POLITECHNIKA LUBELSKA

Marta Juszczyk

Tożsamość cyfrowa pracowników MSP w Polsce

Kwantyfikacja modelu DIAM

MONOGRAFIE

Lublin 2021

Tożsamość cyfrowa pracowników MSP w Polsce

Kwantyfikacja modelu DIAM

Monografie – Politechnika Lubelska

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

Marta Juszczyk

Tożsamość cyfrowa pracowników MSP w Polsce

Kwantyfikacja modelu DIAM

Wydawnictwo
Politechniki Lubelskiej

Lublin 2021

Recenzenci:
prof. dr hab. Ewa Ziemba, Uniwersytet Ekonomiczny w Katowicach
dr hab. inż. Janusz Wielki, prof. Politechniki Opolskiej
dr hab. inż. Jerzy Montusiewicz, prof. Politechniki Lubelskiej

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

Publikacja wydana za zgodą Rektora Politechniki Lubelskiej

ISBN: 978-83-7947-504-9

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

Druk: Soft Vision Mariusz Rajski
www.printone.pl

Nakład: 50 egz.

Spis treści

Tożsamość cyfrowa pracowników MSP w Polsce. Kwantyfikacja modelu DIAM.

Streszczenie

W pracy zbadano praktykę stosowania tożsamości cyfrowych w przedsiębiorstwach oraz skwantyfikowano autorski model DIAM (Digital Identity Acceptance Model) zaproponowany w monografii pt. *Rozbudowa modelu akceptacji technologii dla potrzeb bezpiecznego wykorzystania tożsamości cyfrowej w małych i średnich przedsiębiorstwach. Cz. I Modelowanie*.

W tym celu przebadano 202 respondentów z sektora małych i średnich przedsiębiorstw. Analiza odpowiedzi umożliwiła zbadanie, jak w przedsiębiorstwach respondentów wygląda organizacja dostępu do zasobów, wdrożenie polityki bezpieczeństwa oraz jakie są stosowane narzędzia uwierzytelniające. Przeanalizowano także faktyczne działania respondentów w kwestii korzystania z haseł i przedmiotów uwierzytelniających, ocenę obecnie stosowanych rozwiązań oraz preferencje pracowników co do narzędzi i zasad dotyczącymi uwierzytelnienia.

Dzięki porównaniu bezpieczeństwa użycia tożsamości cyfrowej przez kierowników i osób na stanowiskach wykonawczych, a także oceny siły wpływu działań przełożonych na zachowania ich podwładnych, ujawniono dwie luki kompetencji: w kwestii bezpieczeństwa tożsamości cyfrowych (pracownicy wykonawczy) oraz odpowiedniej motywacji podwładnych (kierownicy).

Wynikiem pracy były: sub-model DIAM-0, identyfikujący działania zarządcze wspierające bezpieczeństwo tożsamości cyfrowych pracowników oraz trzy sub-modele dedykowane poszczególnym narzędziom uwierzytelnienia: DIAM-H (dla haseł), DIAM-P (dla przedmiotów uwierzytelniających) oraz DIAM-B (dedykowany uwierzytelnieniu biometrycznemu).

Na podstawie interpretacji ujawnionych zależności w modelach, praktyki stosowania tożsamości cyfrowych w małych i średnich przedsiębiorstwach oraz zidentyfikowanych luk, sformułowano 17 praktycznych wniosków dotyczących obszaru wspierania bezpieczeństwa tożsamości cyfrowych. Wraz ze zidentyfikowanymi zależnościami, stały się one podstawą do sporządzenia 20 rekomendacji dla kadry menedżerskiej, które mogą być zastosowane na etapie projektowania systemu bezpieczeństwa informacji, do wspierania działań i kompetencji przełożonych, praktycznego kształtowania postaw pracowników wobec bezpiecznego uwierzytelniania się, a także zmniejszania oporu pracowników podczas wprowadzania uwierzytelnienia biometrycznego w przedsiębiorstwach.

Słowa kluczowe: DIAM, TAM, tożsamość cyfrowa, bezpieczeństwo systemów informatycznych.

Digital Identity of the SME’s employees in Poland. DIAM model quantification.

Abstract

The study examines the practice of using digital identity in enterprises and quantifies the original DIAM model (Digital Identity Acceptance Model) proposed in the monograph entitled *Development of the Technology Acceptance Model for the safe use of Digital Identity in small and medium-sized enterprises. I. Modelling.*

For this purpose, 202 respondents from the small and medium-sized enterprises sector were tested. The analysis allow to examine how organizations provide an access to IT resources, implement the security policy, and what authorization solution they have used. The respondents' actual actions in terms of the use of passwords and authentication objects were also analyzed, as well as the assessment of current solutions and their preferences to authentication tools and rules.

Due to the comparison of the security of the use of digital identity by managers and people in executive positions, as well as the assessment of the strength of the impact of superiors' actions on the behavior of their subordinates, two competency gaps were revealed: in terms of the security of digital identities (executive employees) and appropriate motivation of subordinates (managers).

The result of the work were: the DIAM-0 sub-model, identifying management activities supporting the security of employees' digital identities, and three sub-models dedicated to individual authentication tools: DIAM-H (for passwords), DIAM-P (for authentication objects) and DIAM- B (dedicated to biometric authentication).

Based on the interpretation of the revealed dependencies in models, the practice of using digital identities in small and medium-sized enterprises, and the identified gaps, 17 practical conclusions in the area of supporting digital identity security have been formulated. Together with the identified dependencies, they have become the basis for the preparation of 20 recommendations for managerial staff, which can be used at the stage of designing the information security system, to support the activities and competences of superiors, the practical shaping of employees' attitudes towards secure authentication, as well as reducing employee resistance when introducing biometric authentication in enterprises.

Keywords: DIAM, TAM, Digital Identity, Information Systems Security.

1. Wprowadzenie

Jednym z czynników sukcesu przedsiębiorstw wkraczających w erę Przemysłu 4.0 jest właściwe operowanie informacją, czyli jej gromadzenie, filtrowanie, wykorzystywanie do podejmowania działań oraz właściwe zabezpieczenie. Przenoszenie do świata wirtualnego obsługi kolejnych procesów, rozwój automatyzacji czy Internetu Rzeczy sprawiają, że bezpieczeństwo systemów informatycznych przedsiębiorstw staje się kwestią, od której w coraz większym stopniu zależy ciągłość funkcjonowania firmy[1]. Zostało to dostrzeżone przez prawodawców, którzy dostosowują przepisy do wymogów współczesnej, coraz bardziej zwirtualizowanej gospodarki, ale też niestety przez cyberprzestępców. Systemy informatyczne mogą być bowiem miękkim podbrzuszem przedsiębiorstwa.

Paradoksalnie, od lat największym zagrożeniem dla bezpieczeństwa wirtualnych zasobów jest ich użytkownik, szczególnie taki, który nie postrzega wpływu swoich działań na bezpieczeństwo informatyczne przedsiębiorstwa[2]. Pandemia Sars-Cov-2, która rozpoczęła się na przełomie 2019 i 2020 roku jeszcze mocniej uwypukliła znaczenie właściwych nawyków pracowników, którzy masowo zaczęli pracować zdalnie, poza bezpośrednią, fizyczną kontrolą przełożonych korzystając z tzw. tożsamości cyfrowych umożliwiających zdalny dostęp do zasobów informatycznych przedsiębiorstwa.

Zmiana nawyków wymaga relatywnie długiego czasu, stąd ważne jest poznanie nawyków pracowników i identyfikacja czynników, które wspierają bezpieczne korzystanie z systemów informatycznych.

W niniejszej monografii przedstawiono kwantyfikację autorskiego modelu DIAM (Digital Identity Acceptance Model)[3] będącego adaptacją modelu TAM (Technology Acceptance Model)[4] dla potrzeb stosowania tożsamości cyfrowych przez pracowników MSP w sposób bezpieczny.

Model DIAM został przedstawiony w monografii pt. *Rozbudowa modelu akceptacji technologii dla potrzeb bezpiecznego wykorzystania tożsamości cyfrowej w małych i średnich przedsiębiorstwach. Cz. I Modelowanie.* Model DIAM powstał w wyniku procesu, którego pierwszym etapem była analiza literatury dotyczącej tożsamości cyfrowej w systemach informatycznych. Punktem wyjścia

[1] Wendzel, S., Mazurczyk, W., Caviglione, L., Houmansadr, A. (2022). *Emerging topics in defending networked systems*. Future Generation Computer Systems, Vol. 128, s. 317–319.

[2] Ogbanufe, O. (2021). *Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity*. Computers and Security, Vol. 108.

[3] Juszczyk, M. (2020). *Rozbudowa modelu akceptacji technologii dla potrzeb bezpiecznego wykorzystania tożsamości cyfrowej w małych i średnich przedsiębiorstwach. Cz. I Modelowanie*. Wydawnictwo Politechniki Lubelskiej. Lublin.

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

było pojęcie tożsamości oraz różne aspekty jej odzwierciedlenia w systemach informatycznych. Przeanalizowano różne ujęcia tożsamości cyfrowej i na podstawie dyskusji licznych koncepcji, na potrzeby pracy zdefiniowano, że tożsamość cyfrowa to[5]: ***„zbiór atrybutów pozwalających na jednoznaczną identyfikację i uzyskanie uprawnionego dostępu do zasobów przedsiębiorstwa przez pracownika lub pracowników i przez nich współtworzona i współzarządzana."***

Ta definicja niesie za sobą szereg ukonkretnień. Przede wszystkim model dotyczy tzw. kont pracowników w systemach informatycznych, za pomocą których mogą oni uzyskać dostęp do programów czy urządzeń niezbędnych do wykonywania powierzonych obowiązków. W definicji uwypuklone zostały ponadto aspekty identyfikacji i uwierzytelnienia, gdyż czynnikiem krytycznym jest zapewnienie, że osoba korzystająca z danego konta jest osobą do tego uprawnioną. Współtworzenie i współzarządzanie, czyli np. możliwość ustawienia własnego hasła, wskazują na pewną dowolność podejmowanych działań, które mają konkretny wpływ na sposób ochrony dostępu, a przez to wpływają w istotny sposób na poziom bezpieczeństwa zasobów w systemach informatycznych. Dość oczywistym, ale wartym podkreślenia elementem przytoczonej definicji tożsamości cyfrowej jest kwestia zastosowania konta do realizacji zadań związanych z pracą zawodową.

Należy podkreślić, iż przytoczona definicja jest znacznie zawężona, pomija bowiem zarówno inne obszary jak i cele zastosowania tożsamości cyfrowych. Tożsamość cyfrowa bowiem może zapewniać także dostęp do np. usług e–administracji czy powalać na uzyskanie dostępu do zasobów i usług wykorzystywanych w życiu prywatnym[6]. Różne mogą być też cele ich zastosowania, a w tym m.in. tworzenie wirtualnych społeczności[7], personalizacja[8] czy monetyzacja treści[9]. Mimo generalnie podobnych funkcji wspomnianych tożsamości

[5] Juszczyk, M. (2020). *Rozbudowa modelu akceptacji technologii dla potrzeb bezpiecznego wykorzystania tożsamości cyfrowej w małych i średnich przedsiębiorstwach. Cz. I Modelowanie*. Wydawnictwo Politechniki Lubelskiej. Lublin, s. 22.

[6] Jasiewicz, J. i in. (2014). *Ramowy katalog kompetencji cyfrowych*. Warszawa: Centrum Cyfrowe, 68 s. Online: https://www.academia.edu/12624330/Ramowy_Katalog_Kompetencji_Cyfrowych, dostęp: 30.11.2021 oraz 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.

[7] Meng, J. (2022). *Information acquisition, persuasion, and group conformity of online tribalism: Does user activeness matter?*. International Journal of e-Business Research, Vol. 18, Iss. 2.

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

[9] Lu, S. i in. (2021). *Do larger audiences generate greater revenues under pay what you want? Evidence from a live streaming platform.* Marketing Science, Vol. 40, Iss. 5, s. 964-984.

cyfrowych, czyli zapewnienie autoryzowanego dostępu do treści w systemach informatycznych, zachowania użytkowników tych tożsamości cyfrowych mogą być bardzo różne. Wpływ na to mogą mieć m.in. różne polityki bezpieczeństwa, regulaminy, mechanizmy zabezpieczające czy wreszcie znaczenie, jakie użytkownik im przypisuje. Może się to przekładać na sposób korzystania z tożsamości cyfrowych i ich bezpieczeństwo.

Istotne dla kont pracowników, za pomocą których pracownicy uzyskują dostęp do zasobów informatycznych firmy, jest kształtowanie faktycznego sposobu użytkowania kont przez czynnik techniczny (a w tym wymogi egzekwowane przez systemy informatyczne), ludzki (w tym nawyki, ale i świadomość pracownika) oraz organizacyjny (zestaw reguł i polityk, którym podlega pracownik).

Z punktu widzenia przedsiębiorstwa konta mogą być zarządzane w oparciu o różne modele. W literaturze jako podstawowe modele wymieniane są: model autonomiczny, scentralizowany, sfederowany oraz kontrolowany przez użytkownika[10]. Niezależnie jednak od samego modelu tożsamości cyfrowe powiązane są z zestawem podobnych działań podejmowanych w ramach zarządzania kontami użytkowników[11], czyli m.in. przydzielanie czy modyfikacja uprawnień. Z punktu widzenia użytkownika natomiast najczęstszym działaniem jest wielokrotnie powtarzany proces uzyskiwania dostępu do zasobów z wykorzystaniem tożsamości cyfrowych.

Tu warto poświęcić uwagę narzędziom uwierzytelniającym. Generalnie są trzy podstawowe metody uwierzytelnienia: opierające się na znajomości informacji, posiadaniu przedmiotu oraz posiadaniu cech fizycznych lub behawioralnych. Każda z tych metod posiada wady oraz zalety oraz wyznaczniki bezpieczeństwa stosowania. Jednym z podstawowych aspektów, które decydują o bezpieczeństwie uwierzytelnienia jest tzw. „czynnik ludzki", czyli z jednej strony skłonność do wygody[12], ale także obawy użytkowników przed stosowaniem niektórych

[10] *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representtations* (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 oraz 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.

[11] Azhar, M.I. (2017). *Systematic Review of Identity Access Management in Information Security*. International Journal Of Innovations In Engineering Research And Technology [IJIERT], Vol. 4, Iss. 7.

[12] German, R.L., Barber, K.S. (2018). *Consumer Attitudes About Biometric Authentication.* UT CID Biometrics Report. Online: https://identity.utexas.edu/sites/default/files/2020-09/Consumer%20Attitudes%20About%20Biometrics.pdf, dostep: 30.11.2021.

rozwiązań[13] rzutujące na społeczną akceptację tych narzędzi uwierzytelniających[14].

Model DIAM został przygotowany dla celów badań tożsamości cyfrowych wykorzystywanych w małych i średnich przedsiębiorstwach (MSP) w Polsce. Przyczyną tego wyboru było duże znaczenie tych przedsiębiorstw dla gospodarki Polski, ale i analiza specyficznych uwarunkowań tego sektora. Ubogie zasoby finansowe czy ograniczony dostęp do specjalistów, które redukują możliwość zakupu oprogramowania zarządzającego tożsamościami cyfrowymi lub tworzenie odpowiednich procedur, jak ma to miejsce w np. w międzynarodowych korporacjach powodują, że ta grupa przedsiębiorstw staje się podatna na nadużycia związane z korzystaniem z systemów informatycznych firmy z użyciem tożsamości cyfrowych. Potwierdzają to badania związane z cyberprzestępczością[15] wskazujące na wysokie zagrożenie ze strony cyberprzestępców dla przedsiębiorstw sektora MSP.

Same zagrożenia dla bezpieczeństwa informatycznego przedsiębiorstw są liczne. Wielu autorów klasyfikuje zagrożenia w oparciu o różne czynniki takie jak[16] m.in. źródło zagrożeń, ich pochodzenie czy ocenę skutków. Identyfikuje się też sprawców naruszeń bezpieczeństwa[17]: od hakerów, przestępców komputerowych motywowanych osiągnięciem korzyści majątkowej, przez cyberterrorystów, szpiegów przemysłowych po własnych pracowników. W przypadku pracownika działanie narażające bezpieczeństwo zasobów systemów informatycznych na szwank może być nieintencjonalne i wynikać z braków wiedzy czy zwykłej pomyłki. Zdarzają się oczywiście świadome naruszenia powodowane m.in. nieuczciwością pracownika, jego pragnieniem zemsty czy spodziewanymi korzyściami majątkowymi.

Wśród zagrożeń istnieją takie, które związane są bezpośrednio ze zdefiniowaną uprzednio tożsamością cyfrową, w szczególności: wykorzystują słabości wspomnianych mechanizmów uwierzytelniania tożsamości cyfrowych (m in. atak

[13] Kumar M., Kumar N. (2020). *Cancelable Biometrics: a comprehensive survey*. Artificial Intelligence Review, Vol. 53, Iss. 5, s. 3403–3446.

[14] Kostka, G., Steinacker, L., Meckel, M. (2020). *Between Privacy and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the UK and the US*, SSRN, doi: http://dx.doi.org/10.2139/ssrn.3518857.

[15] *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: 2021.11.30.

[16] Król, K. (2015) *Organizacyjne aspekty zarządzania bezpieczeństwem danych z perspektywy zagrożeń phishingu*. Organizacja i Zarządzanie, Wyd. Kwartalnik naukowy 2 (30), Politechniki Śląskiej, s. 23–24.

[17] Brar, H.S., Kumar, G. (2018). *Cybercrimes: A Proposed Taxonomy and Challenges.* Journal of Computer Networks and Communications, Vol. 2018.

brute force, skimming[18], imitacja badanej cechy np. sztuczny odcisk palca[19]) i korzystających z nich użytkowników (phishing[20], atak socjotechniczny[21]).

Aby ograniczyć ryzyko wystąpienia tych zagrożeń oprócz instalowania specjalistycznego oprogramowania przedsiębiorstwa mogą wprowadzać zalecenia i procedury szczególnie, że niektóre działania związane z zarządzaniem tożsamościami cyfrowymi podlegają regulacji ze strony prawodawcy[22]. Wspomniane zalecenia oraz procedury powinny uwzględniać dobre praktyki i zalecenia jednostek zajmujących się zabezpieczeniem systemów informatycznych.

Żadne jednak zabezpieczenia nie zrekompensują w pełni braku odpowiedniego postępowania ze strony użytkowników. W obliczu podatności narzędzi uwierzytelnienia na zagrożenie, proste narzucenie sposobu korzystania z kont jest niewystarczające. Bardzo ważna wydaje się wiedza i wola korzystania z tożsamości cyfrowych w sposób bezpieczny jeśli przekładają się one na bezpieczeństwo stosowania tożsamości cyfrowych.

Wielu autorów podejmuje temat dotyczący zachowań użytkowników systemów informatycznych, identyfikując typowe postawy wobec kwestii bezpieczeństwa (np. kierowanie się wygodą, nieufnością, obawami lub brak wiedzy i chaotyczne działania)[23] oraz upatrując ich przyczyn w przekonaniach użytkowników takich jak niemożność uniknięcia naruszeń bezpieczeństwa[24], myślenia życzeniowego[25] czy też lęku[26]. Z drugiej strony badania wskazują na

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

[19] Saguy, M i in. (2021). *Proactive forensic science in biometrics: Novel materials for fingerprint spoofing*. Journal of Forensic Science, s. 1–9.

[20] Fincher, M., Hadnagy, Ch. (2016). Mroczne odmęty phishingu. Nie daj się złowić!. Gliwice: Wydawnictwo Helion.

[21] Mitnick, K.D., Simon, W. (2016). *Sztuka podstępu. Łamałem ludzi, nie hasła*. Wyd. II. Gliwice: Wydawnictwo Helion.

[22] *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* oraz *Dz.U. 1997 Nr 133 poz. 883 USTAWA z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*.

[23] 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-

[24] McLeodal, A., Dolezel, D. (2022) *Information security policy non-compliance: Can capitulation theory explain user behaviors?*. Computers and Security, Vol. 112.

[25] Chen, D.Q., Liang, H. (2019). *Wishful Thinking and IT Threat Avoidance: An Extension to the Technology Threat Avoidance Theory*. IEEE Transactions on Engineering Management, Volume 66, Issue 4, s. 552–567.

[26] Ogbanufe, O., Pavur, R. (2022). *Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection*. International Journal of Information Management, Vol. 62.

rolę przełożonego w kształtowaniu podejścia jego podwładnych do kwestii bezpieczeństwa[27].

Model DIAM został zbudowany w oparciu o TAM, który jest jednym z najbardziej uniwersalnych i potwierdzonych modeli tłumaczących zachowanie użytkowników technologii. Ponadto DIAM zawiera czynniki indywidualnej percepcji użytkownika (postrzegane korzyści i straty, świadomość zagrożeń, postrzegane wymuszenie), a także dotyczące jego charakterystyki, narzędzi uwierzytelniających oraz wpływu zarządzania i kultury organizacji na bezpieczeństwo tożsamości cyfrowych.

DIAM jest modelem, który zbudowany został na podstawie przesłanek płynących z badań literaturowych i badań wstępnych. Istniała potrzeba zbadania, które z założonych zmiennych oraz zależności znajdują odzwierciedlenie w rzeczywistości. Badania zostały wykonane przed zaostrzeniem przepisów w kwestii ochrony danych osobowych (RODO) oraz przed pandemią Sars-Cov-2. Zatem ich wyniki mogą zostać użyte jako punkt odniesienia, a rekomendacje, szczególnie w obliczu ograniczonego wykorzystania uwierzytelnienia biometrycznego oraz trwałości nawyków, uznane za użyteczne.

1.1. Cele pracy

Cel główny

Celem głównym pracy jest kwantyfikacja Modelu DIAM (Digital Identity Acceptance Model, DIAM)[28] dla pracowników małych i średnich przedsiębiorstw.

Celami poznawczymi są:

1. Zbadanie i opis stanu faktycznego wykorzystania tożsamości cyfrowej przez pracowników MSP w Polsce.
2. Identyfikacja preferencji pracowników w stosunku do tożsamości cyfrowej.
3. Identyfikacja różnic w postrzeganiu bezpieczeństwa tożsamości cyfrowej pomiędzy pracownikami na stanowiskach wykonawczych i kierowniczych.

Cel utylitarny:

1. Sformułowanie rekomendacji dla kadry zarządzającej, określających sposób zwiększenia bezpieczeństwa wykorzystania tożsamości cyfrowej pracowników sektora MSP oraz jego implementację.

---

[27] Liu, C., Wang, N., Liang, H. (2020). *Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment*. International Journal of Information Management, Vol. 54.

[28] Juszczyk, M. (2020). *Rozbudowa modelu akceptacji technologii dla potrzeb bezpiecznego wykorzystania tożsamości cyfrowej w małych i średnich przedsiębiorstwwach. Cz. I Modelowanie*. Wydawnictwo Politechniki Lubelskiej. Lublin.

Ponadto, model DIAM, będzie mógł być użyty do:

- planowania, wdrażania, kontrolowania i usprawniania funkcjonowania (zgodnie z koncepcją PDCA Deminga[29]) obszaru zarządzania tożsamością cyfrową w MSP;
- klasyfikacji czynników oraz ocena istotności ich wpływu na bezpieczeństwo wykorzystania systemów informacyjnych przedsiębiorstw sektora MSP, w szczególności w aspekcie stosowania tożsamości cyfrowej przez ich pracowników;
- wspierania procesów priorytetyzacji działań kierownictwa prowadzących do zwiększenia wieloaspektowego bezpieczeństwa wykorzystania posiadanych systemów informatycznych przedsiębiorstwa (w różnych aspektach: technicznych, organizacyjnych i innych);
- racjonalizacji doboru narzędzi oddziaływania na pracowników MSP w celu zwiększenia bezpieczeństwa stosowania tożsamości cyfrowej, w szczególności w zakresie ich uświadamiania i motywowania do bezpiecznego wykorzystania swojej tożsamości cyfrowej.

1.2. Zakres przedmiotowy, podmiotowy i czasowy badań

Przedmiot badań stanowi zagadnienie bezpiecznego wykorzystania tożsamości cyfrowej przez pracowników w małych i średnich przedsiębiorstwach oraz analiza ich postaw, intencji i użycia tożsamości cyfrowych w kontekście bezpiecznego funkcjonowania systemów informatycznych przedsiębiorstw.

Podmiot badań stanowią małe i średnie przedsiębiorstwa w Polsce. Są one zagrożone niewłaściwym stosowaniem tożsamości cyfrowych w sposób szczególny. Zagrożenie to wynika z ograniczoności zasobów (finansowych, czasowych, osobowych)[30], które mogą być użyte do zapewnienia bezpiecznego stosowania tożsamości cyfrowej.

Zakres czasowy badań to lata 2015-2016.

[29] Deming, W.E. (1993). *The New Economicst*. Cambridge: MIT Press s. 135.

[30] Pasławski, K. (2020). *Z czym nie radzą sobie MŚP*. CRN Polska. Online: https://crn.pl/aktualnosci/z-czym-nie-radza-sobie-msp/, 2021-05-21.

1.3. Ogólne aspekty metodyczne kwantyfikacji wstępnego modelu DIAM

Aby osiągnąć główny cel pracy, czyli skwantyfikować zaproponowany model DIAM przyjęto następujący tok działań:

- Realizacja koncepcji (przeprowadzenie badań).
- Opracowanie i przedstawienie wyników.
- Dyskusja i wnioskowanie.

Dokonano analizy zgromadzonego materiału badawczego. Przedstawiono wyniki analizy poszczególnych pytań, obliczono siłę zależności między elementami modelu DIAM, wyeliminowano czynniki, których siła wpływu nie została potwierdzona wynikami badań.

