocena pracy pracownika w aspekcie bezpiecznego użytkowania systemów informatycznych	
Bieżąca kontrola i reagowanie na nieprzestrzeganie zasad	
Motywacja finansowa	

21. Biorąc pod uwagę bieżącą sytuację Pana(i) zakładu pracy proszę zaznaczyć (używając poniższej skali), w jakim stopniu zgadza się Pan(i) z poszczególnymi sformułowaniami.

1 – zdecydowanie nie zgadzam się | **2** – raczej nie zgadzam się | **3** – stanowisko neutralne | **4** – raczej zgadzam się | **5** – zdecydowanie zgadzam się

Przywództwo

Najwyższa kadra zarządzająca ma na uwadze możliwości oraz zagrożenia, jakie daje dostęp pracownika do zasobów informatycznych	1 2 3 4 5
Zapewnienie bezpieczeństwa dostępu do danych wpisuje się w ogólną strategię mojego zakładu pracy	1 2 3 4 5
W moim zakładzie pracy panuje kultura zabezpieczania informacji w ramach całej organizacji	1 2 3 4 5
Mój zakład pracy posiada jasno określoną i zaakceptowaną strategię rozwoju w zakresie bezpieczeństwa dostępu do systemów informatycznych	1 2 3 4 5
Bezpieczeństwo danych jest ważniejsze niż efektywność pracy	1 2 3 4 5

Styl zarządzania

Mamy standardowy proces administracyjny w zakresie zarządzania dostępem do systemów informatycznych	1 2 3 4 5
Posiadamy stabilne wskaźniki oceny kosztów/korzyści zabezpieczenia dostępu do systemów informatycznych	1 2 3 4 5
Posiadamy jasno sprecyzowane funkcje, zakresy obowiązków, odpowiedzialności i kontroli w odniesieniu do kwestii związanych z dostępem do systemów informatycznych	1 2 3 4 5
Kierownicy są kompetentni i dobrze motywowani do zabezpieczenia dostępu do systemów informatycznych oraz egzekwowania bezpiecznego ich użycia przez ich podwładnych	1 2 3 4 5
Dział IT (wsparcie techniczne) udziela szybkiego i kompleksowego wsparcia, a współpraca z nim przebiega bez zakłóceń	1 2 3 4 5

Kompetencje

Zakład pracy jest w stanie funkcjonować w otoczeniu szybkich i wciąż zachodzących zmian	1 2 3 4 5
Dostęp do odpowiednich zasobów systemów informatycznych jest udzielany niezwłocznie i właściwie (np. w przypadku przyjęcia nowego pracownika)	1 2 3 4 5

Osoby zarządzające biznesem mają wiedzę technologiczną, a osoby zarządzające technologią mają wiedzę biznesową	1	2	3	4	5

22. Załóżmy, że ma Pan(i) możliwość wpływu na to, jak powinno wyglądać uwierzytelnienie na Pana(i) stanowisku pracy. Bazując na swoim doświadczeniu i specyfice zakładu pracy, proszę określić jak powinno wyglądać korzystanie z uwierzytelnień by zapewnić zarówno bezpieczeństwo danych, jak i wygodę dla pracowników? Proszę dokonać wyboru.

Główna metoda uwierzytelnienia to:

- ☐ Login i hasło lub sam PIN
- ☐ Wzór rysowany palcem po ekranie (symbol odblokowania)
- ☐ Przedmiot niezabezpieczony hasłem (urządzenie lub karta kodów jednorazowych)
- ☐ Przedmiot dodatkowo zabezpieczony hasłem
- ☐ Cechy biometryczne, jakie?
  ……
  ……

Liczba narzędzi uwierzytelnienia (orientacyjnie):

- Różne hasła i loginy /PINy / symbole.....
- Różne przedmioty uwierzytelniające .....
- Różne cechy biometryczne .....

Gdyby stosowane miałyby być hasła, jakie określił(a)by Pan(i) wytyczne?

(wielokrotny wybór – proszę zaznaczyć wybrane opcje i ew. uzupełnić wykropkowania)

- ☐ Długość **……** znaków
- ☐ Co najmniej 1 mała i 1 wielka litera
- ☐ Co najmniej 1 cyfra
- ☐ Co najmniej 1 znak specjalny
- ☐ Zmiana hasła **…….** razy na **…….**
- ☐ Hasła do różnych aplikacji nie mogą się powtarzać
- ☐ W hasłach zabrania się stosowania ważnych dat, imion, prostych słów czy sekwencji (np. 12345)

CZĘŚĆ 4. CHARAKTERYSTYKA PRACOWNIKA I JEGO ZAKŁADU PRACY

23. Proszę uzupełnić Pana(i) profil przez uzupełnienie wykropkowania lub podkreślenie właściwych odpowiedzi (tekst pogrubioną czcionką).
    - Staż pracy **…….** lat
    - Stosowanie uwierzytelnienia od około **……** lat
    - Praca w firmie z branży IT lub stanowisko pracy wymagające przygotowania informatycznego: **tak / nie**
    - Samoocena wiedzy dotyczącej bezpiecznego wykorzystania uwierzytelnienia: **wysoka / przeciętna / niska**
    - Wiek **……** lat
    - Płeć: **kobieta / mężczyzna**
    - Wykształcenie: **podstawowe / średnie / wyższe**
    - Stanowisko kierownicze: **tak / nie**
24. Proszę uzupełnić profil Pana(i) zakładu pracy.
    - Wielkość mierzona liczbą pracowników (podana nawiasach)

Jednoosobowe (1)	Mikro (2–9)	Małe (10–50)	Średnie (51–249)	Duże (powyżej 250)
☐	☐	☐	☐	☐

- Charakter działalności

Produkcyjny	Produkcyjno-usługowy	Usługowy	Administracja publiczna
☐	☐	☐	☐