Wypracowano szereg rekomendacji adresowanych do menedżerów:

- przydatnych podczas projektowanie systemu bezpieczeństwa informacji,
- związanych z działaniami i kompetencjami przełożonych,
- wspomagających kształtowanie postaw pracowników wobec bezpiecznego uwierzytelniania się,
- dotyczących zmniejszania oporu pracowników podczas wprowadzania uwierzytelnienia biometrycznego.

Proces podzielono na zadania badawcze, które wraz z rezultatami zadań przedstawiono w tabeli 1.1.

Tabela 1.1. Proces badawczy – kwantyfikacja

Etap badań	Zadania badawcze	Rezultaty
Kwantyfikacja modelu DIAM i wnioskowanie	1. Analiza statystyczna wyników badań właściwych	Rezultaty analizy statystycznej
	2. Skwantyfikowanie modelu DIAM	Model DIAM
	3. Wypracowanie wniosków i rekomendacji wynikających z modelu DIAM	Wnioski i rekomendacje

Źródło: opracowanie własne.

Szczegółowe założenia i metodyka dotyczące kwantyfikacji modelu, takie jak przyjęte nazewnictwo elementów modelu, narzędzia analizy statystycznej, hipotezy statystyczne czy sposób wnioskowania zawarto w rozdziale 5.1.

2. Dobór próby badawczej i realizacja badań

2.1. Założenia dotyczące próby badawczej i praktyki badań

Badanie tożsamości cyfrowych w małych i średnich przedsiębiorstwach jest bardzo trudne z uwagi na dwa, identyfikowane już na etapie badań wstępnych, krytyczne czynniki: trudność pozyskania danych i podwyższone ryzyko ich nierzetelności.

Trudność pozyskania danych wynika z faktu, że bezpieczeństwo systemów informatycznych jest obszarem wrażliwym, dotyczącym informacji poufnych. Pracownicy przedsiębiorstw i ich kierownicy obawiają się ich ujawniania. W konsekwencji, istnieje duże prawdopodobieństwo, że pozyskanie informacji na temat stosowania tożsamości cyfrowej będzie niezwykle trudne, wręcz uniemożliwione przez decyzje kierownictwa, procedury wewnętrzne lub obawy pracowników.

Próby przeprowadzenia badań w wybranych przedsiębiorstwach były nieskuteczne (z jednym wyjątkiem), stąd zrezygnowano z klasycznego losowego doboru próby badawczej z uwagi na ryzyko braku uzyskania wystarczającego materiału badawczego i zdecydowano się na dobór przypadkowy.

Z uwagi na trudny temat, dotykający kompetencji respondentów, ich przełożonych i bezpieczeństwa informatycznego całego przedsiębiorstwa, rzetelność odpowiedzi jest istotnym czynnikiem wpływającym na wiarygodność wyników badań i wnioskowanie.

Zidentyfikowano szereg czynników, które mogłyby mieć wpływ na rzetelność odpowiedzi. Do pierwszej grupy czynników należą: poczucie presji ze strony przełożonych oraz obawy dotyczące wpływu odpowiedzi na karierę zawodową. Skutkiem mogą być działania asekuracyjne, a w szczególności: ukrywanie prawdziwych zachowań, luk bezpieczeństwa informatycznego, nieraportowanie nieprawidłowości. Rozwiązaniem tego problemu jest zapewnienie poczucia braku możliwości powiązania wyników kwestionariusza z osobą, która go wypełniła oraz firmą, w której pracuje. Można to osiągnąć przeprowadzając badania poza siedzibą przedsiębiorstwa, w dużej grupie, w której skład wchodzą osoby spoza przedsiębiorstwa.

Druga grupa czynników związana jest z motywacją respondentów do rzetelnego wypełniania ankiety czyli: skłonność do przestawienia się w jak najlepszym świetle, postawa niezaangażowania czy niechęć do dzielenia się posiadaną wiedzą. Efektem może być niestaranne czy wręcz przypadkowe wypełnianie ankiety, pomijanie pytań czy podawanie nieprawdziwych odpowiedzi. Szczególnie w przypadku długich ankiet zmotywowanie respondentów do udzielenia odpowiedzi jest bardzo trudne. Sposobem na zwiększenie jakości zwracanych kwestionariuszy są: brak presji czasu, osobiste zaangażowanie badacza (rzetelne

przedstawienie badań, wzbudzanie sympatii i zaufania) oraz wykorzystanie autorytetu (powołanie się na osobę lub instytucję).

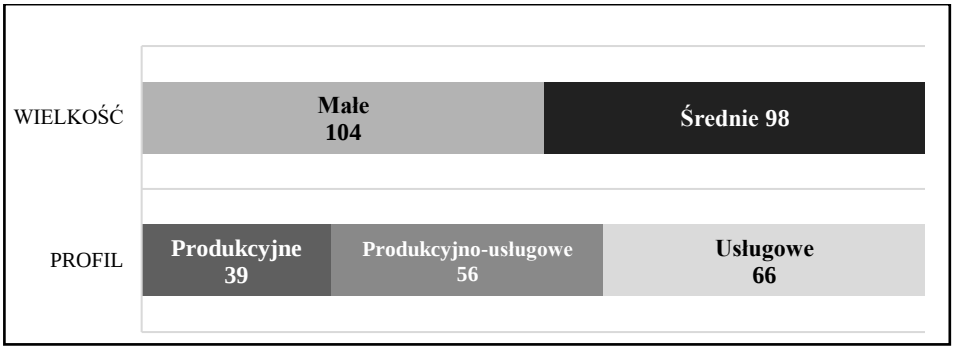
Trzecia grupa czynników związana jest z możliwością kontroli zgodności odpowiedzi respondenta ze stanem faktycznym. W ankiecie występują dwa rodzaje pytań: wprost odnoszące się do obiektywnych faktów np. wielkość przedsiębiorstwa, i takie, na które odpowiedź jest subiektywna tj. wymagające szacowania np. podatność przedsiębiorstwa na ataki oraz te dotyczące odczuć respondenta np. stosunek do narzędzia uwierzytelniania. W procesie badawczym pytania odnoszące się do faktów mogą być kontrolowane przez badacza: niektóre dotyczące np. wieku respondenta, jego płci, czy wielkości przedsiębiorstwa w sposób relatywnie łatwy, inne np. częstotliwość korzystania z narzędzi uwierzytelnienia wymagają znacznego zaangażowania innych pracowników przedsiębiorstwa takich jak przełożony czy wsparcie techniczne. Jednakże kontrolowanie nawet tych podstawowych parametrów może znacząco zmniejszyć poczucie anonimowości i przełożyć się na niższą rzetelność wyników. Głównym celem pracy jest rozbudowa modelu akceptacji technologii dla potrzeb bezpiecznego wykorzystania tożsamości cyfrowej, bazującego w dużej mierze na indywidualnych odczuciach użytkownika, stąd zrezygnowano z weryfikowania odpowiedzi respondentów.

2.2. Charakterystyka próby badawczej

2.2.1. Charakterystyka ogólna próby badawczej

Próbę stanowili w podobnym udziale reprezentanci małych i średnich przedsiębiorstw z województwa lubelskiego (ok. 80%), świętokrzyskiego (ok.15%) oraz innych regionów kraju (ok. 5%).

Najwięcej respondentów zatrudniały przedsiębiorstwa usługowe, najmniej zaś produkcyjne (wykres 2.1.).



Wykres 2.1. Charakterystyka przedsiębiorstw respondentów

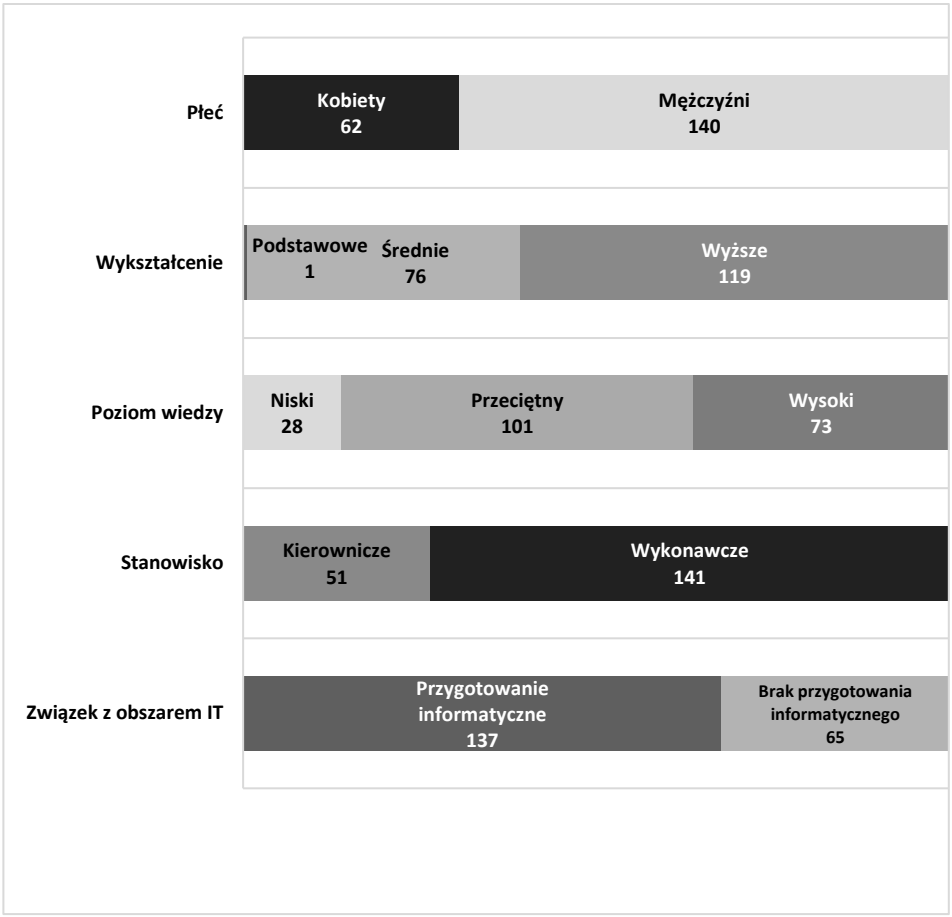
Źródło: opracowanie własne.

Blisko 98% badanych ujawniło swój wiek, który oscylował się między 20 a 58 lat i wynosił średnio 29,56 lat. Odchylenie standardowe dla tego pytania wynosiło 9,1 lat.

Ok. 95% respondentów podało staż pracy, który zawierał się w przedziale 0–25 lat i wynosił średnio 5,62 lat. Odchylenie standardowe dla tego pytania wyniosło 5,77.

Na pytanie dotyczące długości czasu stosowania uwierzytelnień, odpowiedzi udzieliło 93% osób. Przeciętnie czas ten wynosił 4,90 lat i wahał się między 0 a 21 lat. Odchylenie standardowe dla tego pytania wyniosło 4,68.

Charakterystykę przebadanych pracowników sektora MSP przedstawiono na wykresie 2.2.



Wykres 2.2. Charakterystyka respondentów

Źródło: opracowanie własne.

2.2.2. Charakterystyka jakościowa próby badawczej

Podmiotami badań byli pracownicy małych i średnich przedsiębiorstw korzystający w pracy z urządzeń teleinformatycznych, a w szczególności komputera lub urządzenia mobilnego, za pomocą których uzyskiwali dostęp do zasobów systemów informatycznych.

Z uwagi na konieczność zapewnienia anonimowości i wynikający z tego przypadkowy dobór próby badawczej, informacje dotyczące przedsiębiorstw zatrudniających respondentów nie podlegały weryfikacji. Stąd potrzeba uproszczenia kryterium oceny wielkości przedsiębiorstwa tak, by przyporządkowanie miejsca pracy nie sprawiało respondentowi większych trudności. Poza właścicielami bądź osobami zatrudnionymi w sprawozdawczości, przeciętny pracownik nie posiada informacji dotyczącej obrotu netto lub sumy aktywów, natomiast zwykle orientuje się w poziomie zatrudnienia oraz strukturze (np. posiadanie filii). Przyporządkowanie przedsiębiorstwa do grupy małych i średnich przedsiębiorstw oparto na więc deklarowanej wielkości zatrudnienia.

Sposób pozyskania materiału badawczego

Wypełnione kwestionariusze pozyskano z następujących źródeł:

1. Politechnika Lubelska udostępniła dane 550 przedstawicieli firm, do których skierowano kwestionariusz badawczy. Uzyskano zwrot 160 ankiet, z których odrzucono 29 z uwagi na połowiczne wypełnienie lub nie wypełnienie metryczki dotyczącej miejsca zatrudnienia.
2. Kolejną grupę respondentów pozyskano podczas targów ENERGETIX 2015, które miały miejsce w Lublinie, w dniach 17–19 listopada 2015 roku. Z ok. 130 przedsiębiorstw wybrano małe i średnie przedsiębiorstwa. Zwrot z tej grupy wyniósł 39 ankiet.
3. 42 ankiety pozyskano od pracowników małych i średnich przedsiębiorstw metodą kuli śnieżnej.

3. Stosowanie tożsamości cyfrowych w małych i średnich przedsiębiorstwach

3.1. Organizacja dostępu do zasobów systemów informatycznych

Pierwsza część badań dotyczyła rozwiązań stosowanych w przedsiębiorstwach respondentów.

3.2. Wdrożenie polityki bezpieczeństwa

Punktem wyjścia było określenie w ilu przedsiębiorstwach stosowana była polityka bezpieczeństwa. Na 198 udzielonych odpowiedzi (98% respondentów), politykę bezpieczeństwa posiadały przedsiębiorstwa 60% respondentów, kolejnych 6% zamierzało wprowadzić ją w najbliższym czasie. Oznacza to, że pozostali respondenci deklarowali brak polityki bezpieczeństwa w swoich przedsiębiorstwach (19% z nich) lub jej nie znali (15% badanych) (por. tabela 3.1.).

Tabela 3.1. Odpowiedź na pytanie: Czy w Pana(i) zakładzie pracy wdrożona jest polityka bezpieczeństwa?

	Liczba odpowiedzi (L)	**Udział odpowiedzi (%)**
Tak	118	60%
Jest w przygotowaniu	12	6%
Nie wiem	30	15%
Nie	38	19%

Źródło: opracowanie własne.

3.3. Rodzaje kont używane przez respondentów

Najpopularniejszym rozwiązaniem stosowanym przez respondentów były konta indywidualne, czyli przypisane konkretnemu pracownikowi. Takie rozwiązanie zadeklarowało prawie 79% respondentów. Z kont, do których dostęp posiada więcej niż jedna osoba, korzystało prawie 21%, a otwarty dostęp do zasobów wskazało około 12% badanych (tabela 3.2.).

Tabela 3.2. Analiza odpowiedzi na pytanie: W jaki sposób uzyskuje Pan(i) dostęp do zasobów systemów informatycznych w pracy? (wybór wielokrotny)

Odpowiedź	Liczba odpowiedzi (L)	Procentowy udział odpowiedzi (L%)	Odchylenie standardowe (SD)
Mam przydzielony indywidualny dostęp (np. z indywidualnym loginem i hasłem)	159	78,7%	0,389
Dzielę moje konto pracownicze z innymi współpracownikami (np. mamy jeden login i hasło)	42	20,8%	0,412
Mam otwarty dostęp do zasobów (np. nie korzystamy z haseł i loginów)	25	12,4%	0,335

Źródło: opracowanie własne.

3.4. Narzędzia uwierzytelnienia dostępu

Hasła lub numery PIN były wykorzystywane przez prawie 96% z tych respondentów, jako narzędzie ochrony dostępu do zasobów przedsiębiorstwa. Ponad 41% respondentów w sumie, zadeklarowało wykorzystanie następujących przedmiotów: kart elektronicznych (31% respondentów, w tym: 13% – kart zabezpieczonych numerem PIN i 24% – kart bez zabezpieczeń), tokenów (16% respondentów, w tym: 10% – tokenów sprzętowych bez zabezpieczeń, 7% – aplikacji na telefon komórkowy, 3% – tokenów sprzętowych zabezpieczonych numerem PIN), kryptograficznych nośników USB (10%) i kart kodów jednorazowych (7%). Symbol odblokowania, czyli wzór rysowany palcem po ekranie w celu uzyskania dostępu do urządzenia, wskazało13%, a wykorzystanie czytnika linii papilarnych – 7% respondentów.

Prawie 98% respondentów odpowiedziało na pytanie dotyczące częstotliwości korzystania z uwierzytelnienia podczas przeciętnego dnia pracy. Badani potwierdzali hasłem lub numerem PIN swoje uprawnienia dostępu od 1 do 60 razy (średnio 6,1 razy dziennie). Respondenci uwierzytelniający się z wykorzystaniem przedmiotów, rzadziej przeprowadzali tę operację (2,8 razy dziennie, a w tym: posiadacze kart – 2,9 razy dziennie, nośników USB – 2,2 razy dziennie, tokenów – 3,3 razy dziennie oraz karty kodów jednorazowych – 2,0 razy dziennie). Z kolei osoby wykorzystujące odcisk palca lub symbol odblokowania uwierzytelniały się przy pomocy tych metod częściej: 10,9 razy dziennie poprzez odcisk palca i 8,6 razy dziennie za pomocą symbolu odblokowania (por. tabela 3.3.).

Tabela 3.3. Analiza odpowiedzi na pytanie: Ile razy w ciągu przeciętnego dnia pracy musi Pan(i) korzystać z uwierzytelnienia, czyli potwierdzać uprawnienia dostępu np. przez wpisanie hasła?

Odpowiedź	Liczba odp. (L)	Procentowy udział odp. (L%)	Średnia (M)	Wartość max.	Odchylenie standardowe (SD)
Login i hasło / PIN	190	96%	6,1	60	8,63
Karta elektroniczna	47	24%	3,2	10	2,76
Karta elektroniczna + PIN	25	13%	2,3	7	1,50
Nośnik kryptograficzny USB	20	10%	2,2	10	2,78
Token generujący hasła jednorazowe	19	10%	3,0	15	3,67
Token generujący hasła jednorazowe + PIN	6	3%	5,3	20	7,39
Token – aplikacja na komórkę	13	7%	2,8	10	2,73
Karta kodów jednorazowych	14	7%	2,0	4	1,04
Czytnik linii papilarnych	14	7%	10,9	50	15,10
Wzór rysowany palcem po ekranie (symbol odblokowania)	25	13%	8,6	30	9,10
Inne: sieć VPN	1	1%	2,0	2	-

Źródło: opracowanie własne.

3.5. Działania użytkownika w kontekście bezpieczeństwa tożsamości cyfrowej

3.5.1. Wykorzystanie hasła jako narzędzia uwierzytelnienia

3.5.1.1. Rozwiązania systemowe

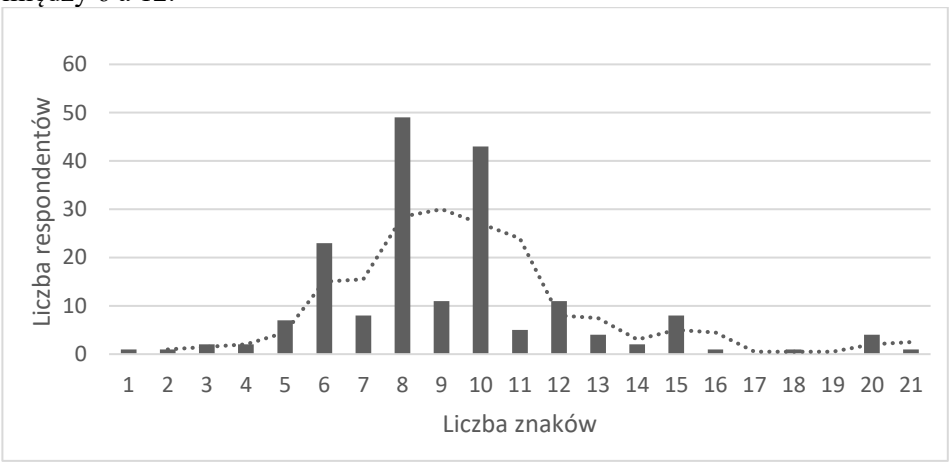
91% respondentów udzieliło odpowiedzi na pytanie wielokrotnego wyboru, dotyczące decyzji o użyciu hasła w celu zabezpieczenia dostępu do zasobów. Wśród nich, 31% respondentów samodzielnie o tym decydowało. W pozostałych przypadkach osobą decyzyjną był przełożony (24%) lub korzystanie z tej metody zabezpieczeń było regulowane przepisami wewnętrznymi (49%).

95% respondentów spośród 186 (92% wszystkich respondentów), którzy udzielili odpowiedzi na to pytanie deklaruje, że podczas wprowadzania hasła, wprowadzane znaki nie są widoczne na ekranie komputera.

20% spośród 186 badanych, którzy udzielili odpowiedzi na to pytanie, deklaruje, że w ich zakładzie pracy zaimplementowane są rozwiązania automatycznie blokujące dostęp do zasobów po określonym czasie braku aktywności użytkownika. Z kolei 23% respondentów opuszczając swoje stanowisko pracy na dłuższy czas nie wylogowuje się z systemu. Aktywną ochronę dostępu poprzez intencjonalne wylogowanie się deklaruje z kolei 57% respondentów.

3.5.1.2. Budowa hasła

91% respondentów podało średnią długość stosowanych haseł. Wśród nich najwięcej, bo 65% deklaruje stosowanie haseł z przedziału <8,13> znaków, natomiast dłuższych haseł – 9% (por. wykres 3.1.). Stąd, hasła zdecydowanie zbyt krótkie, czyli o średniej długości do 7 znaków włącznie wskazało 24% respondentów. Średnia długość hasła badanej grupy wyniosła 9,17 znaków, mediana natomiast 8. Co ciekawe parzystą liczbę znaków deklaruje 137 (74%), a nieparzystą 47 respondentów (26%). Zjawisko to jest zauważalne przy liczbie znaków między 6 a 12.



Wykres 3.1. Średnia długość haseł deklarowana przez respondentów

Źródło: opracowanie własne.

Prawie 70% respondentów odpowiedziało na pytanie dotyczące deklarowanego składu haseł. 41% z nich buduje swoje hasła ze wszystkich typów znaków, prawie 25% z trzech typów znaków: małych i dużych liter oraz cyfr, 17% z małych liter i cyfr, prawie 8% z samych małych liter, 3% stosuje inną kombinację znaków. Najpopularniejsze znaki wykorzystywane w hasłach to małe litery i cyfry. Znajdują się one w średnio 91% haseł (tabela 3.4.).

Tabela 3.4. Deklarowane przez respondentów znaki wchodzące zwykle w skład ich haseł

	Liczba odpowiedzi (L)	**Udział odpowiedzi (%)**
Małe litery	129	91%
Duże litery	96	68%
Cyfry	128	91%
Znaki specjalne	61	43%

Źródło: opracowanie własne.

Ok. 14% ze 180 respondentów, którzy odpowiedzieli na pytanie deklaruje, że w swoich hasłach używa ważnych dla siebie dat, imion lub prostych ciągów znaków (np. qwerty lub 12345).

3.5.1.3. Dostęp do hasła

Większość (71%) ze 188 osób, które odpowiedziały na pytanie wielokrotnego wyboru, dotyczące sposobu przechowywania haseł, polega tylko na swojej pamięci. 27% respondentów zapisuje hasła w formie elektronicznej (10% w postaci zaszyfrowanej, 7% w postaci zwykłego pliku) lub na papierze (9% w prywatnym notatniku, 3% na dokumencie zdeponowanym w sejfie oraz 4% na kartce położonej w wygodnym miejscu np. pod klawiaturą komputera). 4% wykorzystuje programy przechowujące hasła (rozwiązania typu SSO, wirtualny dysk, zdeponowane na urządzeniu mobilnym).

Większość respondentów (58%) udostępniła swoje hasło innym (tabela 3.5.). Ze 186 osób (92% badanych), które odpowiedziały na to pytanie wielokrotnego wyboru, 37% udostępnia niektóre ze swoich haseł osobom, z którymi pracuje. Respondenci ujawniają też swoje hasło osobom ze wsparcia technicznego (19%) lub członkowi rodziny (10%).

Tabela 3.5. Wskazanie przez respondentów osób, które mają dostęp do niektórych z ich haseł

	Liczba odpowiedzi (L)	**Udział odpowiedzi (%)**
Zaufani współpracownicy	47	23%
Przełożony	39	19%
Członek rodziny	21	10%
Osoby ze wsparcia technicznego	38	19%
Nikt	79	42%

Źródło: opracowanie własne.

3.5.1.4. Użytkowanie hasła

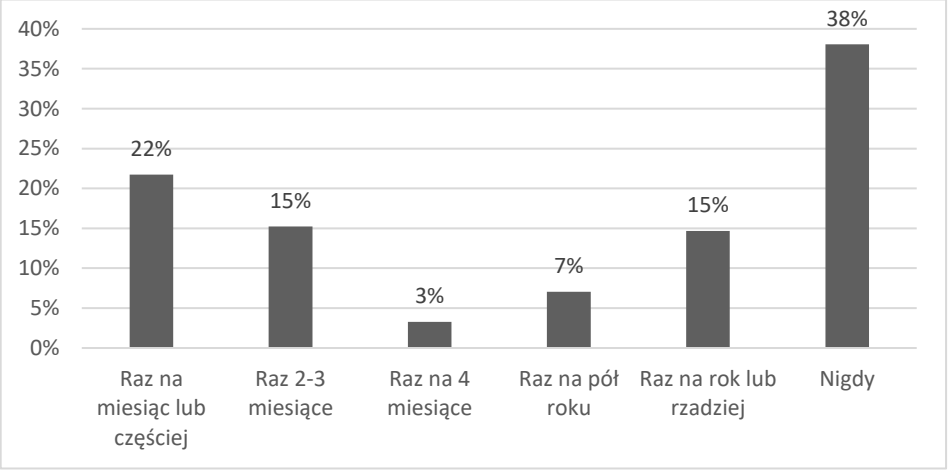
Na pytanie dotyczące zmiany haseł zgodnie z zasadami, udzieliło odpowiedzi 175 (87%) respondentów. Aż 42% z nich nie ma żadnych zaleceń dotyczących zmiany hasła, a 5% zmienia hasła w sposób inny niż zalecany (tabela 3.6.).

Tabela 3.6. Odpowiedzi respondentów na pytanie dotyczące sposobu zmiany haseł

	Liczba odpowiedzi (L)	**Udział odpowiedzi (%)**
Generalnie zmieniam hasła: zgodnie z zaleceniami	93	53%
w sposób inny niż zalecany	8	5%
nie mam żadnych zaleceń	74	42%

Źródło: opracowanie własne.

Ok. 91% badanych (184 osoby) udzieliło odpowiedzi na pytanie dotyczące częstotliwości zmiany haseł. 70 osób (38% respondentów, którzy udzielili odpowiedzi) zadeklarowało, że nigdy nie zmienia haseł. Pozostali respondenci zmieniali hasła średnio 5,97 razy na rok (por. wykres 3.2.). Odchylenie standardowe dla tego pytania wyniosło 4,90.



Wykres 3.2. Częstotliwość zmian haseł przez respondentów

Źródło: opracowanie własne.

Ze 189 respondentów (94% badanych), którzy odpowiedzieli na to pytanie, 54% przyznaje, że używa tego samego hasła do różnych aplikacji.

3.5.1.5. Obsługa zdarzeń

Na pytania dotyczące typowych sytuacji związanych z wykorzystaniem hasła, odpowiedzi udzieliło średnio 94% respondentów. 52% z nich zdarzyło się zapomnieć hasła dostępu, a 14% ujawniło swoje hasło osobie postronnej. Znamienne jest to, że w 9% posłużyło ono osobie postronnej do uzyskania dostępu do zasobów, do których nie miała prawa (tabela 3.7.).

Tabela 3.7. Sytuacje, z którymi mieli do czynienia respondenci, związane z korzystaniem z haseł

	Liczba odpowiedzi (L)	**Udział odpowiedzi (%)**
Zapomnienie hasła	98	52%
Ujawnienie hasła osobie postronnej	27	14%
Wykorzystanie hasła respondenta przez osobę postronną	16	9%

Źródło: opracowanie własne.

Na pytanie wielokrotnego wyboru dotyczące działań, które zostały podjęte w przypadku podejrzenia, że osoba postronna poznała hasło respondenta, odpowiedzi udzieliło 92% badanych. Większość z nich (56%) deklaruje, że sytuacja taka nie miała miejsca. Pozostali respondenci zmieniali hasło (34%), powiadamiali przełożonego (10%) lub nie podejmowali żadnych działań (3%) (tabela 3.8.).

Tabela 3.8. Działania podjęte przez respondentów w przypadku podejrzenia, że hasło zostało podejrzane przez osobę nieuprawnioną

	Liczba odpowiedzi (L)	**Udział odpowiedzi (%)**
Powiadomienie przełożonego	19	10%
Zmiana hasła	64	34%
Brak działań	6	3%
Nie było takiej sytuacji	105	56%

Źródło: opracowanie własne.

3.5.2. Wykorzystanie przedmiotu jako narzędzia uwierzytelnienia

Na pytanie dotyczące udostępniania innym swojego narzędzia uwierzytelnienia odpowiedziało 81 osób, co stanowi 96% respondentów deklarujących wykorzystanie przynajmniej jednego przedmiotu służącego uwierzytelnieniu. 43% osób z tej grupy nie udostępnia nikomu swoich narzędzi uwierzytelnienia. Pozostali respondenci udostępniają je osobom, z którymi pracują (40%, a w tym: zaufanym współpracownikom – 27% i przełożonym – 16%), członkom rodziny (14%) oraz pracownikom wsparcia technicznego (13%) (por. tabela 3.9.).

Tabela 3.9. Wskazanie przez respondentów osób, które mają dostęp do ich przedmiotów uwierzytelniających

	Liczba odpowiedzi (L)	**Udział odpowiedzi (%)**
Zaufani współpracownicy	22	27%
Przełożony	13	16%
Członek rodziny	11	14%
Osoby ze wsparcia technicznego	10	13%
Nikt	35	43%

Źródło: opracowanie własne.

Na pytanie dotyczące przestrzegania zasad związanych z przechowywaniem przedmiotu uwierzytelniającego, odpowiedzi udzieliło 80 osób (95% respondentów korzystających z przedmiotów uwierzytelniających). Generalnie, przestrzeganie zaleceń deklaruje 76% z nich (w tym 65% – przestrzegane, 11% – częścio-

wo przestrzegane), natomiast 26% nie zna zaleceń (por. tabela 3.10.), z czego 18% respondentów utrzymuje, że takie zalecenia nie zostały im przekazane.

Tabela 3.10. Odpowiedzi respondentów na pytanie o przestrzeganie zaleceń dotyczących przechowywania przedmiotów uwierzytelniających

	Liczba odpowiedzi (L)	**Udział odpowiedzi (%)**
Przestrzegane	52	65%
Częściowo przestrzegane	9	11%
Nieprzestrzegane	0	0%
Nie pamiętam zaleceń	6	8%
Nie było takich zaleceń	14	18%

Źródło: opracowanie własne.

Spośród 78 osób, które odpowiedziały na to pytanie (93% respondentów korzystających z przynajmniej jednego przedmiotu uwierzytelniającego), 72 (92%) deklaruje, że nigdy nie zgubiło powierzonego urządzenia. Z 77 osób (92% respondentów korzystających z przynajmniej jednego przedmiotu uwierzytelniającego), 73 (95%) deklaruje, że powierzony przedmiot uwierzytelniający nigdy nie został użyty do uzyskania dostępu do danych przez nieuprawnione osoby.

Na pytanie o działanie w przypadku podejrzenia, że przedmiot mógł trafić w niepowołane ręce odpowiedzi udzieliło 74 respondentów, co stanowi 88% osób korzystających z uwierzytelnienia za pomocą przedmiotu. Wśród nich, 74% deklaruje, że taka sytuacja nie miała miejsca, 18% osób powiadomiło swojego przełożonego, a 8% nie podjęło żadnych działań (tabela 3.11.).

Tabela 3.11. Działania podjęte przez respondentów w przypadku podejrzenia, że przedmiot uwierzytelniający został przejęty przez osobę nieuprawnioną

	Liczba odpowiedzi (L)	**Udział odpowiedzi (%)**
Powiadomienie przełożonego	13	18%
Brak działań	6	8%
Nie było takiej sytuacji	55	74%

Źródło: opracowanie własne.

3.6. Preferencje pracowników i ocena stosowanych rozwiązań

3.6.1. Zarządzanie w obszarze kształtowania postaw – perspektywa pracownika

Respondenci zostali poproszeni o określenie, w jakim stopniu działania przełożonych mają znaczenie w motywowaniu do bezpiecznego korzystania z dostępu

do danych, poprzez przypisanie im wagi w punktach od 1 (nieważne) do 5 (bardzo ważne). Odpowiedzi udzieliło średnio 195 respondentów (96%). Rozkład odpowiedzi został przedstawiony w tabeli 3.12., a prosta analiza w tabeli 3.13.

Tabela 3.12. Rozkład odpowiedzi respondentów na pytanie: Proszę ocenić w skali 1 (nieważne) – 5 (bardzo ważne), na ile poniższe działania mają według Pana(i) znaczenie w motywowaniu do bezpiecznego korzystania z dostępu do danych.

	Liczba przypisanych ocen (L) i udział procentowy w ramach działania (%)									
	1		**2**		**3**		**4**		**5**	
	L	**%**	**L**	**%**	**L**	**%**	**L**	**%**	**L**	**%**
Zapewnienie wsparcia technicznego i merytorycznego	**13**	*6%*	**21**	*10%*	**42**	*21%*	**41**	*20%*	**84**	*42%*
Szkolenie dot. zasad bezpiecznego korzystania z systemów informatycznych podczas wdrażania do pracy	**19**	*10%*	**25**	*13%*	**33**	*17%*	**64**	*33%*	**55**	*28%*
Szkolenia cykliczne (utrwalające) dot. zasad bezpiecznego korzystania z systemów informatycznych	**34**	*18%*	**30**	*16%*	**55**	*29%*	**35**	*18%*	**37**	*19%*
Konsultacje dotyczące zasad i narzędzi uwierzytelniania	**22**	*11%*	**31**	*16%*	**57**	*29%*	**45**	*23%*	**42**	*21%*
Wyznaczanie i komunikowanie zasad dot. bezpiecznego korzystania z systemów informatycznych	**12**	*6%*	**29**	*15%*	**45**	*23%*	**56**	*29%*	**52**	*27%*
Ocena pracy pracownika w aspekcie bezpiecznego użytkowania systemów informatycznych	**34**	*18%*	**31**	*16%*	**52**	*27%*	**47**	*24%*	**27**	*14%*
Bieżąca kontrola i reagowanie na nieprzestrzeganie zasad	**18**	*9%*	**25**	*13%*	**37**	*19%*	**66**	*34%*	**47**	*24%*
Motywacja finansowa	**27**	*14%*	**14**	*7%*	**36**	*19%*	**28**	*15%*	**88**	*46%*

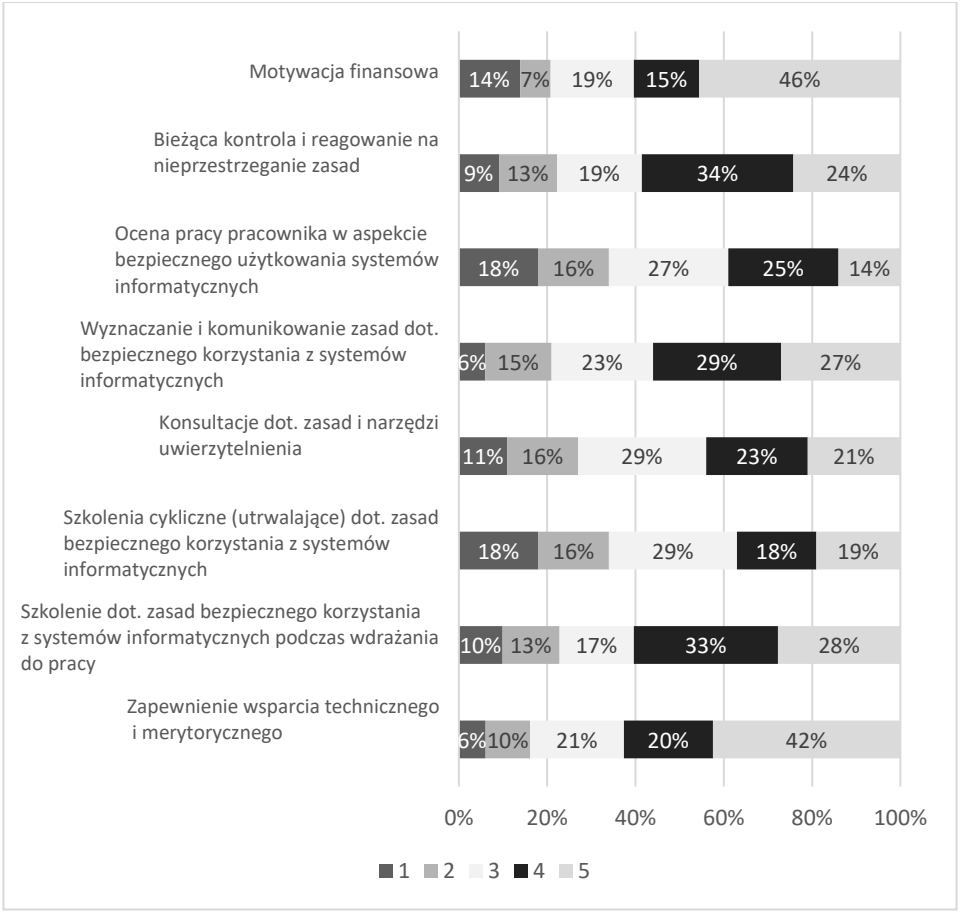
Źródło: opracowanie własne.

Tabela 3.13. Analiza odpowiedzi respondentów na pytanie: Proszę ocenić w skali 1 (nieważne) – 5 (bardzo ważne), na ile poniższe działania mają według Pana(i) znaczenie w motywowaniu do bezpiecznego korzystania z dostępu do danych.

	Średnia	**Mediana**	**Odchylenie standardowe (SD)**
Zapewnienie wsparcia technicznego i merytorycznego	3,81	4	1,26
Szkolenie dot. zasad bezpiecznego korzystania z systemów informatycznych podczas wdrażania do pracy	3,57	4	1,29
Szkolenia cykliczne (utrwalające) dot. zasad bezpiecznego korzystania z systemów informatycznych	3,06	3	1,35
Konsultacje dotyczące zasad i narzędzi uwierzytelniania	3,27	3	1,27
Wyznaczanie i komunikowanie zasad dot. bezpiecznego korzystania z systemów informatycznych	3,55	4	1,23
Ocena pracy pracownika w aspekcie bezpiecznego użytkowania systemów informatycznych	3,01	3	1,32
Bieżąca kontrola i reagowanie na nieprzestrzeganie zasad	3,51	4	1,27
Motywacja finansowa	3,70	4	1,45

Źródło: opracowanie własne.

Z analizy wynika, że największe znaczenie dla respondentów w kwestii działań zwiększających motywację do bezpiecznego stosowania uwierzytelnień mają: zapewnienie wsparcia technicznego i merytorycznego (średnia ocena 3,81) oraz motywacja finansowa (średnia ocen 3,70), które też ma największy odsetek odpowiedzi „*bardzo ważne*" (por. wykres 3.3.). Wymienione działania zostały ocenione przez ponad 61% respondentów jako ważne (4) lub bardzo ważne (5).



Wykres 3.3. Rozkład ocen działań motywujących do bezpiecznego stosowania uwierzytelnienia w skali od 1 (nieważne) do 5 (bardzo ważne)

Źródło: opracowanie własne.

3.6.2. Ocena obecnie stosowanych rozwiązań – łatwość użytkowania

Zbadano, jak respondenci postrzegają łatwość użycia poszczególnych narzędzi wykorzystywanych do uzyskania dostępu do zasobów. Na to pytanie odpowiedzi udzieliło średnio 85% respondentów.

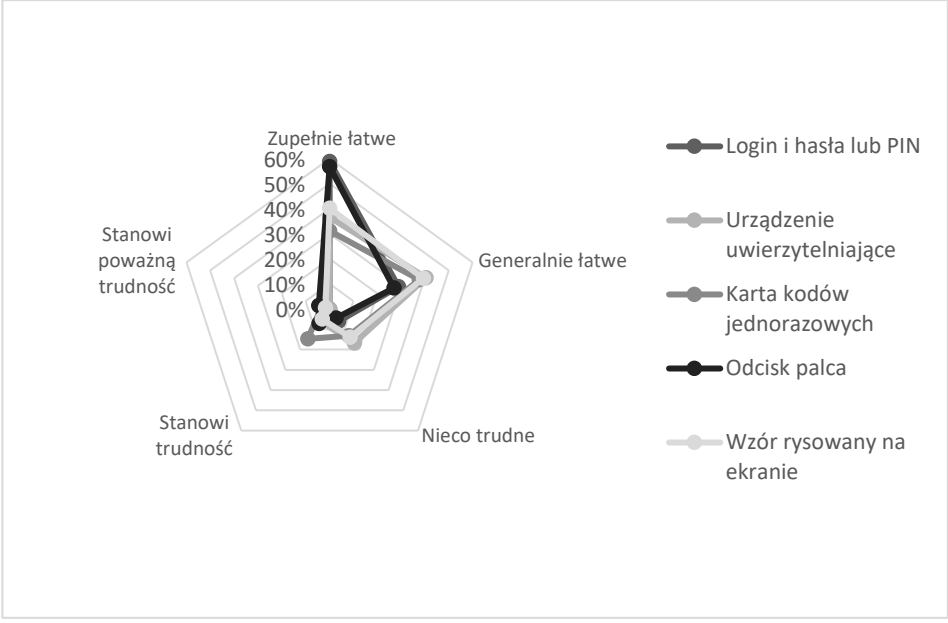
Wśród nich, doświadczenie w korzystaniu z poszczególnych narzędzi deklarowało: 100% respondentów w przypadku haseł i numerów PIN, 78% – urządzeń uwierzytelniających, 74% – karty kodów jednorazowych, 68% – odcisku palca oraz 76% dla wzorów rysowanych na ekranie. Wyniki badania zaprezentowano w tabeli 3.14. oraz na wykresach 3.4. i 3.5.

Za najłatwiejsze w użyciu (ponad 80% ocen *zupełnie łatwe* lub *generalnie łatwe*) badane osoby uznały: hasła i numery PIN (88%), odcisk palca (84%) i wzór rysowany na ekranie (80% odpowiedzi). Wykorzystanie przedmiotów było oceniane jako relatywnie trudniejsze (77% – urządzenie uwierzytelniające, 69% – karta kodów jednorazowych).

Tabela 3.14. Ocena łatwości użycia poszczególnych narzędzi przez respondentów

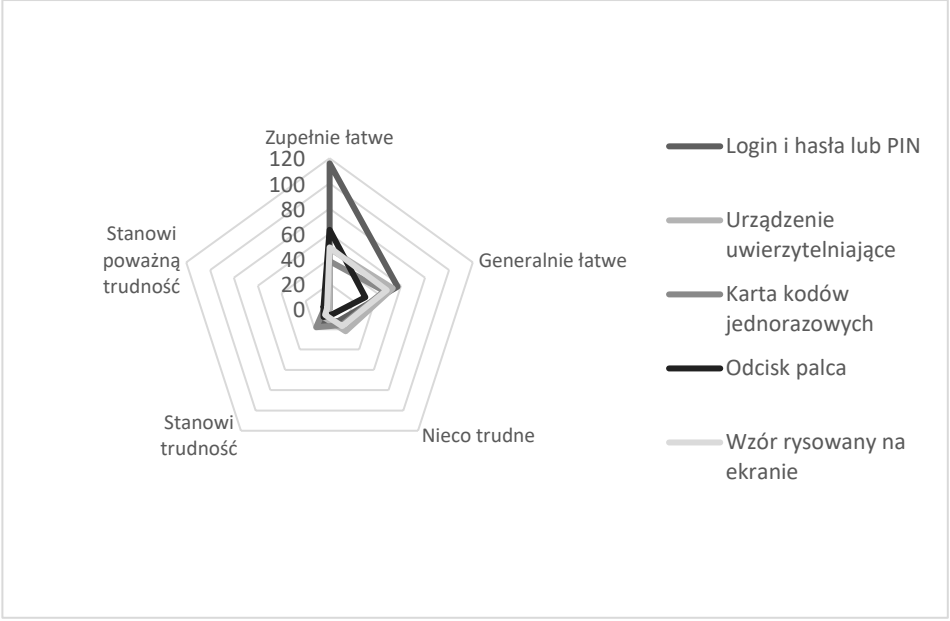
	Liczba odpowiedzi (L)				
	Zupełnie łatwe	**Generalnie łatwe**	**Nieco trudne**	**Stanowi trudność**	**Stanowi poważną trudność**
Login i hasła lub PIN	116	57	12	12	0
Urządzenie uwierzytelniające	48	53	22	8	0
Karta kodów jednorazowych	38	46	16	18	4
Odcisk palca	63	30	5	8	5
Wzór rysowany na ekranie	49	48	17	6	2

Źródło: opracowanie własne.



Wykres 3.4. Ocena łatwości użycia poszczególnych narzędzi przez respondentów (procentowy rozkład odpowiedzi)

Źródło: opracowanie własne.



Wykres 3.5. Ocena łatwości użycia poszczególnych narzędzi przez respondentów (rozkład odpowiedzi)

Źródło: opracowanie własne.

Porównując oceny łatwości użycia, widoczne są dwa wzory rozkładów odpowiedzi (figury zbliżone do jednokładnych na wykresie 3.4. i 3.5.), które dzielą narzędzia na dwie grupy:

1. Loginy i hasła lub numery PIN oraz odcisk palca.
2. Urządzenia uwierzytelniające, karty kodów jednorazowych oraz wzór rysowany na ekranie.

3.6.3. Racjonalizowanie zasad dotyczących uwierzytelnienia – perspektywa użytkownika

Respondenci zostali poproszeni o określenie, w oparciu o swoje doświadczenie i znajomość specyfiki zakładu pracy, jakie powinny być zasady uwierzytelnienia, które zapewniłyby zarówno bezpieczeństwo danych, jak i wygodę pracowników.

Najczęściej wybieraną metodą były loginy i hasła, które zostały wskazane jako główna, preferowana metoda uwierzytelnienia przez 163 ze 196 (97%) respondentów, którzy udzielili odpowiedzi na to pytanie. Na kolejnych miejscach znalazły się: uwierzytelnienie z wykorzystaniem przedmiotu, symbolu odblokowania oraz cech biometrycznych, wśród których wymieniono odcisk palca i skan tęczówki (tabela 3.15.).

Tabela 3.15. Preferowane główne narzędzie uwierzytelnienia

	Liczba odpowiedzi (L)	Procent odpowiedzi (%)
Login	163	83,2%
Symbol odblokowania	8	4,1%
Przedmiot niezabezpieczony hasłem	9	4,6%
Przedmiot zabezpieczony hasłem	9	4,6%
Cecha biometryczna	7	3,6%

Źródło: opracowanie własne.

Na pytanie dotyczące szacunkowej, racjonalnie umotywowanej liczby różnych narzędzi uwierzytelnienia, odpowiedzi udzieliło 159, czyli prawie 79% respondentów. 93% z nich wybrało do ochrony zasobów hasła, 49% przedmioty, natomiast 25% cechy biometryczne. Najczęściej wybierana liczba różnych haseł wyniosła 3, natomiast przedmiotów lub cech biometrycznych 1 (tabela 3.16.).

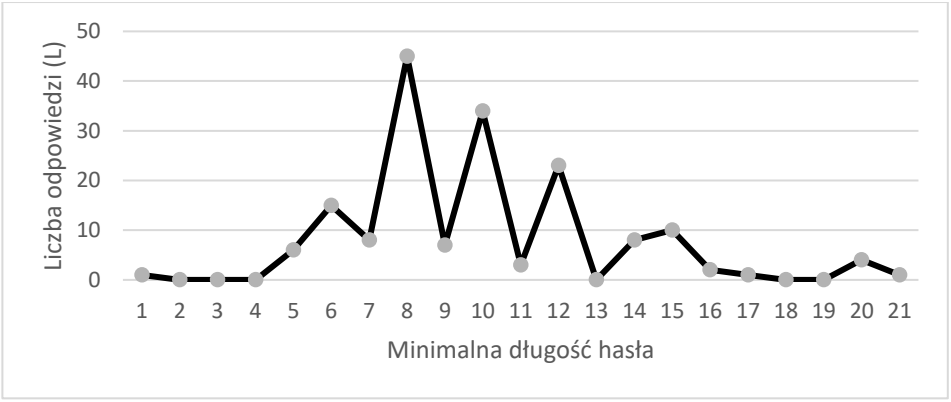
Tabela 3.16. Preferowana szacunkowa liczba narzędzi uwierzytelnienia

	Liczba odpowiedzi (L)	Procent odpowiedzi (%)	Wartość średnia (M)	Mediana (Me)	Odchylenie standardowe (SD)
Hasła	148	93%	4,01	3	5,18
Przedmioty	78	49%	2,48	1	3,58
Cechy biometryczne	40	25%	1,40	1	0,72

Źródło: opracowanie własne.

Respondenci zostali poproszeni o określenie zasad, które ustaliliby w kwestii stosowania haseł, zakładając, że byłyby on używane do zabezpieczenia zasobów w ich przedsiębiorstwie. Na to pytanie odpowiedzi udzieliły 194 osoby (96% respondentów).

88% z nich określiłaby minimalną długość hasła, która wahała się między 1 a 21 znaków (przeciętnie 9,9). Najczęściej wybieraną odpowiedzią było 8 (wykres 3.6., tabela 3.17.).



Wykres 3.6. Preferowane zasady dotyczące haseł – minimalna długość

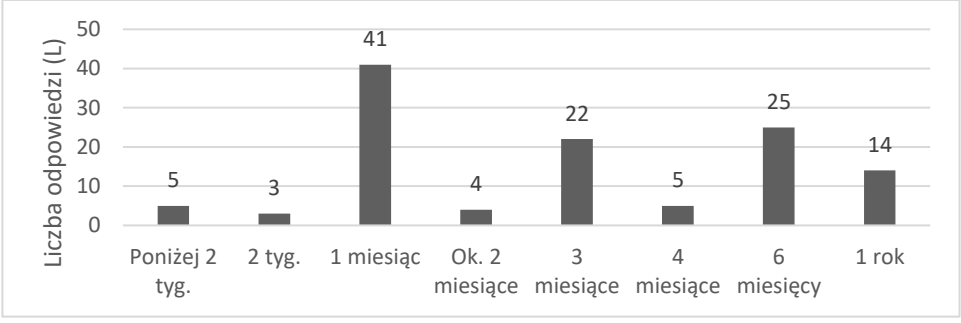
Źródło: opracowanie własne.

61% respondentów określiłaby maksymalną ważność hasła (tj. czas, po którym hasło powinno być zmienione), która wahała się między 7 a 365 dni (przeciętnie 116 dni). Najczęściej wybieraną odpowiedzią było 30 dni (tabela 5.17., wykres 3.7.).

Tabela 3.17. Preferowane zasady dotyczące haseł – minimalna długość i maksymalna ważność hasła

	Liczba odpowiedzi (L)	**Procent odpowiedzi (%)**	**Wartość**			**Mediana (Me)**	**Odchylenie standardowe (SD)**
			Min.	**Max.**	**Średnia (M)**		
Długość hasła *(liczba znaków)*	171	88%	1	21	9,9	10	4,64
Ważność hasła *(liczba dni)*	119	61%	7	365	116,17	90	101,61

Źródło: opracowanie własne.



Wykres 3.7. Preferowane zasady dotyczące haseł – maksymalna ważność hasła

Źródło: opracowanie własne.

Wyniki ankiety pokazują, że 175 respondentów ma następujące preferencje dotyczące haseł, tj. określenie jakie znaki muszą wchodzić w skład hasła (litery małe/duże, cyfry, znaki specjalne) oraz jakie łańcuchy znaków nie powinny być stosowane jako hasła (ważne daty, imiona, proste słowa czy sekwencje np. 1234). Najczęstszym wymaganiem byłoby zawarcie w haśle minimum jednej cyfry, najrzadszym natomiast zakaz stosowania ryzykownych sekwencji (tabela 3.18.).

Tabela 3.18. Preferowane zasady dotyczące haseł – skład

		Liczba odpowiedzi (L)	**Procent odpowiedzi (%)**
Minimalnie 1 znak	mała i duża litera	127	73%
	cyfra	151	86%
	znak specjalny	84	48%
Zakaz stosowania ważnych dat, imion, prostych słów czy sekwencji (np. 1234)		79	45%

Źródło: opracowanie własne.

Większość (40%) respondentów ustawiłaby dwa minimalne wymagania co do znaków wchodzących w skład hasła (np. minimum 1 cyfra i 1 znak specjalny), 36% badanych wymagałoby stosowania w hasłach zarówno małych i dużych liter, jak i cyfr oraz znaków specjalnych. Pozostali (24%) wprowadziliby zasadę stosowania w hasłach przynajmniej jednej z wymienionych zasad (tj. 1 mała i 1 duża litera; 1 cyfra lub 1 znak specjalny).

31% z tych respondentów, którzy odpowiedzieli na pytanie dotyczące wymagań co do haseł, wprowadziłoby zakaz powtarzania haseł dla różnych aplikacji.

3.6.4. Porównanie obecnie stosowanych rozwiązań z preferencjami respondentów

Respondenci najlepiej ocenili metody oparte na wiedzy. Loginy i hasła lub numery PIN są rozwiązaniem najchętniej wybieranym jako główne narzędzie zabezpieczenia przez osoby, które mają z nimi doświadczenie. Podobnie respondenci oceniają wzór rysowany na ekranie czyli symbol odblokowania (tabela 3.19. i tabela 3.20.).

Na drugim biegunie znajdują się przedmioty uwierzytelniające. Mimo dość dużego doświadczenia w korzystaniu z urządzeń zabezpieczonych, jak i niezabezpieczonych numerem PIN, odpowiednio 91% i 80% respondentów wybrałoby inne rozwiązanie na główne narzędzie uwierzytelniające. Respondenci są natomiast podzieleni w kwestii postrzegania cech biometrycznych jako głównego narzędzia uwierzytelnienia.

Tabela 3.19. Rozkład odpowiedzi dotyczących preferowanych narzędzi uwierzytelniania w kontekście obecnie stosowanych rozwiązań

Wybór narzędzia stosowanego do tej pory	Wybór respondenta (preferowane narzędzie)				
	Login i hasło lub numer PIN	Symbol odblokowania	Przedmiot bez numeru PIN	Przedmiot z numerem PIN	Cecha biometryczna
Niestosowane obecnie	**4**	**6**	**6**	**7**	**4**
Tak	158	66	2	2	3
Nie	30	2	81	37	11

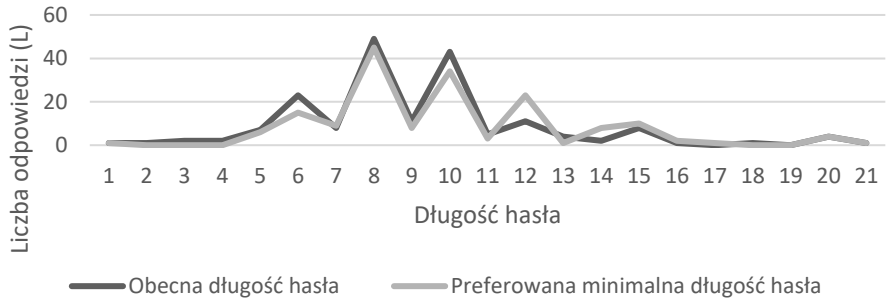
Źródło: opracowanie własne.

Tabela 3.20. Procentowy rozkład odpowiedzi dotyczących preferowanych narzędzi uwierzytelniania w kontekście obecnie stosowanych rozwiązań

Wybór narzędzia stosowanego do tej pory	Wybór respondenta (preferowane narzędzie)				
	Login i hasło lub numer PIN	Symbol odblokowania	Przedmiot bez numeru PIN	Przedmiot z numerem PIN	Cecha biometryczna
Niestosowane obecnie	2%	8%	7%	15%	22%
Tak	82%	89%	2%	4%	17%
Nie	16%	3%	91%	80%	61%

Źródło: opracowanie własne.

Z analizy porównawczej długości obecnie stosowanych i preferowanych haseł (wykres 3.8.) wynika, że istnieje między nimi zależność (współczynnik korelacji r = 0,37). Jednakże respondenci preferują dłuższe hasła od obecnie stosowanych: średnia liczba znaków w haśle stosowanych obecnie wynosi 9,17, natomiast preferowanych 9,87.



Wykres 3.8. Porównanie długości obecnych i preferowanych długości haseł
Źródło: opracowanie własne.

Porównano złożoność obecnie stosowanych haseł z preferowaną liczbą wymagań dotyczącą składu hasła (kategorie wykorzystywanych znaków i niepowtarzalność haseł w innych aplikacjach). W badanej grupie respondentów wykryto zależność między obecnie stosowanymi a preferowanymi rozwiązaniami (współczyn-

nik korelacji r = 0,38), z tym, że respondenci preferują zasady średnio o 29% bardziej restrykcyjne od tych, które charakteryzują ich własne hasła. Średnia liczba wymagań spełnianych przez obecnie stosowane hasła wynosi 1,61, podczas gdy liczba ustalonych przez respondentów wymagań wobec haseł wynosi 2,01.

4. Skwantyfikowany model DIAM

4.1. Postrzegane korzyści z wykorzystania tożsamości cyfrowej

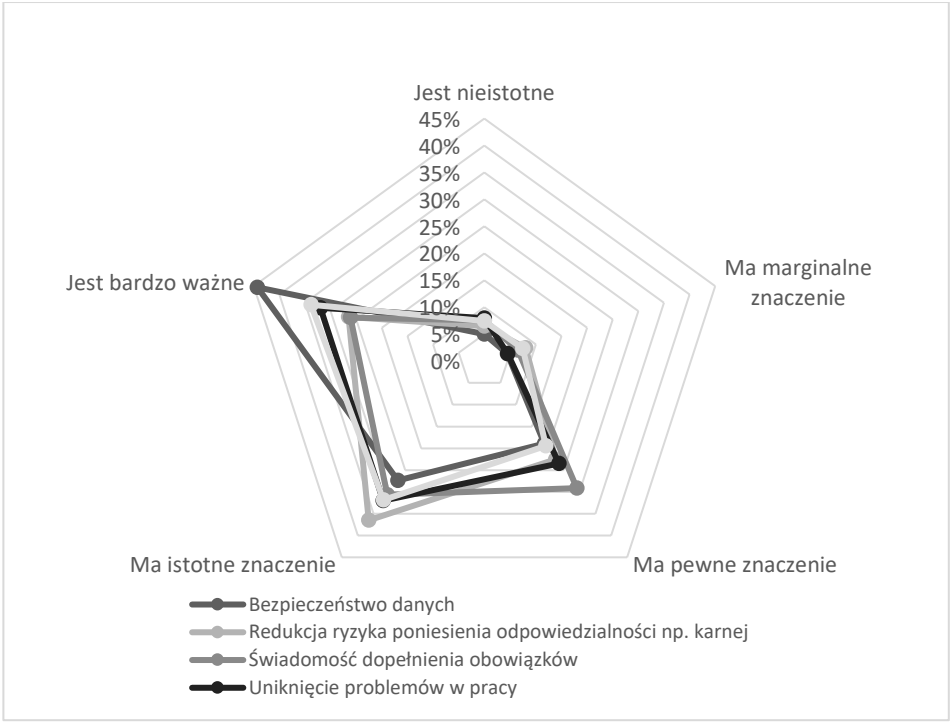
Zbadano, jak respondenci postrzegają korzyści z bezpiecznego korzystania z dostępu do zasobów informatycznych. Metodą delficką wytypowano szereg motywów, którymi mogą kierować się użytkownicy systemów informatycznych i poproszono badane osoby o określenie, na ile mają one dla nich znaczenie. W procesie obróbki danych przypisano im skalę od 1 (jest nieistotne) do 5 (jest bardzo ważne).

Na to pytanie odpowiedzi udzieliło średnio 99% respondentów. Dla badanych najistotniejsze były aspekty związane z bezpieczeństwem danych (średnia ważność 4,01), bezpieczeństwem komunikacji elektronicznej (średnia ważność 3,77) oraz uniknięciem problemów w pracy (średnia ważność 3,76). Mniej istotna była redukcja odpowiedzialności karnej (średnia ważność 3,69) oraz świadomość dopełnienia obowiązków (średnia ważność 3,61). Rozkład odpowiedzi i podstawowe statystyki przedstawiono w tabeli 4.1. oraz na wykresie 4.1.

Tabela 4.1. Odpowiedź respondentów na pytanie: Proszę ocenić na ile ważne są dla Pana(i) korzyści z bezpiecznego korzystania z dostępu do zasobów informatycznych Pana(i) zakładu pracy

	Liczba odpowiedzi (L)					Wartość średnia (M)	Odchylenie standardowe (SD)
	Jest nieistotne	Ma marginalne znaczenie	Ma pewne znaczenie	Ma istotne znaczenie	Jest bardzo ważne		
Bezpieczeństwo danych	10	9	38	55	89	4,01	1,12
Redukcja ryzyka poniesienia odpowiedzialności np. karnej	13	16	45	73	53	3,69	1,14
Świadomość dopełnienia obowiązków	15	13	58	61	52	3,61	1,16
Uniknięcie problemów w pracy	16	9	47	64	64	3,76	1,18
Bezpieczna komunikacja	15	15	39	64	68	3,77	1,21

Źródło: opracowanie własne.



Wykres 4.1. Znaczenie korzyści w bezpiecznego stosowania tożsamości cyfrowych

Źródło: opracowanie własne.

4.2. Postrzegana użyteczność bezpiecznego korzystania z tożsamości cyfrowej

W celu określenia, jak postrzegana jest użyteczność bezpiecznego korzystania z tożsamości cyfrowych, zadano respondentom następujące pytanie:

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)?

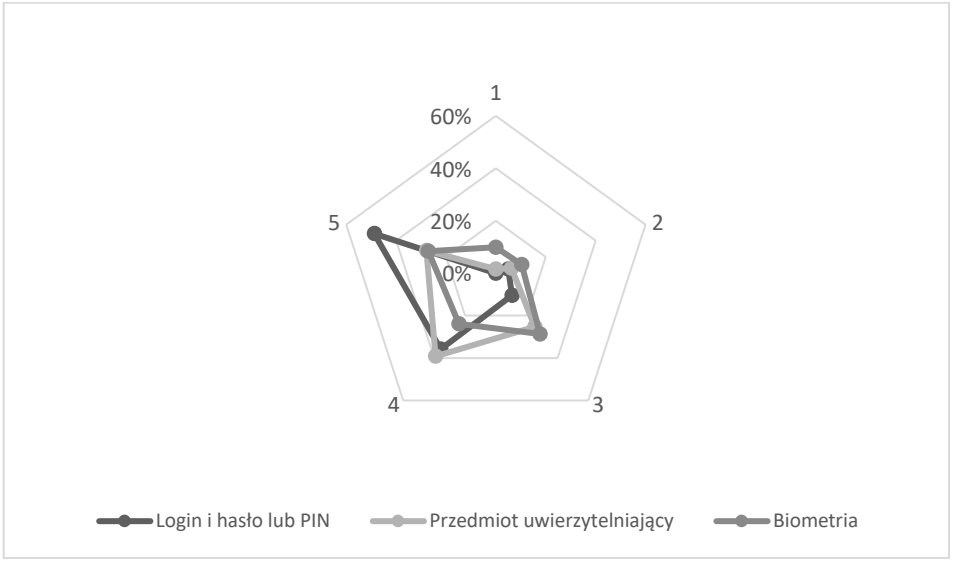
Pojęcie bezpiecznego korzystania z poszczególnych narzędzi uwierzytelnienia, zostało określone w poprzednich pytaniach. Na potrzeby obliczeń skala (-2 do 2) została przeliczona na skalę 1 do 5, gdzie 1 – nieużyteczne, a 5 – bardzo użyteczne.

Według respondentów (tabela 4.2., wykres 4.2.), największą użytecznością charakteryzują się hasła (średnia użyteczność 4,28 przy najmniejszym odchyleniu standardowym 0,85), a najmniejszą biometria (średnia użyteczność 3,48 przy największym odchyleniu standardowym 1,27).

Tabela 4.2. Postrzegana użyteczność bezpiecznego stosowania tożsamości cyfrowej w skali od 1 (nieużyteczne) do 5 (bardzo użyteczne)

	Liczba odpowiedzi (L)					Wartość średnia (M)	Odchylenie standardowe (SD)
	1	2	3	4	5		
Login i hasło lub PIN	0	10	21	72	98	4,28	0,85
Przedmiot uwierzytelniający	3	12	49	76	54	3,86	0,95
Biometria	19	20	55	46	52	3,48	1,27

Źródło: opracowanie własne.



Wykres 4.2. Ocena użyteczności bezpiecznego stosowania tożsamości cyfrowej przez respondentów w skali od 1 (nieużyteczne) do 5 (bardzo użyteczne)

Źródło: opracowanie własne.

4.3. Czynniki zarządcze

Zbadano czy i w jaki sposób respondenci są bezpośrednio motywowani przez przełożonych do bezpiecznego wykorzystania tożsamości cyfrowych. 200 osób, czyli prawie 99% badanych odpowiedziało na to pytanie.

Najwięcej, bo 78% badanych deklaruje, że ma wsparcie techniczne i merytoryczne. Ponadto, 53% respondentów uważa, że zasady dotyczące dostępu do danych są w ich przedsiębiorstwach wyznaczone i komunikowane w jasny sposób oraz 53% badanych zostało przeszkolonych z bezpiecznego uwierzytelnienia. Pozostałe działania są stosowane na mniejszą skalę: 12% do 26%, a 6% respondentów wybrało opcję *żadne z powyższych* (tabela 4.3.).

Tabela 4.3. Odpowiedź respondentów na pytanie: Proszę wskazać, które twierdzenia są prawdziwe w Pana(i) jednostce organizacyjnej w zakładzie pracy (wybór wielokrotny).

	Liczba odpowiedzi (L)	**Udział odpowiedzi (%)**
Mamy zapewnione wsparcie techniczne i merytoryczne, wiemy, do kogo się zwrócić w razie problemów	156	78%
Przeszkolono nas z bezpieczeństwa uwierzytelniania się	106	53%
Przechodzimy cykliczne szkolenia, na których poruszana jest kwestia bezpieczeństwa danych	36	18%
Mieliśmy wpływ na ustalenie zasad i wybór narzędzi uwierzytelniania	33	17%
Zasady dotyczące korzystania z kont pracowniczych i narzędzi uwierzytelniania są wyznaczone i jasno komunikowanie	106	53%
Bezpieczeństwo uwierzytelnienia ma realny wpływ na ocenę naszej pracy	52	26%
Działania związane z uwierzytelnieniem są kontrolowane na bieżąco, występuje reakcja przełożonych na nieprzestrzeganie zasad	40	20%
Można powiedzieć, że bezpieczeństwo danych ma bezpośrednie przełożenie na nasze zarobki	23	12%
Żadne z powyższych	11	6%

Źródło: opracowanie własne.

Zbadano jak kształtuje się postrzeganie przedsiębiorstw przez ich pracowników w obszarach: przywództwa, stylu zarządzania i kompetencji. Odpowiedzi na te pytania udzieliło średnio 199 respondentów, co stanowi prawie 99% badanych.

Respondenci udzielali odpowiedzi na pytania zgadzając się z opisywanym stanowiskiem (przypisanie odpowiedzi 4 – raczej się zgadzam i 5 – zgadzam się całkowicie), deklarując przeciwny stan rzeczy w macierzystym zakładzie pracy (1 – zupełnie się nie zgadzam oraz 2 – raczej się nie zgadam), bądź wybierali stanowisko neutralne (3).

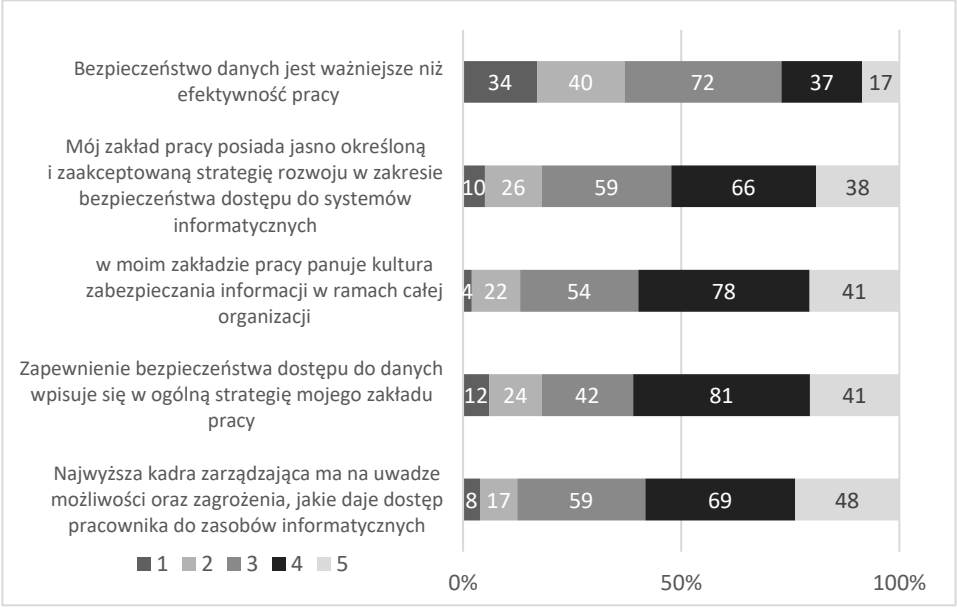
Poddając ocenie **przywództwo** (tabela 4.4.), w obszarze ochrony informacji większość (52%) respondentów deklaruje, że ich zakład pracy posiada jasno określoną i zaakceptowaną strategię ochrony dostępu do zasobów informatycznych, oraz, że jest ona istotnym elementem strategii zakładu pracy (61%), jego kultury organizacyjnej (60%), a także jest uwzględniana przez kadrę zarządzającą najwyższego szczebla (58%) (wykres 4.3.). Jednakże odpowiedzi dotyczące porównania znaczenia zapewnienia bezpieczeństwa danych z efektywnością pracy, rozkładają się inaczej: 27% respondentów deklaruje, że bezpieczeństwo

danych jest ważniejsze niż efektywność pracy, przeciwnego zdania jest 37% badanych, a 36% z nich wybrało stanowisko neutralne.

Tabela 4.4. Analiza odpowiedzi na pytania dotyczące przywództwa w przedsiębiorstwie w obszarze bezpieczeństwa informacji

	Wartość średnia (M)	**Odchylenie standardowe (SD)**
Najwyższa kadra zarządzająca ma na uwadze możliwości oraz zagrożenia, jakie daje dostęp pracownika do zasobów informatycznych	3,66	1,06
Zapewnienie bezpieczeństwa dostępu do danych wpisuje się w ogólną strategię mojego zakładu pracy	3,58	1,12
W moim zakładzie pracy panuje kultura zabezpieczania informacji w ramach całej organizacji	3,65	0,99
Mój zakład pracy posiada jasno określoną i zaakceptowaną strategię rozwoju w zakresie bezpieczeństwa dostępu do systemów informatycznych	3,48	1,10
Bezpieczeństwo danych jest ważniejsze niż efektywność pracy	2,82	1,17

Źródło: opracowanie własne.



Wykres 4.3. Rozkład odpowiedzi na pytania dotyczące przywództwa w przedsiębiorstwie w obszarze bezpieczeństwa informacji

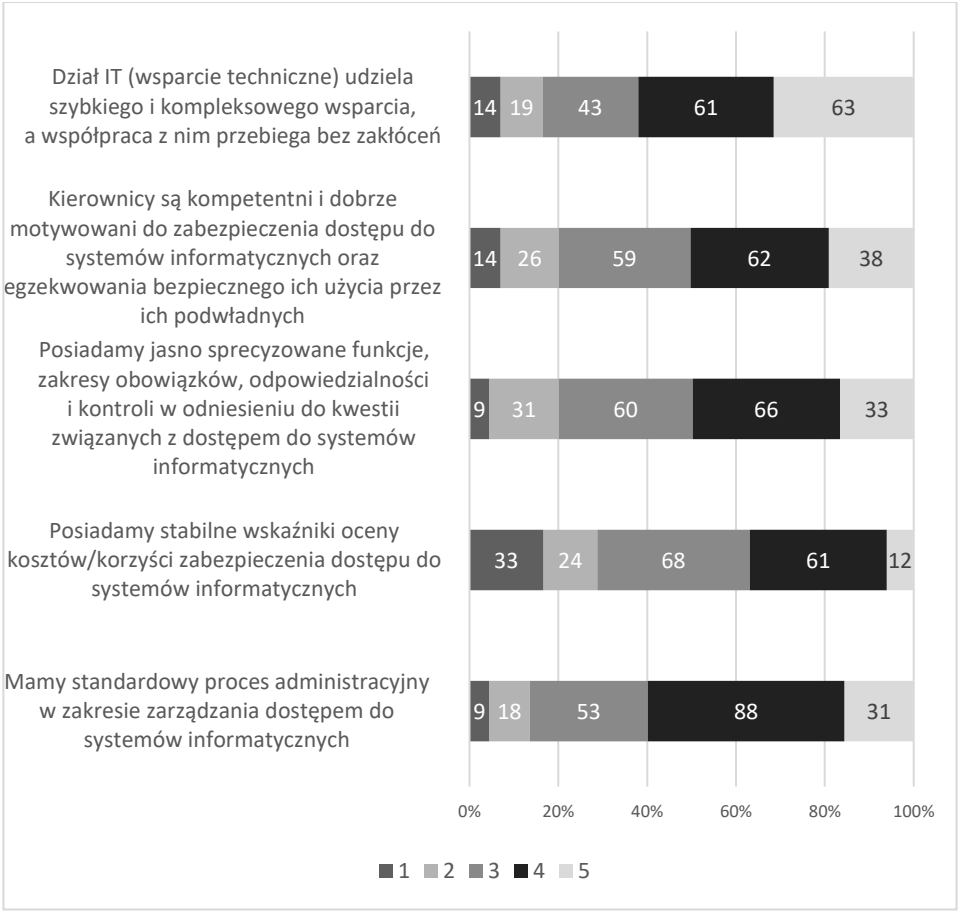
Źródło: opracowanie własne.

Respondenci ocenili **styl zarządzania** w obszarze ochrony dostępu do danych (tabela 4.5.). Większość (średnio 60% badanych) deklaruje, że ich przedsiębiorstwa posiadają: standardowy proces administracyjny związany z zarządzaniem dostępem do systemów informatycznych, jasny i kompletny podział funkcji, określenie zakresu obowiązków, odpowiedzialności i kontroli w odniesieniu do kwestii związanych z dostępem do systemów informatycznych (50%), kompetentne działania przełożonych (50%) oraz działu IT (62%). Natomiast istnienie stabilnych wskaźników do oceny kosztów/korzyści zabezpieczenia dostępu do systemów informatycznych deklaruje 37% respondentów (wykres 4.4.).

Tabela 4.5. Analiza odpowiedzi na pytania dotyczące stylu zarządzania przedsiębiorstwem w obszarze bezpieczeństwa informacji

	Wartość średnia (M)	**Odchylenie standardowe (SD)**
Mamy standardowy proces administracyjny w zakresie zarządzania dostępem do systemów informatycznych	3,57	1,01
Posiadamy stabilne wskaźniki oceny kosztów/korzyści zabezpieczenia dostępu do systemów informatycznych	2,97	1,16
Posiadamy jasno sprecyzowane funkcje, zakresy obowiązków, odpowiedzialności i kontroli w odniesieniu do kwestii związanych z dostępem do systemów informatycznych	3,42	1,08
Kierownicy są kompetentni i dobrze motywowani do zabezpieczenia dostępu do systemów informatycznych oraz egzekwowania bezpiecznego ich użycia przez ich podwładnych	3,42	1,15
Dział IT (wsparcie techniczne) udziela szybkiego i kompleksowego wsparcia, a współpraca z nim przebiega bez zakłóceń	3,70	1,21

Źródło: opracowanie własne.



Wykres 4.4. Odpowiedzi na pytania dotyczące stylu zarządzania w przedsiębiorstwie w obszarze bezpieczeństwa informacji

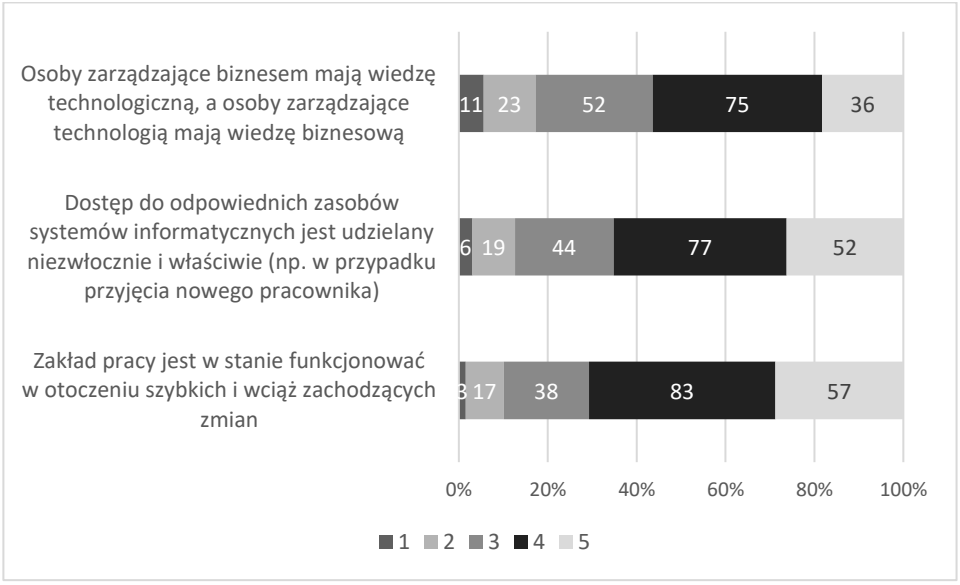
Źródło: opracowanie własne.

Respondenci wysoko ocenili **kompetencje kadry kierowniczej** (tabela 4.6.). 71% z nich uznało, że ich przedsiębiorstwo dobrze radzi sobie w szybko zmieniającym się otoczeniu. 65% badanych deklaruje, że dostęp do niezbędnych zasobów informatycznych udzielany jest niezwłocznie. Według 56% badanych, zarówno kadra zarządzająca procesami biznesowymi, jak i odpowiedzialna za aspekty techniczne w przedsiębiorstwie, posiada zarówno biznesową jak i technologiczną wiedzę (wykres 4.5.).

Tabela 4.6. Analiza odpowiedzi na pytania dotyczące kompetencji kadry kierowniczej przedsiębiorstwa

	Wartość średnia (M)	Odchylenie standardowe (SD)
Zakład pracy jest w stanie funkcjonować w otoczeniu szybkich i wciąż zachodzących zmian	3,88	0,97
Dostęp do odpowiednich zasobów systemów informatycznych jest udzielany niezwłocznie i właściwie (np. w przypadku przyjęcia nowego pracownika)	3,76	1,04
Osoby zarządzające biznesem mają wiedzę technologiczną, a osoby zarządzające technologią mają wiedzę biznesową	3,52	1,09

Źródło: opracowanie własne.



Wykres 4.5. Odpowiedzi na pytania dotyczące kompetencji kadry zarządzającej w przedsiębiorstwie
Źródło: opracowanie własne.

4.4. Postrzegana łatwość użycia

W celu oceny łatwości użycia rozwiązania o określonym standardzie bezpieczeństwa, przyjęto miarę postrzeganej uciążliwości danego rozwiązania. Aby móc estymować poziom uciążliwości, jaki generuje korzystanie danego narzędzia w określony sposób, od respondentów wymagane jest doświadczenie pracy z hasłem, przedmiotem lub metodą biometryczną.

Na pytania dotyczące uciążliwości bezpiecznego stosowania tożsamości cyfrowych odpowiedzi udzieliło średnio ponad 95% badanych, a wśród nich odpowiednio 100%, 97% i 92% stosowało hasła, przedmioty uwierzytelniające oraz narzędzie oparte o biometrię. Respondenci, którzy mieli do czynienia z narzędziami opartymi o poszczególne metody uwierzytelnienia, zostali poproszeni o estymację uciążliwości ich stosowania w sposób bezpieczny, poprzez wybór cyfry odpowiadającej jednej z opcji: 1 – zupełnie nieuciążliwe, 2 – generalnie nieuciążliwe, 3 – nieco uciążliwe, 4 – stanowiące pewną uciążliwość, 5 – stanowiące poważną uciążliwość.

Bezpieczne uwierzytelnienie oparte o hasło zdefiniowano w kwestionariuszu podając zasady budowy i użytkowania hasła, czyli: jego *długość* (min. 14 znaków), *skład* (co najmniej 1: wielka i mała litera, cyfra, znak specjalny; hasło nie mogłoby zawierać ważnych dla respondenta dat ani imion), *zmienność* (różne hasła do kluczowych aplikacji, zmiana hasła minimum co miesiąc) i *sposób przechowywania* (hasła nie mogłoby być przechowywane w postaci niezaszyfrowanej lub w miejscu, gdzie są łatwo dostępne, nie byłyby znane nikomu w miejscu pracy ani poza nim).

Bezpieczne uwierzytelnienie oparte o przedmiot zdefiniowano w kwestionariuszu podając zasady użytkowania przedmiotu, czyli: pieczołowite przechowywanie urządzenia / karty kodów (np. stale noszenie przy sobie, ew. złożenie w sejfie lub bardzo bezpiecznym miejscu) i nieprzekazywanie nikomu innemu oraz niezapisywanie i nieprzekazanie ewentualnego dodatkowego zabezpieczenia (PINu).

Wskazano, że uciążliwość uwierzytelniania biometrycznego może wynikać z jego wrażliwości na tymczasowe zmiany cech fizycznych / behawioralnych tj. otarcia naskórka / skaleczenia (odcisk palca), chrypka / przeziębienie (głos), spuchnięcie twarzy (geometria twarzy) oraz wrażliwości na zmiany warunków odczytu np. oświetlenia (geometria twarzy).

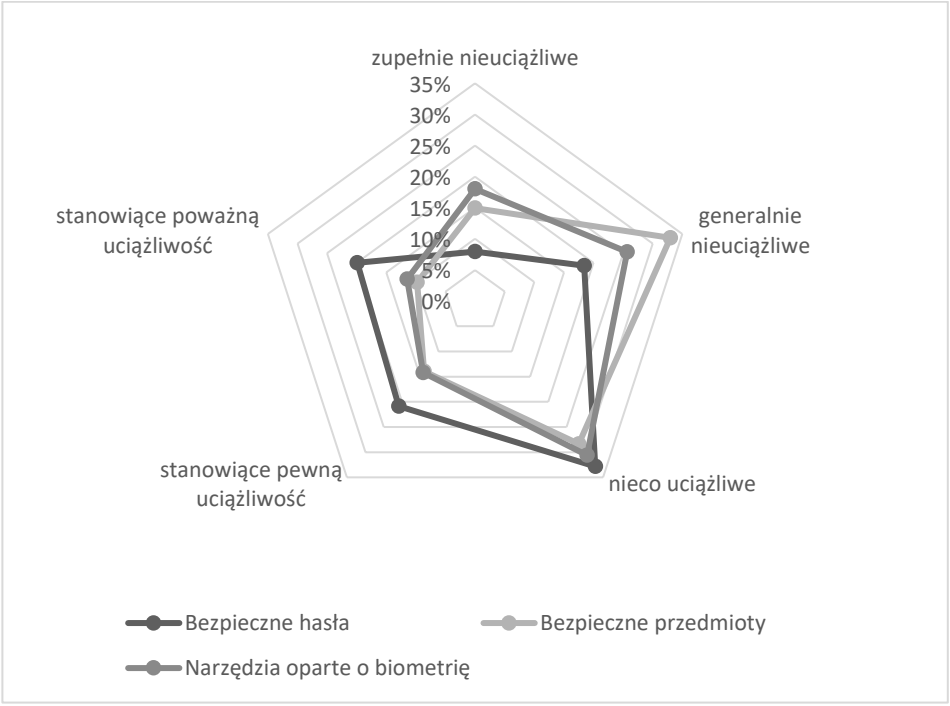
Postrzeganie przez respondentów uciążliwości korzystania z poszczególnych metod uwierzytelnienia przedstawiono w tabeli 4.7.

Tabela 4.7. Ocena uciążliwości poszczególnych metod uwierzytelnienia w skali od 1 (zupełnie nieuciążliwe) do 5 (stanowiące poważną uciążliwość)

	Wartość średnia (M)	**Odchylenie standardowe (SD)**	**Liczba odpowiedzi (L)**				
			1	**2**	**3**	**4**	**5**
Bezpieczne hasła	3,26	1,20	16	37	66	42	40
Bezpieczne przedmioty	2,71	1,23	29	64	55	27	19
Narzędzia oparte o biometrię	2,75	1,41	33	47	56	26	21

Źródło: opracowanie własne.

Uśredniając, respondenci wskazywali, że tak zdefiniowane bezpieczne uwierzytelnienie byłoby nieuciążliwe (2) lub nieco uciążliwe (3), przy czym bezpieczne uwierzytelnienie z użyciem przedmiotów uznano za najmniej, a haseł najbardziej uciążliwe (por. wykres 4.6.).



Wykres 4.6. Uciążliwość bezpiecznego stosowania poszczególnych narzędzi
Źródło: opracowanie własne.

4.5. Postrzegane straty z tytułu korzystania z tożsamości cyfrowych

Straty z tytułu bezpiecznego stosowania tożsamości cyfrowych podzielono na dwie grupy: straty na efektywności pracy oraz potencjalne zagrożenia, związane z korzystaniem z poszczególnych metod. W ramach pierwszej grupy postrzeganych strat, respondenci określali, w jakim stopniu zdefiniowane uprzednio bezpieczne korzystanie z tożsamości cyfrowych wpływałoby na efektywność ich pracy.

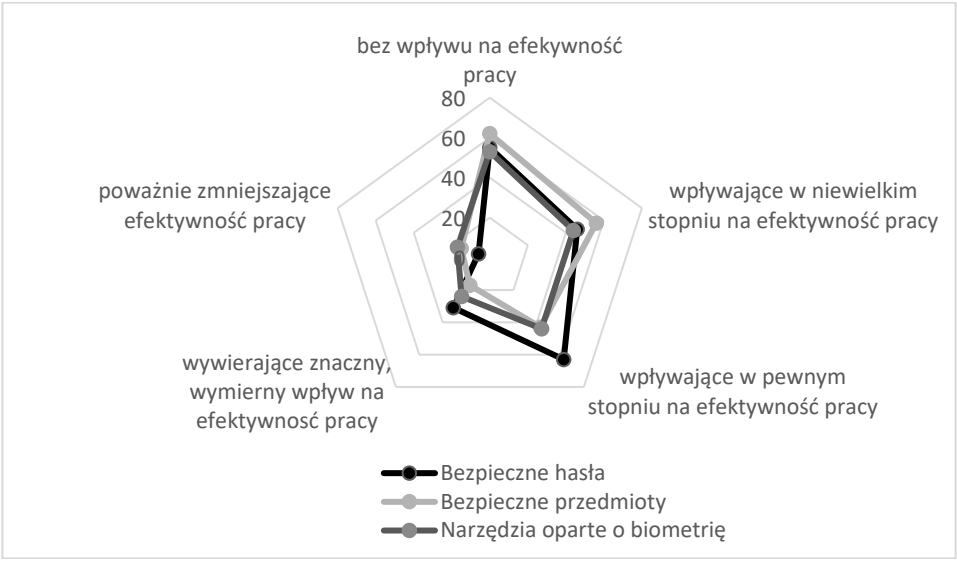
Na pytanie o wpływ korzystania w sposób bezpieczny z uwierzytelnienia na efektywność wykonywanej pracy, odpowiedzi udzieliło średnio prawie 99% badanych. Narzędziem, które było odbierane jako najmniej obniżające efektywność pracy, było uwierzytelnienie z wykorzystaniem przedmiotu, a za wywiera-

jące największy wpływ na efektywność pracy respondenci uznali uwierzytelnienie biometryczne (tabela 4.8, wykres 4.7).

Tabela 4.8. Ocena wpływu na efektywność pracy poszczególnych metod uwierzytelnienia w skali 1 (bez wpływu na efektywność pracy) – 5 (poważnie zmniejszające efektywność pracy)

	Wartość średnia (M)	**Odchylenie standardowe (SD)**	**Liczba odpowiedzi (L)**				
			1	**2**	**3**	**4**	**5**
Bezpieczne hasła	2,43	1,13	55	46	63	31	6
Bezpieczne przedmioty	2,31	1,61	62	56	43	17	15
Narzędzia oparte o biometrię	2,49	2,03	53	44	44	24	17

Źródło: opracowanie własne.



Wykres 4.7. Wpływ bezpiecznego stosowania poszczególnych narzędzi na efektywność pracy
Źródło: opracowanie własne.

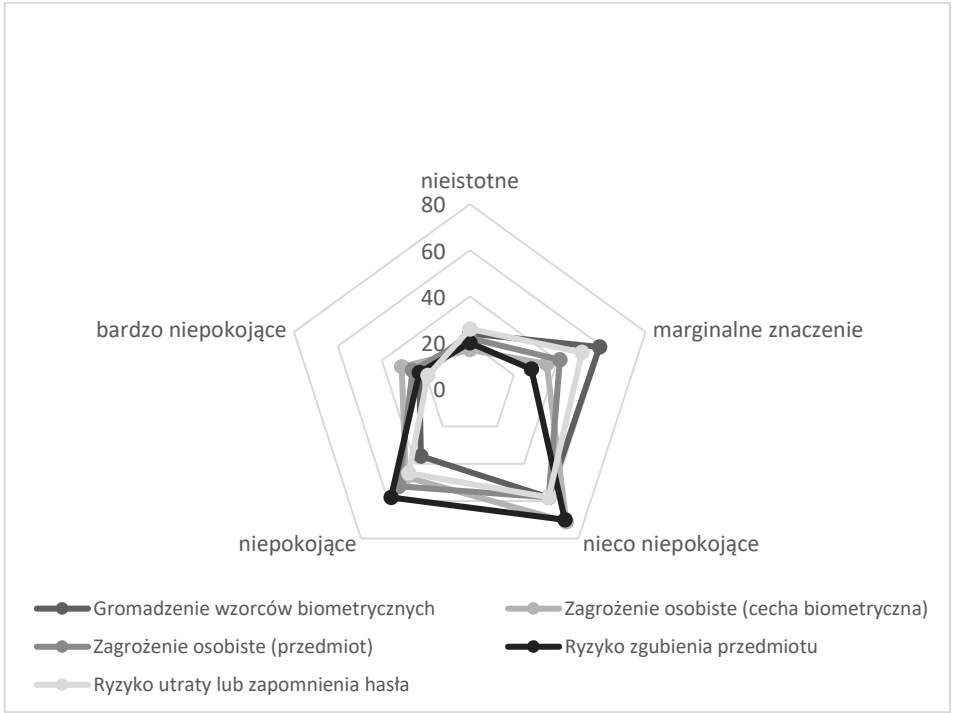
Na pytania dotyczące zagrożeń związanych z uwierzytelnieniem się, odpowiedzi udzieliło średnio prawie 99% badanych.

Największe obawy respondentów dotyczyły osobistego zagrożenia przy próbie dotarcia do zasobów chronionych cechami biometrycznymi oraz zgubienia przedmiotu. Respondenci najmniej obawiają się zapomnienia lub utraty hasła oraz gromadzenia wzorców biometrycznych przez przedsiębiorstwa, w których pracują (tabela 4.9., wykres 4.8.).

Tabela 4.9. Odczucia respondentów względem wybranych zdarzeń w skali 1 (nieistotne) – 5 (bardzo niepokojące)

	Wartość średnia (M)	**Odchylenie standardowe (SD)**	**Liczba odpowiedzi (L)**				
			1	**2**	**3**	**4**	**5**
Gromadzenie wzorców biometrycznych	2,88	1,19	24	59	58	36	23
Zagrożenie osobiste (cecha biometryczna)	3,20	1,15	17	35	71	47	31
Zagrożenie osobiste (przedmiot)	3,10	1,20	22	41	58	52	26
Ryzyko zgubienia przedmiotu	3,18	1,13	20	28	70	58	23
Ryzyko utraty lub zapomnienia hasła	2,90	1,18	26	51	58	45	19

Źródło: opracowanie własne.



Wykres 4.8. Odczucia respondentów względem wybranych zdarzeń

Źródło: opracowanie własne.

4.6. Stosunek do różnych metod uwierzytelnienia

Średnio 98% respondentów udzieliło odpowiedzi na pytanie dotyczące stosunku do różnych metod uwierzytelnienia.

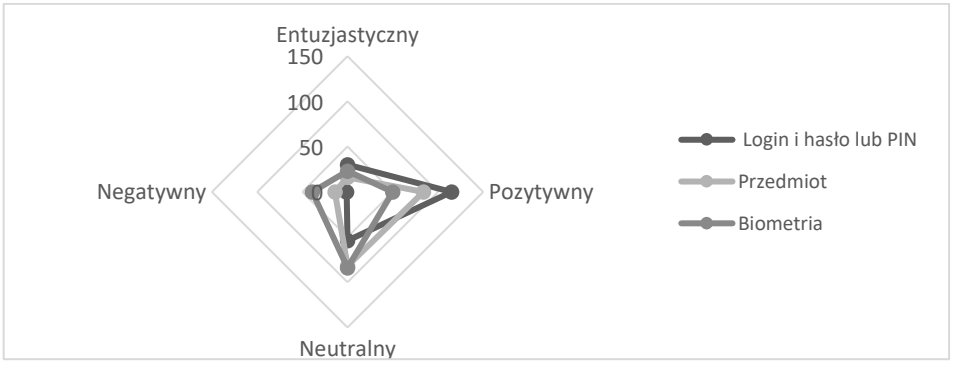
Z badań wynika, że największą akceptacją cieszyły się loginy, hasła lub numery PIN (por. tabela 4.10.). Stosunek nienacechowany pozytywnie zadeklarowało tylko 27,5% respondentów (1% badanych – negatywny, 26,5% – neutralny stosunek do tego narzędzia). W przypadku przedmiotów uwierzytelniających, udział deklarowanego negatywnego i neutralnego stosunku wynosił odpowiednio 7% i 42%, czyli w sumie niemal połowę odpowiedzi. W przypadku metod biometrycznych odsetek osób nastawionych negatywnie do tej metody uwierzytelnienia był znacząco wyższy (20%), podobnie jak respondentów z podejściem neutralnym (43%).

Tabela 4.10. Stosunek do różnych metod uwierzytelnienia

	Wartość średnia (M)	**Odchylenie standardowe (SD)**	**Liczba odpowiedzi (L)**			
			Entuzjastyczny	**Pozytywny**	**Neutralny**	**Negatywny**
Login i hasło lub PIN	2,13	0,65	30	115	54	1
Przedmiot	2,48	0,75	16	84	82	14
Biometria	2,71	0,92	23	50	84	39

Źródło: opracowanie własne.

Ponadto, najmniejsze zróżnicowanie odpowiedzi było w przypadku loginów, haseł lub numerów PIN, które były odbierane generalnie pozytywnie, a największe w przypadku metod biometrycznych, odbieranych najczęściej neutralnie i mniej pozytywnie niż uwierzytelnienia oparte o przedmiot (por. tabela 4.10. i wykres 4.9.).



Wykres 4.9. Stosunek do różnych metod uwierzytelnienia

Źródło: opracowanie własne.

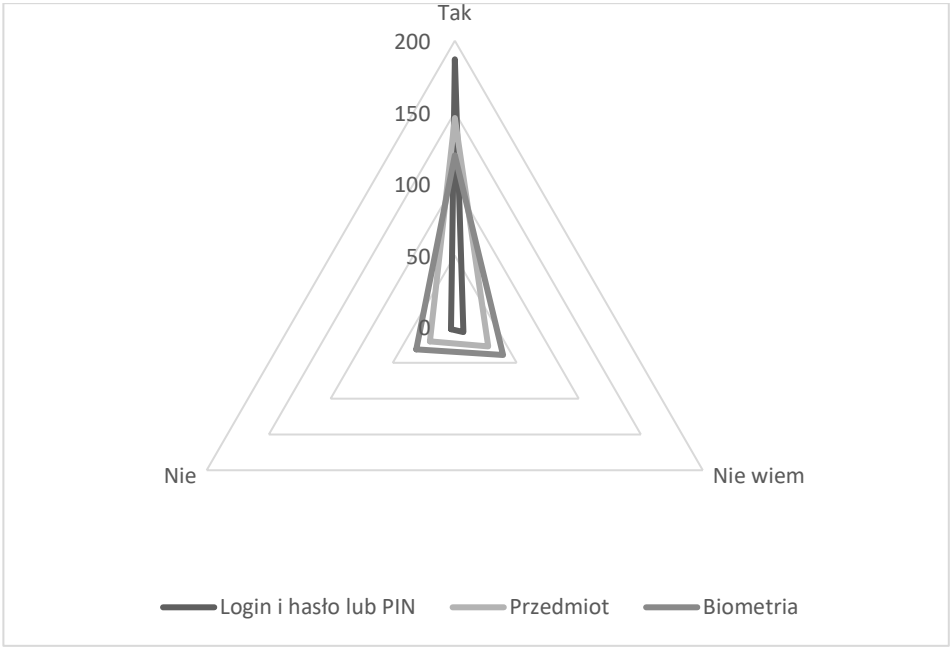
4.7. Intencje użycia

Respondenci zostali poproszeni o zdeklarowanie się, czy chcą używać uwierzytelnienia w sposób bezpieczny. Odpowiedzi na to pytanie udzieliło średnio 96% respondentów. Zdecydowana większość respondentów odpowiedziała na zadane pytanie twierdząco, choć wyraźnie zaznaczyły się różnice w zależności od wykorzystywanej metody uwierzytelnienia (wykres 4.10.). 95% respondentów jest gotowych stosować w sposób bezpieczny loginy i hasła lub numery PIN. W przypadku metod biometrycznych odsetek ten wynosi tylko 63% (tabela 4.11.).

Tabela 4.11. Deklarowana chęć respondentów do używania tożsamości cyfrowej w sposób bezpieczny w skali: 1 (tak), 2 (nie wiem), 3 (nie)

	Wartość średnia (M)	**Odchylenie standardowe (SD)**	**Liczba odpowiedzi (L)**		
			Tak	**Nie wiem**	**Nie**
Login i hasło lub PIN	1,07	0,30	187	7	3
Przedmiot	1,35	0,66	146	27	20
Biometria	1,53	0,77	120	39	31

Źródło: opracowanie własne.



Wykres 4.10. Odpowiedź respondentów na pytanie: Czy chce Pan(i) używać metod uwierzytelniania w sposób bezpieczny?

Źródło: opracowanie własne.

4.8. Postrzeganie wymuszenia

193 respondentów (96%) udzieliło odpowiedzi na pytanie wielokrotnego wyboru dotyczące pobudek, którymi kierują się stosując uwierzytelnienie. Większość z nich (69%) deklaruje, że kieruje nimi konieczność – bez uwierzytelnienia nie mogą dopełnić obowiązków zawodowych. Tyle samo osób kieruje się pobudkami wewnętrznymi (świadomością zalet dla zakładu pracy i samego respondenta), 12% respondentów deklaruje, że stosowanie przez nich uwierzytelnienia jest następstwem konkretnych działań przełożonych (tabela 4.12.).

Tabela 4.12. Odpowiedź respondentów na pytanie dotyczące czynników, które powodują, że korzystają oni z uwierzytelnień

	Liczba odpowiedzi (L)	**Procent odpowiedzi (%)**
Konieczność	133	69%
Świadomość zalet dla zakładu pracy	74	38%
Świadomość zalet dla respondenta	59	31%
Konkretne działania ze strony przełożonego	24	12%
Żadne	7	4%
Brak stosowanych uwierzytelnień	3	2%

Źródło: opracowanie własne.

4.9. Postrzeganie zagrożeń

Na pytanie dotyczące określenia, czy prawdopodobne są ataki cyberprzestępców na zakład pracy taki jak ich macierzyste przedsiębiorstwo, odpowiedziało 199 (prawie 99%) respondentów. Większość z nich (57%) uważa, że taki zakład pracy nie jest narażony na tego typu zagrożenie. Pozostali respondenci są przeciwnego zdania.

Odpowiedzi na pytanie, dotyczące oszacowania ryzyka powodzenia cyberataku, udzieliło 184 (91%) badanych. Większość (54%) określiła szansę na powodzenie takiego ataku jako średnie, 42% jako małe, a 4% jako duże (tabela 4.13.).

Tabela 4.13. Postrzeganie ryzyka powodzenia cyberataku na przedsiębiorstwo takie jak respondenta

	Wartość średnia (M)	**Odchylenie standardowe (SD)**	**Liczba odpowiedzi (L)**		
			Małe (1)	**Średnie (2)**	**Duże (3)**
Ryzyko powodzenia cyberataku na zasoby informatyczne przedsiębiorstwa	1,62	0,67	77	100	7

Źródło: opracowanie własne.

Łącznie 130 respondentów (64%) udzieliło odpowiedzi na wszystkie pytania, które stanowią czynniki krytyczne dla określenia poziomu bezpieczeństwa uwierzytelnienia zapewnianego przez respondentów. W przypadku nie posługiwania się hasłem (uwierzytelnienie z wykorzystaniem innych metod) poziom bezpieczeństwa oceniono indywidualnie dla każdego z 6 zakwalifikowanych przypadków. Zatem liczba respondentów, której poziom bezpieczeństwa korzystania z uwierzytelnienia został określony, to 136, czyli 67% osób badanych. W grupie 130 respondentów, którzy udzielili odpowiedzi na pytania dotyczące stosowanych przez nich haseł:

- 76% stosowało hasła dłuższe niż 8 znaków (co oznacza, że prawie 24% z tych osób stosuje hasła zbyt krótkie).
- Prawie 24% zmieniało hasła co 2 miesiące lub częściej, a 60% raz w roku lub częściej (prawie 34% respondentów nie zmienia haseł nigdy).
- 65% stosowało minimum 3 rodzaje znaków w hasłach, a hasła 21% składały się z 2 rodzajów znaków.
- Przytłaczająca większość (prawie 97%) deklarowała, że nie przechowuje haseł w wygodnym miejscu np. pod klawiaturą komputera.

Dla wspomnianych 136 osób określono poziomy bezpieczeństwa uwierzytelnienia (tabela 4.14.): prawie jednej czwartej z nich przypisano wysoki poziom, niecałej połowie – poziom niski, pozostałym poziom średni.

Tabela 4.14. Poziomy bezpieczeństwa określone na podstawie czynników krytycznych – rozkład odpowiedzi

	Klasyfikacja oparta o hasła		**Klasyfikacja ogólna**	
	Liczb odpowiedzi (L)	**Procent kwalifikowanych odpowiedzi (%)**	**Liczb odpowiedzi (L)**	**Procent kwalifikowanych odpowiedzi (%)**
Poziom wysoki	26	19%	32	24%
Poziom średni	43	32%	43	32%
Poziom niski	61	45%	61	45%

Źródło: opracowanie własne.

Przeanalizowano, jak zmieniają się podstawowe statystyki dla 130 odpowiedzi przypisanych do poszczególnych poziomów na postawie analizy parametrów haseł (vide tabela 4.15.). Zarówno średnia, jak i mediana wyraźnie wskazują na pogarszanie się parametrów haseł wraz z obniżeniem się przypisanego poziomu bezpieczeństwa. Generalnie natomiast, obserwowane jest zwiększanie się odchyleń standardowych, czyli rozrzutu odpowiedzi, co wskazywałoby, że w stosowanych hasłach zakwalifikowanych do średniego i niskiego poziomu, istnieją tylko luki bezpieczeństwa (niespełnianie części, nie wszystkich wymogów).

Tabela 4.15. Analiza odpowiedzi przypisanych do poszczególnych poziomów bezpieczeństwa na podstawie czynników krytycznych

Czynnik krytyczny	średnia	min	max	mediana	odchylenie standardowe
POZIOM WYSOKI					
Długość hasła	10,81	8,00	20,00	10,00	2,67
Częstotliwość zmiany hasła (liczba zmian na rok)	11,59	6,00	12,17	12,00	1,65
Liczba rodzajów znaków	3,77	3,00	4,00	4,00	0,20
POZIOM ŚREDNI					
Długość hasła	10,55	8,00	20,00	9,00	3,52
Częstotliwość zmiany hasła (liczba zmian na rok)	2,93	1,00	12,00	2,43	1,90
Liczba rodzajów znaków	3,21	2,00	4,00	3,00	0,86
POZIOM NISKI					
Długość hasła	7,70	1,00	21,00	7,50	3,15
Częstotliwość zmiany hasła (liczba zmian na rok)	0,89	0,00	12,17	0,00	2,72
Liczba rodzajów znaków	2,36	1,00	4,00	2,00	1,16

Źródło: opracowanie własne.

Dokonano korekty przypisanych poziomów z uwzględnieniem czynników dopełniających. W jej wyniku obniżono poziomy bezpieczeństwa dla 4 przypadków: 2 ze średniego na niski oraz 2 z wysokiego na średni. Ostateczne przypisanie poziomów przedstawiono w tabeli 4.16.

Tabela 4.16. Poziomy bezpieczeństwa – rozkład odpowiedzi

	Liczb odpowiedzi (L)	Procent kwalifikowanych odpowiedzi (%)
Poziom wysoki	30	22%
Poziom średni	43	32%
Poziom niski	63	46%

Źródło: opracowanie własne.

Ok. 125 respondentów (62%) udzieliło odpowiedzi na wszystkie pytania, które umożliwiły zestawienie poziomów bezpieczeństwa z postrzeganiem ryzyka powodzenia cyberataku. Wynik przyporządkowano do jednej z czterech grup (tabela 4.17.):

- Zgodność między poziomem bezpieczeństwa a postrzeganym poziomem ryzyka (OK).
- Wynik wątpliwy (W).
- Wynik nieprawidłowy 1 – niedoszacowanie ryzyka (NOK1).
- Wynik nieprawidłowy 2 – przeszacowanie lub inne czynniki ryzyka (NOK2) .

Tabela 4.17. Ocena świadomości respondenta dotyczącej jego roli w ochronie zasobów systemów informatycznych – rozkład odpowiedzi

	Liczba odpowiedzi (L)	**Procent odpowiedzi (%)**
OK	36	29%
W	63	50%
NOK1	26	21%
NOK2	0	0%

Źródło: opracowanie własne.

Niecałe 29% respondentów trafnie określa poziom ryzyka powodzenia cyberataku w kontekście użycia przez nich swoich tożsamości cyfrowych (tabela 4.17.). W przypadku połowy respondentów niemożliwe było jednoznaczne określenie zależności, natomiast w przypadku 21% respondentów widoczny jest brak refleksji dotyczącej przełożenia niskiego poziomu bezpieczeństwa, zapewnianego przez bieżący sposób korzystania przez nich z konta na bezpieczeństwo zasobów systemów informatycznych.

4.10. Charakterystyka użytkownika

Na pytanie dotyczące oceny własnej wiedzy dotyczącej uwierzytelnień odpowiedziało 174 (86%) respondentów. Badani generalnie dobrze oceniają swoją wiedzę: 58% przeciętnie, a 42% wysoko. Tylko 2% respondentów uważa, że ma niską wiedzę dotyczącą uwierzytelnień.

4.11. Charakterystyka narzędzi uwierzytelnienia

Na pytanie dotyczące narzędzi uwierzytelnienia stosowanych przez respondenta w zakładzie pracy, odpowiedzi udzieliło 99% respondentów (200 osób). Większość z nich deklarowała stosowanie haseł (97%), 48% przedmiotów uwierzytelniających, a 7,5% narzędzi biometrycznych – czytników linii papilarnych (tabela 4.18.).

Tabela 4.18. Narzędzia stosowane w zakładzie pracy respondenta do ochrony zasobów systemów informatycznych – rozkład odpowiedzi

Narzędzia uwierzytelniające	Liczba odpowiedzi (L)	Procent odpowiedzi (%)
Loginy i hasła / PIN	194	97,0%
Przedmioty	96	48,0%
Biometria	15	7,5%

Źródło: opracowanie własne.

Na pytanie dotyczące częstotliwości użycia narzędzi uwierzytelnienia przedstawionych w tabeli 4.18. odpowiedziało ponad 97% respondentów (197 osób). Narzędziem wykorzystywanym najczęściej w ciągu przeciętnego dnia pracy było uwierzytelnienie biometryczne (czytnik linii papilarnych), a najrzadziej – uwierzytelnienie z użyciem przedmiotów uwierzytelniających (tabela 4.19.).

Tabela 4.19. Częstotliwość wykorzystywania narzędzi uwierzytelnienia w ciągu przeciętnego dnia pracy

Narzędzia uwierzytelniające	Liczba odpowiedzi (L)	Procent odpowiedzi (%)	Średnia (M)	Mediana (Me)	Wartość max.	Odchylenie standardowe (SD)
Loginy i hasła / PIN	190,00	96%	6,13	3	60	8,63
Przedmioty	84,00	43%	4,84	2,25	20	5,78
Biometria	14,00	7%	10,93	3,5	50	15,10

Źródło: opracowanie własne.

Pozostałe parametry haseł zostały opisane w rozdziale 3.5.1.

4.12. Bezpieczeństwo użycia narzędzi uwierzytelnienia

194 osoby (96% respondentów) deklarowały wykorzystanie loginów i haseł lub numerów PIN do uwierzytelnienia się. Obszary, w których najwięcej było działań pozytywnie wpływających na bezpieczeństwo użycia tożsamości cyfrowych to (tabela 4.20.):

1. Stosowanie kont indywidualnych, właściwe przechowywanie hasła, ukrywanie znaków podczas wpisywania hasła, właściwa reakcja w sytuacji, gdy istnieje podejrzenie, że osoba postronna poznała hasło respondenta oraz zmiana hasła zgodnie z zaleceniami (powyżej 90%).
2. Unikanie stosowania w haśle treści łatwych do odgadnięcia (daty, imiona, proste sekwencje liter lub liczb) oraz stosowanie haseł o długości minimum 8 znaków (powyżej 70%).

Działania podnoszące bezpieczeństwo użytkowania hasła lub numeru PIN, które podejmowane były najrzadziej (poniżej 50% odpowiedzi respondentów) to:

nieudostępnianie swojego hasła innym osobom, stosowanie niepowtarzalnych haseł do każdej z aplikacji oraz zmiana haseł co najmniej raz na pół roku (tabela 4.20.).

Tabela 4.20. Elementy wpływające na bezpieczeństwo stosowania haseł – rozkład odpowiedzi

Element wpływający na bezpieczeństwo użycia hasła	Liczba udzielonych odpowiedzi (L)	Procent udzielonych odpowiedzi (%)	Bezpieczne użycie	
			Liczba odpowiedzi (L)	Procent odpowiedzi (%)
Długość hasła	184	95%	139	76%
Liczba grup znaków wykorzystywanych w haśle	141	73%	93	66%
Stosowanie w haśle ważnych dat, imion, sekwencji itp.	180	93%	155	86%
Częstotliwość zmiany hasła na rok	184	95%	87	47%
Przechowywanie hasła	167	86%	160*	96%
Udostępnianie hasła innym osobom	186	96%	79	42%
Wykorzystywanie jednego hasła do różnych aplikacji	189	97%	87	46%
Zmiana hasła zgodnie z zaleceniami	101	52%	93	92%
Reakcja na sytuację, gdy mogła nastąpić kompromitacja hasła	79	41%	74**	94%
Sposób uzyskiwania dostępu do zasobów systemów informatycznych	154	79%	154	100%
Zabezpieczenie przed podejrzeniem wprowadzanego hasła	186	96%	174	94%

**dotyczy osób, które wybrały działanie, które jednoznacznie może być przyporządkowane do grupy wspierającej bezpieczeństwo*

***dotyczy osób, które miały do czynienia z incydentem naruszenia bezpieczeństwa (ryzyko kompromitacji hasła)*

Źródło: opracowanie własne.

96 osób (48% respondentów) zadeklarowało stosowanie przedmiotu w celu potwierdzenia uprawnień dostępu do zasobów systemów informatycznych. Generalnie respondenci dobrze reagują w sytuacji podejrzenia, że przedmiot uwierzytelniający znalazł się w rękach nieuprawnionej osoby (powyżej 90%). Zdecydowana większość respondentów deklaruje, że posiada konto indywidualne (tabela

4.21.). Z drugiej strony większość badanych deklaruje, że udostępniło swój przedmiot innym osobom (powyżej 50%).

Tabela 4.21. Elementy wpływające na bezpieczeństwo stosowania przedmiotów – rozkład odpowiedzi

Element wpływający na bezpieczeństwo użycia przedmiotu	**Liczba udzielonych odpowiedzi (L)**	**Procent udzielonych odpowiedzi (%)**	**Bezpieczne użycie**	
			Liczba odpowiedzi (L)	**Procent odpowiedzi (%)**
Udostępnianie przedmiotu innym osobom	81	84%	35	43%
Przestrzeganie zasad związanych z przechowywaniem przedmiotu	19	20%	13*	68%
Reakcja na sytuację, gdy mogło nastąpić przejęcie przedmiotu przez osobę postronną	66	69%	60	91%
Sposób uzyskiwania dostępu do zasobów systemów informatycznych	96	100%	83	86%

**dotyczy osób, które miały do czynienia z incydentem naruszenia bezpieczeństwa (ryzyko kompromitacji przedmiotu)*

Źródło: opracowanie własne.

5. Wyznaczanie współczynników modelu

5.1. Założenia

W celu ujednolicenia, oznaczenia badanych czynników budowano z:

- Skrótów nazw elementów, których dotyczą np. PU, PEOU.
- *Opcjonalnie:*
    - *Liczby określającej numer pytania dotyczącego badanego elementu.*
    - *Małych liter określających odpowiedzi w ramach jednego pytania (wielokrotna odpowiedź).*
    - *Wielkich liter wskazujących na zawężenie badanego elementu do jednej metody uwierzytelnienia: H (hasła), P (przedmioty uwierzytelniające) oraz B (biometria).*

Przykładowo, pytanie dotyczące postrzegania użyteczności bezpiecznego korzystania z uwierzytelnienia biometrycznego zapisano jako: PU_1B.

Przeprowadzono następującą procedurę badawczą:

I. Zbadanie wewnętrznej spójności czynników – analiza współczynnika Alfa-Cronbacha.
II. Zbadanie siły związku i istotności statystycznej dla par zmiennych o danych ze skali nominalnej - testy niezależności Chi kwadrat (χ^2) ze współczynnikami siły związku. Dla zmiennych o danych ze skali porządkowej (rangowej) – współczynniki korelacji rang Spearmana z testami istotności.

Ad. I W ramach analizy współczynnika Alfa-Cronbacha badano spójność wewnętrzną tych elementów modelu, które badane były z wykorzystaniem wielu pytań. Badano także podgrupy pytań, w szczególności dotyczące różnych metod uwierzytelniających. Zaprezentowano wartość współczynnika oraz wyniki cząstkowe obliczeń według schematu przedstawionego w tabeli 5.1.

Tabela 5.1. Prezentacja wartości współczynnika Alfa-Cronbacha dla badanych elementów modelu

	Współczynnik
k=	
k/(k-1)=	
suma wariancji=	
wariancja sumy=	
alfa-C=	

Źródło: opracowanie własne.

Za graniczny poziom spójności wewnętrznej przyjęto wartość współczynnika Alfa-Cronbacha (alfa-C) na poziomie 0,7. Po przekroczeniu tej wartości tworzono wskaźnik będący średnią arytmetyczną wyników odpowiedzi.

Obliczeń dokonano z użyciem programu Excel 2016 (EXCEL PL dla Windows 10, Microsoft Sp. z.o.o.).

Ad. II W celu obliczenia siły związku i istotności statystycznej przyjęto następujący schemat postępowania:

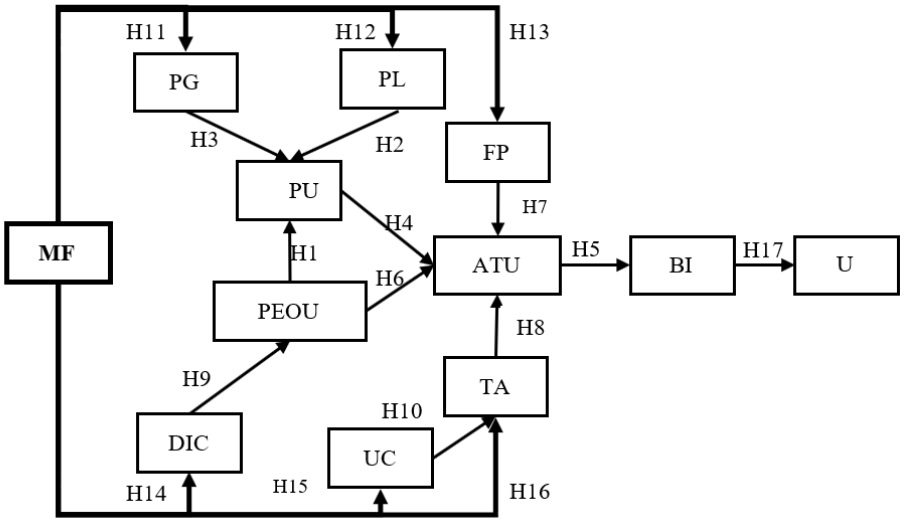
1. Postawiono statystyczne hipotezy $\boldsymbol{H^o_n}$, dotyczące braku zależności między poszczególnymi zmiennymi modelu.
2. Dla postawionych hipotez $\boldsymbol{H^o_n}$ definiowano hipotezy alternatywne $\boldsymbol{H^1_n}$, które stanowiły, że istnieje istotna zależność pomiędzy badanymi elementami modeli (rysunek 5.1. i tabela 5.2.).

Jeśli wykryto zależność między dwoma czynnikami, przedstawiono tabele zawierające wyniki analiz statystycznych, badania parami zależności zmiennych, przy użyciu trzech metod nieparametrycznych, opartych o tablice kontyngencji, trzy różne testy Chi-kwadrat oraz trzy wybrane współczynniki zależności.

Wyniki analiz zawierają tabele liczebności odpowiedzi, wartości obliczone zastosowanych funkcji testowych (z odpowiednimi stopniami swobody), obliczone prawdopodobieństwa odpowiadające funkcjom testowym, umożliwiające podjęcie decyzji dotyczących weryfikacji postawionych hipotez statystycznych H^0_n (na przyjętym poziomie istotności alfa = 0,05) oraz obliczone wartości współczynników zależności.

W celu identyfikacji relacji, jakie zachodzą między tabelaryzowanymi zmiennymi, dokonano analizy liczebności odpowiadających kategoriom wyznaczanym przez więcej niż jedną zmienną. Dane te przedstawiono w postaci tablic wielodzielczych, stanowiących kombinację dwóch lub więcej tabeli liczebności ułożonych w ten sposób, że każda komórka tabeli reprezentuje w jednoznaczny sposób kombinację konkretnych wartości tabelaryzowanych zmiennych.

W oparciu o opinie statystyków, bazowano głównie na teście **Chi-kwadrat (χ^2) oraz Chi-kwadrat największej wiarygodności** (*maximum likelihood test),* wartości współczynnika **Fi (**Φ *Yule'a), gdzie* (-1≤Fi≤1) oraz wartości współczynnika **korelacji rang Spearmana**.



Rysunek 5.1. Model i robocze hipotezy badawcze

Źródło: opracowanie własne.

Tabela 5.2. Statystyczne hipotezy badawcze

Nr hipotezy statystycznej	Badana zależność	Opis statystycznych hipotez zerowych H^0_n dla analizowanych par zmiennych
H1	PEOU → PU	Postrzegana łatwość bezpiecznego użycia tożsamości cyfrowej nie koreluje z postrzeganą użyteczność tożsamości cyfrowej stosowanej w sposób bezpieczny.
H2	PL → PU	Postrzegane straty z tytułu korzystania z tożsamości cyfrowych nie zależą od postrzeganej użyteczność tożsamości cyfrowej stosowanej w sposób bezpieczny.
H3	PG → PU	Postrzegane korzyści z tytułu bezpiecznego korzystania z tożsamości cyfrowych nie mają istotnego wpływu na postrzeganą użyteczność tożsamości cyfrowej stosowanej w sposób bezpieczny.
H4	PU → ATU	Postrzegana użyteczność tożsamości cyfrowej stosowanej w sposób bezpieczny nie koreluje z postawą wobec tożsamości cyfrowej.
H5	ATU → BI	Postawa wobec tożsamości cyfrowej nie wpływa na intencje użycia.
H6	PEOU →ATU	Postrzegana łatwość użycia tożsamości cyfrowej stosowanej w sposób bezpieczny nie koreluje z postawą wobec tożsamości cyfrowej.

H7	FP → ATU	Postrzeganie wymuszenia nie ma wpływu na postawę wobec tożsamości cyfrowej.
H8	TA → ATU	Świadomość zagrożeń nie ma wpływu na stosunek do tożsamości cyfrowej.
H9	DIC → PEOU	Charakterystyka stosowania narzędzi uwierzytelniających nie ma wpływu na łatwość ich użytkowania.
H10	UC → TA	Charakterystyka użytkownika nie ma wpływu na postrzeganie przez niego zagrożeń.
H11	MF → PG	Zarządzanie przedsiębiorstwem nie wpływa na postrzeganie korzyści wynikających z bezpiecznego uwierzytelniania się przez użytkownika.
H12	MF → PL	Zarządzanie przedsiębiorstwem nie wpływa na postrzeganie straty z tytułu bezpiecznego uwierzytelniania się przez użytkownika.
H13	MF → FP	Zarządzanie przedsiębiorstwem nie wpływa na postrzeganie wymuszenia stosowania uwierzytelnienia.
H14	MF → DIC	Zarządzanie przedsiębiorstwem nie wpływa na charakterystykę stosowanych narzędzi.
H15	MF → UC_4	Zarządzanie przedsiębiorstwem nie przekłada się na samoocenę wiedzy dotyczącej uwierzytelniania się.
H16	MF → TA	Poziom zarządzania nie ma wpływu na świadomość zagrożeń.
H17	BI →U	Intencje użycia nie przekładają się na bezpieczeńswo bieżącego użycia.

Źródło: opracowanie własne.

Przy wnioskowaniu (interpretacja obliczonych zależności) uwzględniono dwie kwestie. Po pierwsze stosowane testy analizy zależności (korelacji zmiennych) nie wskazują, która z pary analizowanych zmiennych jest zmienną zależną, a która niezależną. Przyczynowość określono w oparciu o wiedzę badacza lub wskazano tylko fakt zależności.

Po drugie, z podejmowaniem decyzji o przyjęciu bądź odrzuceniu hipotezy zerowej wiąże się ryzyko popełnienia błędów[31]:

- błąd I rodzaju = P(H^0 odrzucona, gdzie H^0 jest prawdziwa),
- błąd II rodzaju = P(H^0 nieodrzucona, gdzie H^0 jest fałszywa).

[31] Aczel, A.D. (2000). *Statystyka w zarządzaniu*, Warszawa: Wydawnictwo Naukowe PWN, s. 269.

Błąd I rodzaju nazywany jest w statystyce poziomem istotności (*dopuszczalnym ryzykiem błędu*) i jest oznaczany przez α. We wszystkich analizach statystyki matematycznej niniejszej pracy przyjęto α=0,05.

Błąd II rodzaju (β) minimalizuje się poprzez wybór testu o maksymalnej mocy (moc testu jest równa 1-β).

W przypadkach odrzucania hipotez zerowych (H^0), możliwe było popełnienie błędu I rodzaju, stąd proste implikacje dotyczące poziomu istotności. Jeśli wynik testu wskazywał na brak podstaw do odrzucenia H^0, sytuacja jest bardziej skomplikowana, gdyż brak jest kontroli nad błędem β. Powodem tego może być zarówno prawdziwość H^1, jak i zbyt słaba reprezentatywność próby – duża zmienność obiektów doświadczalnych, zbyt małe liczebności prób, błędy w pobieraniu prób itp. Jest to istotny problem ze względu na podmiot badań (ludzie), charakteryzujący się dużym udziałem w analizie tzw. błędu eksperymentalnego, wynikającego z dużej zmienności jednostek badanych obiektów. Tak więc nie odrzucenie hipotezy zerowej H^0 nie upoważnia jeszcze do zdecydowanego uznania braku korelacji pomiędzy zmiennymi i, w ramach dalszych badań, może zostać ponownie zweryfikowana.

W realizacji analiz statystycznych korzystano z systemów SAS oraz STATISTICA (STATISTICA PL dla Windows 1997, StatSoft Polska Sp. z o.o.).

5.2. Analiza współczynnika Alfa-Cronbacha

Przeprowadzono badanie rzetelności skali. Celem badania było zbadanie spójności wewnętrznej pytań oraz sprawdzenie, czy metoda uwierzytelnienia stanowi czynnik różnicujący odpowiedzi. Wykorzystano w tym celu wartość współczynnika Alfa-Cronbacha liczony według wzoru[32]:

$$\alpha c = \frac{k}{k-1}\left(1 - \frac{suma\ wariancji}{wariancja\ sum}\right)$$

5.2.1. Postrzegana użyteczność bezpiecznego korzystania z tożsamości cyfrowej (PU)

Czynnik PU był badany za pomocą trzech pytań odnoszących się do trzech różnych metod uwierzytelnienia, dlatego zbadano zgodność wewnętrzną testu (obliczenia w tabeli 5.3).

[32] *Analiza rzetelności i pozycji*. StatSoft. Online: http://www.statistica.pl/textbook/stathome_stat.html?http%3A%2F%2Fwww.statistica. pl%2Ftextbook%2Fstreliab.html, dostęp: 30.11.2021.

Tabela 5.3. Współczynnik Alfa-Cronbacha postrzeganej użyteczności bezpiecznego korzystania z tożsamości cyfrowej

	PU
k=	3
k/(k-1)=	1,5000
suma wariancji=	3,2172
wariancja sumy=	4,8122
alfa-C=	**0,4972**

Źródło: opracowanie własne.

Wartość współczynnika na poziomie 0,497 wskazuje, że metoda uwierzytelnienia jest istotnym czynnikiem różnicującym odpowiedzi, a czynnik PU powinien być rozpatrywany osobno jako trzy czynniki: PU_1H, PU_1P oraz PU_1B.

5.2.2. Postrzegana łatwość bezpiecznego korzystania z tożsamości cyfrowej (PEOU)

Również czynnik PEOU był badany za pomocą trzech pytań odnoszących się do trzech różnych metod uwierzytelnienia, dlatego zbadano spójność wewnętrzną pytań (obliczenia w tabeli 5.4).

Tabela 5.4. Współczynnik Alfa-Cronbacha postrzeganej łatwości bezpiecznego korzystania z tożsamości cyfrowej

	PEOU
k=	3
k/(k-1)=	1,5000
suma wariancji=	4,3518
wariancja sumy=	6,5240
alfa-C=	**0,4994**

Źródło: opracowanie własne.

Wynik współczynnika na poziomie 0,499 wskazuje, że metoda uwierzytelnienia jest istotnym czynnikiem różnicującym odpowiedzi, a czynnik PEOU powinien być rozpatrywany osobno jako trzy czynniki: PEOU_1H, PEOU_1P oraz PEOU_1B.

5.2.3. Postrzegane straty z tytułu bezpiecznego korzystania z tożsamości cyfrowej (PL)

Zbadano spójność pytań badających postrzegane straty z tytułu korzystania z tożsamości cyfrowych wszystkich pozycji oraz w podziale na dwie grupy (obliczenia w tabeli 5.5).

Tabela 5.5. Współczynnik Alfa-Cronbacha dla postrzeganych strat z tytułu bezpiecznego korzystania z tożsamości cyfrowej

	PL	**Grupa 1**	**Grupa 2**
k=	8	5	3
k/(k-1)=	1,1429	1,2500	1,5000
suma wariancji=	11,8184	6,8208	4,9594
wariancja sumy=	28,3775	18,7499	8,9085
alfa-C=	**0,6669**	**0,7953**	**0,6649**

Źródło: opracowanie własne.

Wynik na poziomie 0,670 wskazuje, że spójność pytań jest zbyt niska. Czynnik PL badany był za pomocą dwóch grup pytań:

Grupa 1.Związanej z potencjalnym intencjonalnym bądź nieintencjonalnym zagrożeniem, którym obarczone jest korzystanie z tożsamości cyfrowej. Wynik na poziomie 0,795 wskazuje na spójność wewnętrzną pytań. Utworzono wskaźnik PL_1 jako średnią arytmetyczną przypisanych przez użytkownika wag.

Grupa 2.Związanej z wpływem na efektywność pracy w odniesieniu do trzech metod uwierzytelnienia. Wynik na poziomie 0,665 wskazuje na konieczność badania trzech czynników: PL_2H, PL_2P, PL_2B osobno.

5.2.4. Postrzegane korzyści z tytułu bezpiecznego stosowania tożsamości cyfrowej (PG)

Zbadano spójność wewnętrzną pytań dotyczących postrzeganych korzyści z tytułu bezpiecznego korzystania z tożsamości cyfrowych (obliczenia w tabeli 5.6).

Tabela 5.6. Współczynnik Alfa-Cronbacha dla postrzeganych korzyści z tytułu bezpiecznego korzystania z tożsamości cyfrowej

	PG
k=	5
k/(k-1)=	1,2500
suma wariancji=	6,7774
wariancja sumy=	25,5346
alfa-C=	**0,9182**

Źródło: opracowanie własne.

Wynik na poziomie 0,918 wskazuje na wysoką rzetelność skali czynnika PG. Utworzono wskaźnik PG jako średnią arytmetyczną odpowiedzi respondentów.

5.2.5. Postawa wobec tożsamości cyfrowej (ATU)

Czynnik ATU był badany za pomocą trzech pytań odnoszących się do trzech różnych metod uwierzytelnienia, stąd badanie spójności pytań (wyniki obliczeń w tabeli 5.7).

Tabela 5.7. Współczynnik Alfa-Cronbacha dla postrzeganych korzyści z tytułu bezpiecznego korzystania z tożsamości cyfrowej

	ATU
k=	3
k/(k-1)=	1,5000
suma wariancji=	1,8270
wariancja sumy=	2,4323
alfa-C=	**0,3733**

Źródło: opracowanie własne.

Wynik współczynnika na poziomie 0,373 wskazuje, że metoda uwierzytelnienia jest istotnym czynnikiem różnicującym odpowiedzi, a czynnik ATU powinien być rozpatrywany osobno jako trzy czynniki: ATU_1H, ATU_1P oraz ATU_1B.

5.2.6. Intencje użycia (BI)

Podobnie jak w przypadku innych elementów modelu, czynnik BI był badany za pomocą trzech pytań odnoszących się do trzech różnych metod uwierzytelnienia (wyniki obliczeń w tabeli 5.8).

Tabela 5.8. Współczynnik Alfa-Cronbacha dla intencji użycia tożsamości cyfrowej

	BI
k=	3
k/(k-1)=	1,5000
suma wariancji=	1,3281
wariancja sumy=	2,3799
alfa-C=	**0,6629**

Źródło: opracowanie własne.

Wynik współczynnika na poziomie 0,663 wskazuje, że metoda uwierzytelnienia jest istotnym czynnikiem różnicującym odpowiedzi, a czynnik BI powinien być rozpatrywany osobno jako trzy czynniki: BI_1H, BI_1P oraz BI_1B.

5.2.7. Czynniki zarządcze (MF)

Czynniki zarządcze były elementem modelu badanym za pomocą 21 parametrów, dlatego sprawdzono spójność pytań (wyniki obliczeń w tabeli 5.9).

Tabela 5.9. Współczynnik Alfa-Cronbacha dla czynników zarządczych

	MF
k=	22
k/(k-1)=	1,0476
suma wariancji=	52,1478
wariancja sumy=	213,7226
alfa-C=	**0,7920**

Źródło: opracowanie własne.

Wynik na poziomie 0,792 wskazuje na akceptowalną rzetelność skali czynnika MF. Utworzono zatem wskaźnik MF jako średnią arytmetyczną odpowiedzi respondentów.

5.2.8. Porównanie współczynnika Alfa-Cronbacha po eliminacji pytań dotyczących poszczególnych metod uwierzytelnienia

W większości pytań spójność pytań była większa dla pytań dotyczących haseł i przedmiotów, a najniższa gdy pytania dotyczyły haseł i biometrii (tabela 5.10.).

Tabela 5.10. Współczynnik Alfa-Cronbacha obliczony dla par pytań

	Metoda uwierzytelnienia w wyeliminowanym pytaniu		
	Hasło	**Przedmiot**	**Biometria**
PU	0,6417	0,0317	0,4053
PEOU	0,4799	0,2413	0,4821
PL	0,4624	0,2628	0,5009
ATU	0,3102	-0,1665	0,6322
BI	0,7620	0,4660	0,6516

Źródło: opracowanie własne.

5.3. Analiza statystyczna zależności pomiędzy elementami modelu

5.3.1. Badanie hipotezy statystycznej H1 (zależność PU od PEOU)

Zbadano związek pomiędzy postrzeganą użytecznością bezpiecznego stosowania tożsamości cyfrowej (PU) i postrzeganą łatwością bezpiecznego stosowania tożsamości cyfrowej (PEOU). Oba te czynniki rozpatrywano dla trzech metod uwierzytelnienia (tabela 5.11.).

Tabela 5.11. Współczynniki korelacji Spearmana (Rang Spearmana) PU i PEOU

Prawd. > |r| (p obliczone) przy H0: Rho=0 (H^0_1)			
n - liczba obserwacji			
	PEOU_1H	PEOU_1P	PEOU_1B
PU_1H	-0.05173	0,12889	0,09223
	0.4669	0,0703	0,1951
	200	198	199
PU_1P	0,08471	-0,02539	0,03314
	0,2415	0,7273	0,6482
	193	191	192
PU_1B	0,04197	-0,08582	**r = -0,22133**
	0,5643	0,2378	**p = 0.0021**
	191	191	**n = 190**

Źródło: opracowanie własne.

Nie wykazano zależności istotnej statystycznie między postrzeganą użytecznością bezpiecznego stosowania tożsamości cyfrowej z wykorzystaniem haseł i przedmiotów uwierzytelniających (odpowiednio PU_1H, PU_1P), a postrzeganą łatwością bezpiecznego stosowania tożsamości cyfrowej z wykorzystaniem tych metod uwierzytelniania (odpowiednio PEOU_1H, PEOU_1P) – obliczane prawdopodobieństwo p > 0,05 (vide tabela 5.11.).

Wykazano niezbyt dużą, ale istotną statystycznie (obliczone **p = 0,0021** < 0.05) zależność między postrzeganą łatwością użycia biometrii, a postrzeganą użytecznością tej metody.

Przeprowadzono analizę za pomocą testu Chi^2. Wyniki przedstawiono w tabeli 5.12. i 5.13.

Tabela 5.12. Analiza statystyczna liczności odpowiedzi PU_1B wg PEOU_1B

Tabela PU_1B wg PEOU_1B								
PU_1B		PEOU_1B						Razem
		0	1	2	3	4	5	
1	Liczebność	1	1	2	2	4	9	19
	Procent	0,53	0,53	1,05	1,05	2,11	4,74	10,00
2	Liczebność	2	2	4	7	4	0	19
	Procent	1,05	1,05	2,11	3,68	2,11	0	10,00
3	Liczebność	6	5	13	19	6	6	55
	Procent	3,16	2,63	6,84	10	3,16	3,16	28,95
4	Liczebność	1	9	18	8	6	4	46
	Procent	0,53	4,74	9,47	4,21	3,16	2,11	24,21
5	Liczebność	3	16	6	19	5	2	51
	Procent	1,58	8,42	3,16	10	2,63	1,05	26,84
Razem	Liczebność	13	33	43	55	25	21	190
	Procent	6,84	17,37	22,63	28,95	13,16	11,05	100.00
	Procent	6,84	17,37	22,63	28,95	13,16	11,05	100.00

Źródło: opracowanie własne.

Tabela 5.13. Statystyki dla tabeli PU_1B wg PEOU_1B

Statystyka	Stopnie swobody	Wartość	Obliczone prawdopodobieństwo p
Chi-kwadrat	**20**	**59,3183**	**<.0001**
Chi-kw. ilorazu wiarygodności	**20**	**52,8287**	**<.0001**
Chi-kwadrat Mantela-Haenszela	1	11,5627	0,0007
Współczynnik FI		**0,5588**	
Współczynnik wielodzielczości		0,4878	
V Cramera		0,2794	

Źródło: opracowanie własne.

Otrzymano obliczone prawdopodobieństwo **p <0,0001**. Stwierdzono dosyć dużą zależność.

Wnioski:

1. W przypadku uwierzytelnień opartych o hasła oraz przedmioty nie ma podstaw do odrzucenia hipotezy zerowej H^0_1 ; w przypadku uwierzytelnień biometrycznych należy odrzucić hipotezę zerową H^0_1 o niezależności badanych zmiennych, na korzyść hipotezy alternatywnej H^1_1.
2. **Zależność 1**: im wyższa uciążliwość uwierzytelnienia biometrycznego, tym mniejsza postrzegana jego użyteczność – ujemny współczynnik korelacji.

Siła zależności 1: niezbyt duży, ale wysoko istotny statystycznie współczynnik korelacji Rang Spearmana: r = -0,22 i dla testu $Chi^{2;}$ duży fi = 0,56.

5.3.2. Badanie hipotezy statystycznej H2 (zależność PU od PL)

Zbadano związek pomiędzy postrzeganą użytecznością bezpiecznego stosowania tożsamości cyfrowej (PU) i postrzeganymi stratami z tytułu stosowania tożsamości cyfrowej (PL). PU rozpatrywano dla trzech metod uwierzytelnienia, natomiast czynnik PL badano w kontekście wpływu różnych metod uwierzytelnienia na efektywność pracy (PL_1) oraz różnych obaw dotyczących uwierzytelnień (PL_2).

Tabela 5.14. Współczynniki korelacji Spearmana (Rang Spearmana) PL i PU

Współczynniki korelacji Spearmana				
Prawd. > |r| przy H0: Rho=0				
Liczba obserwacji				
	PL_1H	PL_1P	PL_1B	PL_2
PU_1H	-0,05584	0,06766	0,13328	0,07659
	0,4334	0,3436	0,0606	0,2811
	199	198	199	200
PU_1P	0,07619	-0,01856	0,05905	0,01981
	0,2936	0,7989	0,4159	0,7845
	192	191	192	193
PU_1B	-0,02733	**r = -0,15524**	-0,13223	0,04916
	0,7082	**p = 0,032**	0,069	0,4995
	190	**n = 191**	190	191

Źródło: opracowanie własne.

Nie wykazano zależności istotnej statystycznie między postrzeganą użytecznością bezpiecznego stosowania tożsamości cyfrowej z wykorzystaniem haseł i przedmiotów uwierzytelniających (PU_1H, PU_1P), a postrzeganymi stratami na efektywności z tytułu bezpiecznego stosowania tożsamości cyfrowej (PL_1H, PL_1P) – obliczone prawdopodobieństwo p > 0,05 (vide tabela 5.14.).

Wykazano zależność (obliczone **p = 0,032** < 0,05) między postrzeganymi stratami na efektywności pracy z tytułu bezpiecznego korzystania z przedmiotów uwierzytelniających a postrzeganą użytecznością biometrii.

Przeprowadzono analizę z wykorzystaniem testu Chi^2. Wykryto zależność między postrzeganymi stratami na efektywności pracy z tytułu korzystania z bio-

metrii a postrzeganiem jej użyteczności. Wyniki analizy zawarte są w tabelach 5.15. i 5.16.

Tabela 5.15. Analiza statystyczna liczności odpowiedzi PU_1B wg PL_1B

Tabela PU_1B wg PL_1B								
PU_1B		**PL_1B**						**Razem**
		0	**1**	**2**	**3**	**4**	**5**	
1	Liczebność	2	1	3	3	4	6	19
	Procent	1,05	0,53	1,58	1,58	2,11	3,16	10
	Proc. wier.	10,53	5,26	15,79	15,79	21,05	31,58	
	Proc. kol.	15,38	2	7,14	6,82	16,67	35,29	
2	Liczebność	2	5	4	5	2	1	19
	Procent	1,05	2,63	2,11	2,63	1,05	0,53	10
	Proc. wier.	10,53	26,32	21,05	26,32	10,53	5,26	
	Proc. kol.	15,38	10	9,52	11,36	8,33	5,88	
3	Liczebność	6	15	9	10	8	7	55
	Procent	3,16	7,89	4,74	5,26	4,21	3,68	28,95
	Proc. wier.	10,91	27,27	16,36	18,18	14,55	12,73	
	Proc. kol.	46,15	30	21,43	22,73	33,33	41,18	
4	Liczebność	1	11	16	11	6	1	46
	Procent	0,53	5,79	8,42	5,79	3,16	0,53	24,21
	Proc. wier.	2,17	23,91	34,78	23,91	13,04	2,17	
	Proc. kol.	7,69	22	38,1	25	25	5,88	
5	Liczebność	2	18	10	15	4	2	51
	Procent	1,05	9,47	5,26	7,89	2,11	1,05	26,84
	Proc. wier.	3,92	35,29	19,61	29,41	7,84	3,92	
	Proc. kol.	15,38	36	23,81	34,09	16,67	11,76	
Razem	Liczebność	13	50	42	44	24	17	190
	Procent	6,84	26,32	22,11	23,16	12,63	8,95	100

Źródło: opracowanie własne.

Tabela 5.16. Statystyki dla tabeli PU_1B wg PL_1B

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**20**	**33,7818**	**0,0276**
Chi-kw. ilorazu wiarygodn.	**20**	**32,2075**	**0,0411**
Chi-kwadrat Mantela-Haenszela	1	5,3119	0,0212
Współczynnik FI		**0,4217**	
Współczynnik wielodzielczości		0,3885	
V Cramera		0,2108	

Źródło: opracowanie własne.

Otrzymano obliczone prawdopodobieństwo **p = 0,0411 < 0,05**. Stwierdzono istotną statystycznie zależność badanych zmiennych.

Wnioski:

1. W przypadku uwierzytelnień opartych o hasła oraz przedmioty nie ma podstaw do odrzucenia hipotezy zerowej H^0_2 ; w przypadku uwierzytelnień biometrycznych należy odrzucić hipotezę zerową H^0_2 o niezależności badanych zmiennych, na korzyść hipotezy alternatywnej H^1_2.
2. **Zależność 2**: im niższe straty na efektywności pracy spowodowane bezpiecznym korzystaniem z przedmiotu uwierzytelniającego, tym większa postrzegana użyteczność uwierzytelnienia biometrycznego – ujemny współczynnik korelacji.

   Siła zależności 2: mała (wg badania korelacji Rang Spearmana; r = -0,16) i dość duża (test Chi^2; fi = 0,42).

5.3.3. Badanie hipotezy statystycznej H3 (zależność PU od PG)

Zbadano związek pomiędzy postrzeganą użytecznością bezpiecznego stosowania tożsamości cyfrowej (PU) i postrzeganymi korzyściami z tytułu bezpiecznego stosowania tożsamości cyfrowej (PG). PU rozpatrywano dla trzech metod uwierzytelnienia (PU_1H, P_1P, PU_1B), PG natomiast łącznie (PG_1) oraz w rozbiciu na poszczególne pytania (PG_1a, PG_1b, PG_1c, PG_1d, PG_1e).

Tabela 5.17. Współczynniki korelacji Spearmana (Rang Spearmana) PG i PU

Współczynniki korelacji Spearmana						
Prawd. > |r| przy H0: Rho=0						
Liczba obserwacji						
	PG_1a	PG_1b	PG_1c	PG_1d	PG_1e	PG_1
PU_1H	-0,00865	0,03422	-0,01413	-0,02814	-0,01783	-0,01526
	0,9032	0,6313	0,8433	0,6931	0,8022	0,8297
	200	199	198	199	200	201
PU_1P	-0,00536	-0,01957	0,00505	-0,02839	0,02045	-0,01435
	0,9411	0,7876	0,9447	0,6959	0,7778	0,8426
	193	192	191	192	193	194
PU_1B	0,07845	0,13935	0,10139	0,07558	0,12475	0,12681
	0,2807	0,0552	0,1651	0,300	0,0855	0,0796
	191	190	189	190	191	192

Źródło: opracowanie własne.

Badanie współczynników korelacji Spearmana nie wykazało zależności istotnej statystycznie między PU a PG (tabela 5.17.). Współczynniki korelacji między PU_1B a PG_1b, PG_1e i PG_1 znalazły się blisko granicy uznania za istotne statystycznie.

Przeprowadzona analiza Chi^2 wykazała:

1. Zależność między znaczeniem redukcji ryzyka odpowiedzialności np. karnej, rozumianej jako korzyść z bezpiecznego stosowania tożsamości cyfrowej (PG_1b), a postrzeganiem użyteczności biometrii jako metody uwierzytelnienia (PU_1B) – obliczone prawdopodobieństwo **p = 0,0027** < 0,05 (vide tabela 5.18. i tabela 5.19.).
2. Zależność między świadomością wypełnienia obowiązków (zgodność z wytycznymi), rozumianą jako korzyść z bezpiecznego stosowania tożsamości cyfrowej (PG_1c), a postrzeganiem użyteczności biometrii jako metody uwierzytelnienia (PU_1B) – obliczone prawdopodobieństwo **p = 0,0231** < 0,05 (vide tabela 5.20. i tabela 5.21.).

Tabela 5.18. Analiza statystyczna liczności odpowiedzi PU_1B wg PG_1b

Tabela PU_1B wg PG_1b							
PU_1B		**PG_1b**					Razem
		1	**2**	**3**	**4**	**5**	
1	Liczebność	5	2	3	2	6	18
	Procent	2,63	1,05	1,58	1,05	3,16	9,47
	Proc. wier.	27,78	11,11	16,67	11,11	33,33	
	Proc. kol.	38,46	13,33	6,98	2,9	12	
2	Liczebność	0	4	8	7	1	20
	Procent	0	2,11	4,21	3,68	0,53	10,53
	Proc. wier.	0	20	40	35	5	
	Proc. kol.	0	26,67	18,6	10,14	2	
3	Liczebność	3	1	16	19	16	55
	Procent	1,58	0,53	8,42	10	8,42	28,95
	Proc. wier.	5,45	1,82	29,09	34,55	29,09	
	Proc. kol.	23,08	6,67	37,21	27,54	32	
4	Liczebność	1	3	10	18	13	45
	Procent	0,53	1,58	5,26	9,47	6,84	23,68
	Proc. wier.	2,22	6,67	22,22	40	28,89	
	Proc. kol.	7,69	20	23,26	26,09	26	
5	Liczebność	4	5	6	23	14	52
	Procent	2,11	2,63	3,16	12,11	7,37	27,37
	Proc. wier.	7,69	9,62	11,54	44,23	26,92	
	Proc. kol.	30,77	33,33	13,95	33,33	28	
Razem	Liczebność	13	15	43	69	50	190
	Procent	6,84	7,89	22,63	36,32	26,32	100

Źródło: opracowanie własne.

Tabela 5.19. Statystyki dla tabeli PU_1B wg PG_1b

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**16**	**36,4501**	**0,0025**
Chi-kw. ilorazu wiarygodn.	**16**	**36,2086**	**0,0027**
Chi-kwadrat Mantela-Haenszela	1	4,7477	0,0293
Współczynnik FI		**0,438**	
Współczynnik wielodzielczości		0,4012	
V Cramera		0,219	

Źródło: opracowanie własne.

Tabela 5.20. Analiza statystyczna liczności odpowiedzi PU_1B wg PG_1c

Tabela PU_3B wg PG_1c							
PU_1B		**PG_1c**					Razem
		1	**2**	**3**	**4**	**5**	
1	Liczebność	3	4	1	4	6	18
	Procent	1,59	2,12	0,53	2,12	3,17	9,52
	Proc. wier.	16,67	22,22	5,56	22,22	33,33	
	Proc. kol.	20	30,77	1,79	7,02	12,5	
2	Liczebność	1	3	9	4	3	20
	Procent	0,53	1,59	4,76	2,12	1,59	10,58
	Proc. wier.	5	15	45	20	15	
	Proc. kol.	6,67	23,08	16,07	7,02	6,25	
3	Liczebność	5	1	16	21	11	54
	Procent	2,65	0,53	8,47	11,11	5,82	28,57
	Proc. wier.	9,26	1,85	29,63	38,89	20,37	
	Proc. kol.	33,33	7,69	28,57	36,84	22,92	
4	Liczebność	1	1	18	14	11	45
	Procent	0,53	0,53	9,52	7,41	5,82	23,81
	Proc. wier.	2,22	2,22	40	31,11	24,44	
	Proc. kol.	6,67	7,69	32,14	24,56	22,92	
5	Liczebność	5	4	12	14	17	52
	Procent	2,65	2,12	6,35	7,41	8,99	27,51
	Proc. wier.	9,62	7,69	23,08	26,92	32,69	
	Proc. kol.	33,33	30,77	21,43	24,56	35,42	
Razem	Liczebność	15	13	56	57	48	189
	Procent	7,94	6,88	29,63	30,16	25,4	100

Źródło: opracowanie własne.

Tabela 5.21. Statystyki dla tabeli PU_1B wg PG_1c

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**16**	**28,6942**	**0,0261**
Chi-kw. ilorazu wiarygodn.	**16**	**29,1299**	**0,0231**
Chi-kwadrat Mantela-Haenszela	1	2,1733	0,1404
Współczynnik FI		**0,3896**	
Współczynnik wielodzielczości		0,3631	
V Cramera		0,1948	

Źródło: opracowanie własne.

Wnioski:

1. W przypadku uwierzytelnień opartych o hasła oraz przedmioty, nie ma podstaw do odrzucenia hipotezy zerowej H^0_3; w przypadku uwierzytelnień biometrycznych należy odrzucić hipotezę zerową H^0_3 o niezależności badanych zmiennych, na korzyść hipotezy alternatywnej H^1_3 dla: redukcji ryzyka odpowiedzialności (np. karnej) oraz świadomością wypełnienia obowiązków, rozumianych jako korzyści z bezpiecznego stosowania tożsamości cyfrowej.
2. **Zależność 3**: Redukcja odpowiedzialności (np. karnej), wynikającej z bezpiecznego stosowania tożsamości cyfrowej wpływa na postrzegalną użyteczność uwierzytelnienia biometrycznego.
   Siła zależności 3: duża (test Chi^2; fi = 0,44).
3. **Zależność 4**: Świadomość dopełnienia obowiązków, poprzez bezpieczne stosowanie tożsamości cyfrowej, wpływa na postrzegalną użyteczność uwierzytelnienia biometrycznego.
   Siła zależności 4: dość duża (test Chi^2; fi = 0,39).

5.3.4. Badanie hipotezy statystycznej H4 (zależność ATU od PU)

Zbadano związek pomiędzy postrzeganą użytecznością bezpiecznego stosowania tożsamości cyfrowej (PU) a stosunkiem do uwierzytelnienia (ATU). Oba te czynniki rozpatrywano dla trzech metod uwierzytelnienia (tabela 5.22.).

Tabela 5.22. Współczynniki korelacji Spearmana (Rang Spearmana) PU i ATU

Współczynniki korelacji Spearmana			
Prawd. > |r| przy H0: Rho=0			
Liczba obserwacji			
	PU_1H	PU_1P	PU_1B
ATU_1H	-0,0751	0,04012	**r=0,14585**
	0,2921	0,5806	**p=0,0441**
	199	192	**n=191**
ATU_1P	0,0404	-0,1413	**r=-0,1753**
	0,575	0,0525	**p=0,0153**
	195	189	**n=191**
ATU_1B	0,01014	-0,0266	**r =-0,432**
	0,8881	0,7154	**p<0,0001**
	195	190	**n=191**

Źródło: opracowanie własne.

Nie wykazano zależności istotnej statystycznie między postrzeganą użytecznością bezpiecznego stosowania tożsamości cyfrowej z wykorzystaniem haseł i przedmiotów uwierzytelniających (odpowiednio PU_1H, PU_1P), a stosunkiem

do tych metod uwierzytelniania (odpowiednioATU_1H, ATU_1P) – obliczone prawdopodobieństwo p > 0,05 (vide tabela 5.22.).

Wykazano natomiast zależności istotne statystycznie między postrzeganiem użyteczności metod biometrycznych a stosunkiem do poszczególnych metod uwierzytelnienia (**p = 0,0441**; **p = 0,0153** oraz **p<0,0001**).

Przeprowadzono analizę z wykorzystaniem testu Chi^2 i wykryto:

1. Wysoko istotną statystycznie zależność (p = 0,002) między postrzeganą użytecznością bezpiecznego korzystania z haseł a stosunkiem do tych narzędzi uwierzytelnienia. Wyniki analizy zawarte są w tabelach 5.23. i 5.24.
2. Bardzo istotną statystycznie zależność (p < 0,0001) między postrzeganą użytecznością korzystania z biometrii a stosunkiem do tych narzędzi uwierzytelnienia. Wyniki analizy zawarte są w Tabelach 5.25 i 5.26.

Tabela 5.23. Analiza statystyczna liczności odpowiedzi ATU_1H wg PU_1H

Tabela ATU_1H wg PU_1H						
		ATU_1H				Razem
		1	2	3	4	
PU_1H						
2	Liczebność	0	6	3	1	10
	Procent	0	3,02	1,51	0,5	5,03
	Proc. wier.	0	60	30	10	
	Proc. kol.	0	5,26	5,56	100	
3	Liczebność	6	8	7	0	21
	Procent	3,02	4,02	3,52	0	10,55
	Proc. wier.	28,57	38,1	33,33	0	
	Proc. kol.	20	7,02	12,96	0	
4	Liczebność	9	41	21	0	71
	Procent	4,52	20,6	10,55	0	35,68
	Proc. wier.	12,68	57,75	29,58	0	
	Proc. kol.	30	35,96	38,89	0	
5	Liczebność	15	59	23	0	97
	Procent	7,54	29,65	11,56	0	48,74
	Proc. wier.	15,46	60,82	23,71	0	
	Proc. kol.	50	51,75	42,59	0	
Razem	Liczebność	30	114	54	1	199
	Procent	15,08	57,29	27,14	0,5	100

Źródło: opracowanie własne.

Tabela 5.24. Statystyki dla tabeli ATU_1H wg PU_1H

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**9**	**25,7059**	**0,0023**
Chi-kw. ilorazu wiarygodn.	**9**	**13,9481**	**0,1242**
Chi-kwadrat Mantela-Haenszela	1	1,7512	0,1857
Współczynnik FI		**0,3594**	
Współczynnik wielodzielczości		0,3382	
V Cramera		0,2075	

Źródło: opracowanie własne

Tabela 5.25. Analiza statystyczna liczności odpowiedzi ATU_1B wg PU_1B

Tabela PU_3B wg ATU_3B						
PU_3B		ATU_3B				Razem
		1	2	3	4	
1	Liczebność	2	0	5	11	18
	Procent	1,05	0	2,62	5,76	9,42
	Proc. wier.	11,11	0	27,78	61,11	
	Proc. kol.	8,7	0	6,1	30,56	
2	Liczebność	0	5	10	5	20
	Procent	0	2,62	5,24	2,62	10,47
	Proc. wier.	0	25	50	25	
	Proc. kol.	0	10	12,2	13,89	
3	Liczebność	1	9	37	8	55
	Procent	0,52	4,71	19,37	4,19	28,8
	Proc. wier.	1,82	16,36	67,27	14,55	
	Proc. kol.	4,35	18	45,12	22,22	
4	Liczebność	4	17	19	6	46
	Procent	2,09	8,9	9,95	3,14	24,08
	Proc. wier.	8,7	36,96	41,3	13,04	
	Proc. kol.	17,39	34	23,17	16,67	
5	Liczebność	16	19	11	6	52
	Procent	8,38	9,95	5,76	3,14	27,23
	Proc. wier.	30,77	36,54	21,15	11,54	
	Proc. kol.	69,57	38	13,41	16,67	
Razem	Liczebność	23	50	82	36	191
	Procent	12,04	26,18	42,93	18,85	100

Źródło: opracowanie własne.

Tabela 5.26. Statystyki dla tabeli ATU_1B wg PU_1B

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**12**	**68,5426**	**<0,0001**
Chi-kw. ilorazu wiarygodn.	**12**	**67,9303**	**<0,0001**
Chi-kwadrat Mantela-Haenszela	1	34,7981	<0,0001
Współczynnik FI		**0,5991**	
Współczynnik wielodzielczości		0,5139	
V Cramera		0,3459	

Źródło: opracowanie własne.

Wnioski:

1. W przypadku uwierzytelnień opartych o przedmioty uwierzytelniające nie ma podstaw do odrzucenia hipotezy zerowej H^0_4; w przypadku uwierzytelnień opartych o hasła i biometrię należy odrzucić hipotezę zerową H^0_4 o niezależności badanych zmiennych, na korzyść hipotezy alternatywnej H^1_4.
2. **Zależność 5**: im lepsze postrzeganie użyteczności haseł, tym bardziej negatywny stosunek do uwierzytelnienia biometrycznego – dodatni współczynnik korelacji.
   Siła zależności 5: mała (test Spearmana; r = 0,15).
3. **Zależność 6**: im lepsze postrzeganie użyteczności przedmiotów uwierzytelniających, tym mniej negatywny stosunek do uwierzytelnienia biometrycznego – ujemny współczynnik korelacji.
   Siła zależności 6: mała (test Spearmana; r = -0,18).
4. **Zależność 7**: im lepsze postrzeganie użyteczności uwierzytelnienia biometrycznego, tym mniej negatywny stosunek do uwierzytelnienia biometrycznego – ujemny współczynnik korelacji.
   Siła zależności 7: dość duża (test Spearmana; r = -0,4); duża (test Chi^2; fi = 0,6).
5. **Zależność 8**: istnieje zależność między postrzegana użytecznością bezpiecznego stosowania haseł a stosunkiem do haseł.
   Siła zależności 8: dość duża (test Chi^2; fi = 0,36).

5.3.5. Badanie hipotezy statystycznej H5 (zależność BI od ATU)

Zbadano związek pomiędzy stosunkiem do metod uwierzytelnienia (ATU) a ich chęcią stosowania w sposób bezpieczny (BI). Oba te czynniki rozpatrywano dla trzech metod uwierzytelnienia (tabela 5.27.).

Tabela 5.27. Współczynniki korelacji Spearmana (Rang Spearmana) ATU i BI

Współczynniki korelacji Spearmana			
Prawd. > |r| przy H0: Rho=0			
Liczba obserwacji			
	ATU_1H	ATU_1P	ATU_1B
BI_1H	0,11814	**r = 0,14473**	0,03185
	0,0982	**p = 0,0452**	0,661
	197	**n = 192**	192
BI_1P	-0,0381	**r = 0,42773**	**r = 0,20542**
	0,5994	**p <0,0001**	**p = 0,0044**
	193	**n = 192**	**n = 191**
BI_1B	0,01217	**r = 0,17254**	**r = 0,42293**
	0,8673	**p = 0,0173**	**p <0,0001**
	191	**n = 190**	**n = 190**

Źródło: opracowanie własne.

Nie wykazano zależności istotnej statystycznie między stosunkiem do haseł (ATU_1H) a chęcią stosowania uwierzytelnienia w sposób bezpieczny (BI_1H, BI_1P, BI_1B) – obliczone prawdopodobieństwo p > 0,05 (vide tabela 5.27.).

Wykazano natomiast zależności istotne i bardzo istotne statystycznie między:

1. Stosunkiem do przedmiotów uwierzytelniających (ATU_1P) a chęcią stosowania uwierzytelnienia w sposób bezpieczny (BI_1H, BI_1P, BI_1B), w szczególności z wykorzystaniem przedmiotów (odpowiednio **p = 0,05**; **p < 0,0001**; **p = 0,02**).
2. Stosunkiem do uwierzytelnienia biometrycznego (ATU_1B) a chęcią stosowania przedmiotów uwierzytelniających w sposób bezpieczny (BI_1P; **p = 0,004**).
3. Stosunkiem do uwierzytelnienia biometrycznego (ATU_1B) a chęcią stosowania biometrycznej metody uwierzytelnienia (BI_1B; **p < 0,0001**).

Przeprowadzono analizę z wykorzystaniem testu Chi^2 i wykryto:

1. Istotną statystycznie zależność (**p < 0,0001**) między stosunkiem do haseł a chęcią stosowania haseł w sposób bezpieczny. Wyniki analizy zawarte są w tabelach 5.28. i 5.29.
2. Istotną statystycznie zależność (**p < 0,0001**) między stosunkiem do przedmiotów uwierzytelniających a chęcią stosowania tych narzędzi w sposób bezpieczny. Wyniki analizy zawarte są w tabelach 5.30. i 5.31.
3. Istotną statystycznie zależność (**p = 0,043**) między stosunkiem do przedmiotów uwierzytelniających a chęcią stosowania biometrii. Wyniki analizy zawarte są w tabelach 5.32. i 5.33.

4. Istotną statystycznie zależność (**p = 0,005**) między stosunkiem do uwierzytelnienia biometrycznego a chęcią stosowania przedmiotów uwierzytelniających. Wyniki analizy zawarte są w tabelach 5.34. i 5.35.
5. Istotną statystycznie zależność (**p < 0,0001**) między stosunkiem do uwierzytelnienia biometrycznego a chęcią jego stosowania. Wyniki analizy zawarte są w tabelach 5.36. i 5.37.

Tabela 5.28. Analiza statystyczna liczności odpowiedzi BI_1H wg ATU_1H

Tabela BI_1H wg ATU_1H						
BI_1H		ATU_1H				Razem
		1	2	3	4	
1	Liczebność	28	111	48	0	187
	Procent	14,21	56,35	24,37	0	94,92
	Proc. wier.	14,97	59,36	25,67	0	
	Proc. kol.	93,33	98,23	90,57	0	
2	Liczebność	0	1	1	1	3
	Procent	0	0,51	0,51	0,51	1,52
	Proc. wier.	0	33,33	33,33	33,33	
	Proc. kol.	0	0,88	1,89	100	
3	Liczebność	2	1	4	0	7
	Procent	1,02	0,51	2,03	0	3,55
	Proc. wier.	28,57	14,29	57,14	0	
	Proc. kol.	6,67	0,88	7,55	0	
Razem	Liczebność	30	113	53	1	197
	Procent	15,23	57,36	26,9	0,51	100

Źródło: opracowanie własne.

Tabela 5.29. Statystyki dla tabeli BI_1H wg ATU_1H

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**6**	**71,1776**	**<0,0001**
Chi-kw. ilorazu wiarygodn.	**6**	**15,6182**	**0,016**
Chi-kwadrat Mantela-Haenszela	1	1,8566	0,173
Współczynnik FI		**0,6011**	
Współczynnik wielodzielczości		0,5152	
V Cramera		0,425	

Źródło: opracowanie własne.

Tabela 5.30. Analiza statystyczna liczności odpowiedzi BI_1P wg ATU_1P

Tabela BI_1P wg ATU_1P						
BI_1P		ATU_1P				Razem
		1	2	3	4	
1	Liczebność	16	73	53	4	146
	Procent	8,33	38,02	27,6	2,08	76,04
	Proc. wier.	10,96	50	36,3	2,74	
	Proc. kol.	100	91,25	64,63	28,57	
2	Liczebność	0	5	8	7	20
	Procent	0	2,6	4,17	3,65	10,42
	Proc. wier.	0	25	40	35	
	Proc. kol.	0	6,25	9,76	50	
3	Liczebność	0	2	21	3	26
	Procent	0	1,04	10,94	1,56	13,54
	Proc. wier.	0	7,69	80,77	11,54	
	Proc. kol.	0	2,5	25,61	21,43	
Razem	Liczebność	16	80	82	14	192
	Procent	8,33	41,67	42,71	7,29	100

Źródło: opracowanie własne.

Tabela 5.31. Statystyki dla tabeli BI_1P wg ATU_1P

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**6**	**52,1171**	**<0,0001**
Chi-kw. ilorazu wiarygodn.	**6**	**48,8857**	**<0,0001**
Chi-kwadrat Mantela-Haenszela	1	30,2815	<0,0001
Współczynnik FI		**0,521**	
Współczynnik wielodzielczości		0,4621	
V Cramera		0,3684	

Źródło: opracowanie własne.

Tabela 5.32. Analiza statystyczna liczności odpowiedzi BI_1B wg ATU_1P

Tabela BI_1B wg ATU_1P						
BI_1B		ATU_P				Razem
		1	2	3	4	
0	Liczebność	0	0	1	0	1
	Procent	0	0	0,53	0	0,53
	Proc. wier.	0	0	100	0	
	Proc. kol.	0	0	1,22	0	
1	Liczebność	12	54	51	3	120
	Procent	6,32	28,42	26,84	1,58	63,16
	Proc. wier.	10	45	42,5	2,5	
	Proc. kol.	75	69,23	62,2	21,43	
2	Liczebność	0	13	12	5	30
	Procent	0	6,84	6,32	2,63	15,79
	Proc. wier.	0	43,33	40	16,67	
	Proc. kol.	0	16,67	14,63	35,71	
3	Liczebność	4	11	18	6	39
	Procent	2,11	5,79	9,47	3,16	20,53
	Proc. wier.	10,26	28,21	46,15	15,38	
	Proc. kol.	25	14,1	21,95	42,86	
Razem	Liczebność	16	78	82	14	190
	Procent	8,42	41,05	43,16	7,37	100

Źródło: opracowanie własne.

Tabela 5.33. Statystyki dla tabeli BI_1B wg ATU_1P

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**9**	**17,3598**	**0,0434**
Chi-kw. ilorazu wiarygodn.	**9**	**19,9818**	**0,018**
Chi-kwadrat Mantela-Haenszela	1	5,5841	0,0181
Współczynnik FI		**0,3023**	
Współczynnik wielodzielczości		0,2893	
V Cramera		0,1745	

Źródło: opracowanie własne.

Tabela 5.34. Analiza statystyczna liczności odpowiedzi BI_1P wg ATU_1B

Tabela BI_1P wg ATU_1B						
BI_1P		ATU_1B				Razem
		1	2	3	4	
1	Liczebność	19	43	59	24	145
	Procent	9,95	22,51	30,89	12,57	75,92
	Proc. wier.	13,1	29,66	40,69	16,55	
	Proc. kol.	82,61	91,49	71,08	63,16	
2	Liczebność	1	3	7	9	20
	Procent	0,52	1,57	3,66	4,71	10,47
	Proc. wier.	5	15	35	45	
	Proc. kol.	4,35	6,38	8,43	23,68	
3	Liczebność	3	1	17	5	26
	Procent	1,57	0,52	8,9	2,62	13,61
	Proc. wier.	11,54	3,85	65,38	19,23	
	Proc. kol.	13,04	2,13	20,48	13,16	
Razem	Liczebność	23	47	83	38	191
	Procent	12,04	24,61	43,46	19,9	100

Źródło: opracowanie własne.

Tabela 5.35. Statystyki dla tabeli BI_1P wg ATU_1B

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**6**	**18,3883**	**0,0053**
Chi-kw. ilorazu wiarygodn.	**6**	**19,1823**	**0,0039**
Chi-kwadrat Mantela-Haenszela	1	5,2321	0,0222
Współczynnik FI		**0,3103**	
Współczynnik wielodzielczości		0,2963	
V Cramera		0,2194	

Źródło: opracowanie własne.

Tabela 5.36. Analiza statystyczna liczności odpowiedzi BI_1B wg ATU_1B

Tabela BI_1B wg ATU_1B						
BI_1B		ATU_1B				Razem
		1	2	3	4	
0	Liczebność	0	0	1	0	1
	Procent	0	0	0,53	0	0,53
	Proc. wier.	0	0	100	0	
	Proc. kol.	0	0	1,2	0	
1	Liczebność	22	42	44	12	120
	Procent	11,58	22,11	23,16	6,32	63,16
	Proc. wier.	18,33	35	36,67	10	
	Proc. kol.	95,65	89,36	53,01	32,43	
2	Liczebność	0	3	10	17	30
	Procent	0	1,58	5,26	8,95	15,79
	Proc. wier.	0	10	33,33	56,67	
	Proc. kol.	0	6,38	12,05	45,95	
3	Liczebność	1	2	28	8	39
	Procent	0,53	1,05	14,74	4,21	20,53
	Proc. wier.	2,56	5,13	71,79	20,51	
	Proc. kol.	4,35	4,26	33,73	21,62	
Razem	Liczebność	23	47	83	37	190
	Procent	12,11	24,74	43,68	19,47	100

Źródło: opracowanie własne.

Tabela 5.37. Statystyki dla tabeli BI_1B wg ATU_1B

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**9**	**61,5104**	**<0,0001**
Chi-kw. ilorazu wiarygodn.	**9**	**62,3957**	**<0,0001**
Chi-kwadrat Mantela-Haenszela	1	26,7979	<0,0001
Współczynnik FI		**0,569**	
Współczynnik wielodzielczości		0,4945	
V Cramera		0,3285	

Źródło: opracowanie własne.

Wnioski:

1. Należy odrzucić hipotezę zerową H^0_5 o niezależności badanych zmiennych, na korzyść hipotezy alternatywnej H^1_5.
2. **Zależność 9**: im bardziej pozytywny stosunek do uwierzytelnienia za pomocą przedmiotu, tym większa chęć bezpiecznego stosowania uwierzytelnienia w ogóle –-dodatni współczynnik korelacji.

   Siła zależności 9: słaba dla uwierzytelnienia za pomocą haseł (test Spearmana; r = 0,15), duża dla uwierzytelnienia za pomocą przedmiotów (test Spearmana; r = 0,43; test Chi^2; fi = 0,52) i słaba dla uwierzytelnienia z użyciem biometrii (test Spearmana; r = 0,18, test Chi^2; fi = 0,30).
3. **Zależność 10**: im bardziej pozytywny stosunek do uwierzytelnienia biometrycznego, tym większa chęć bezpiecznego stosowania uwierzytelnienia z użyciem przedmiotu oraz biometrii – dodatni współczynnik korelacji.

   Siła zależności 10: dość duża dla uwierzytelnienia za pomocą przedmiotów (test Spearmana; r = 0,21; test Chi^2; fi = 0,31) i duża dla uwierzytelnienia z użyciem biometrii (test Spearmana; r = 0,42; test Chi^2; fi = 0,60).
4. **Zależność 11**: Pozytywny stosunek do uwierzytelnienia z użyciem haseł, wpływa na chęć bezpiecznego stosowania uwierzytelnienia z użyciem haseł.

   Siła zależności 11: duża (test Chi^2; fi = 0,60).

5.3.6. Badanie hipotezy statystycznej H6 (zależność ATU od PEOU)

Zbadano związek między postrzeganą łatwością bezpiecznego stosowania tożsamości cyfrowych (PEOU) a stosunkiem respondentów do tożsamości cyfrowych (ATU). Oba te czynniki rozpatrywano dla trzech metod uwierzytelnienia (tabela 5.38.).

Tabela 5.38. Współczynniki korelacji Spearmana (Rang Spearmana) PEOU i ATU

Współczynniki korelacji Spearmana			
Prawd. > |r| przy H0: Rho=0			
Liczba obserwacji			
	ATU_1H	ATU_1P	ATU_1B
PEOU_1H	0,04113	-0,04275	-0,07182
	0,5641	0,5529	0,3184
	199	195	195
PEOU_1P	0,01408	**r = 0,1831**	0,06893
	0,8443	**p = 0,0104**	0,3396
	197	**n = 195**	194
PEOU_1B	-0,06616	0,04603	**r = 0,25563**
	0,3544	0,5239	**p = 0,0003**
	198	194	**n = 194**

Źródło: opracowanie własne.

Nie wykazano zależności istotnej statystycznie między postrzeganą łatwością bezpiecznego stosowania tożsamości cyfrowej z wykorzystaniem haseł (PEOU_1H), a stosunkiem do tożsamości cyfrowej (ATU) – obliczane prawdopodobieństwo p > 0,05 (vide tabela 5.38.).

Wykazano niezbyt dużą zależność (obliczone **p = 0,01** < 0,05) między postrzeganą łatwością bezpiecznego użycia przedmiotów (PEOU_1P), a stosunkiem do uwierzytelnień z użyciem przedmiotów (ATU_1P). Tę zależność wykazano również z użyciem testu Chi kwadrat (tabela 5.39. i tabela 5.40.) – obliczone prawdopodobieństwo **p = 0,0012**.

Wykazano zależność istotną statystycznie (**p = 0,0003**) między postrzeganą łatwością użycia biometrii (PEOU_1B), a stosunkiem do uwierzytelnień biometrycznych (ATU_1B). Potwierdza to badanie z wykorzystaniem testu Chi kwadrat (tabela 5.41. i tabela 5.42.) – obliczone prawdopodobieństwo **p < 0,0001**.

Tabela 5.39. Analiza statystyczna liczności odpowiedzi ATU_1P wg PEOU_1P

Tabela PEOU_1P wg ATU_1P						
PEOU_1P		ATU_1P				Razem
		1	2	3	4	
		0	0	5	0	5
0	Liczebność					
	Procent	0	0	2,56	0	2,56
	Proc. wier.	0	0	100	0	
	Proc. kol.	0	0	6,1	0	
1	Liczebność	6	11	9	3	29
	Procent	3,08	5,64	4,62	1,54	14,87
	Proc. wier.	20,69	37,93	31,03	10,34	
	Proc. kol.	37,5	13,25	10,98	21,43	
2	Liczebność	3	40	19	1	63
	Procent	1,54	20,51	9,74	0,51	32,31
	Proc. wier.	4,76	63,49	30,16	1,59	
	Proc. kol.	18,75	48,19	23,17	7,14	
3	Liczebność	4	19	28	3	54
	Procent	2,05	9,74	14,36	1,54	27,69
	Proc. wier.	7,41	35,19	51,85	5,56	
	Proc. kol.	25	22,89	34,15	21,43	
4	Liczebność	2	7	15	3	27
	Procent	1,03	3,59	7,69	1,54	13,85
	Proc. wier.	7,41	25,93	55,56	11,11	
	Proc. kol.	12,5	8,43	18,29	21,43	
5	Liczebność	1	6	6	4	17
	Procent	0,51	3,08	3,08	2,05	8,72
	Proc. wier.	5,88	35,29	35,29	23,53	
	Proc. kol.	6,25	7,23	7,32	28,57	
Razem	Liczebność	16	83	82	14	195
	Procent	8,21	42,56	42,05	7,18	100

Źródło: opracowanie własne.

Tabela 5.40. Statystyki dla tabeli ATU_1P wg PEOU_1P

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**15**	**38,5739**	**0,0007**
Chi-kw. ilorazu wiarygodn.	**15**	**37,2735**	**0,0012**
Chi-kwadrat Mantela-Haenszela	1	5,5935	0,018
Współczynnik FI		**0,4448**	
Współczynnik wielodzielczości		0,4064	
V Cramera		0,2568	

Źródło: opracowanie własne.

Tabela 5.41. Analiza statystyczna liczności odpowiedzi ATU_1B wg PEOU_1B

Tabela PEOU_1B wg ATU_1B						
PEOU_1B		ATU_1B				Razem
		1	2	3	4	
0	Liczebność	0	3	9	4	16
	Procent	0	1,55	4,64	2,06	8,25
	Proc. wier.	0	18,75	56,25	25	
	Proc. kol.	0	6	10,71	10,53	
1	Liczebność	8	13	8	4	33
	Procent	4,12	6,7	4,12	2,06	17,01
	Proc. wier.	24,24	39,39	24,24	12,12	
	Proc. kol.	36,36	26	9,52	10,53	
2	Liczebność	3	16	20	5	44
	Procent	1,55	8,25	10,31	2,58	22,68
	Proc. wier.	6,82	36,36	45,45	11,36	
	Proc. kol.	13,64	32	23,81	13,16	
3	Liczebność	10	15	22	8	55
	Procent	5,15	7,73	11,34	4,12	28,35
	Proc. wier.	18,18	27,27	40	14,55	
	Proc. kol.	45,45	30	26,19	21,05	
4	Liczebność	1	3	16	6	26
	Procent	0,52	1,55	8,25	3,09	13,4
	Proc. wier.	3,85	11,54	61,54	23,08	
	Proc. kol.	4,55	6	19,05	15,79	
5	Liczebność	0	0	9	11	20
	Procent	0	0	4,64	5,67	10,31
	Proc. wier.	0	0	45	55	
	Proc. kol.	0	0	10,71	28,95	
Razem	Liczebność	22	50	84	38	194
	Procent	11,34	25,77	43,3	19,59	100

Źródło: opracowanie własne.

Tabela 5.42. Statystyki dla tabeli ATU_1B wg PEOU_1B

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**15**	**47,0826**	**<0,0001**
Chi-kw. ilorazu wiarygodn.	**15**	**51,81**	**<0,0001**
Chi-kwadrat Mantela-Haenszela	1	11,5371	0,0007
Współczynnik FI		**0,4926**	
Współczynnik wielodzielczości		0,4419	
V Cramera		0,2844	

Źródło: opracowanie własne.

Badanie z wykorzystaniem testu Chi kwadrat wykazuje zależność między łatwością użycia przedmiotów, a stosunkiem do uwierzytelnienia z wykorzystaniem biometrii (tabela 5.43. i tabela 5.44.) – obliczone prawdopodobieństwo **p = 0,0008**.

Tabela 5.43. Analiza statystyczna liczności odpowiedzi ATU_1B wg PEOU_1P

Tabela PEOU_1P wg ATU_1B						
PEOU_1P		ATU_1B				Razem
		1	2	3	4	
0	Liczebność	0	0	5	0	5
	Procent	0	0	2,58	0	2,58
	Proc. wier.	0	0	100	0	
	Proc. kol.	0	0	5,95	0	
1	Liczebność	3	10	14	2	29
	Procent	1,55	5,15	7,22	1,03	14,95
	Proc. wier.	10,34	34,48	48,28	6,9	
	Proc. kol.	13,04	20	16,67	5,41	
2	Liczebność	5	20	25	13	63
	Procent	2,58	10,31	12,89	6,7	32,47
	Proc. wier.	7,94	31,75	39,68	20,63	
	Proc. kol.	21,74	40	29,76	35,14	
3	Liczebność	5	17	24	8	54
	Procent	2,58	8,76	12,37	4,12	27,84
	Proc. wier.	9,26	31,48	44,44	14,81	
	Proc. kol.	21,74	34	28,57	21,62	
4	Liczebność	4	3	12	7	26
	Procent	2,06	1,55	6,19	3,61	13,4
	Proc. wier.	15,38	11,54	46,15	26,92	
	Proc. kol.	17,39	6	14,29	18,92	
5	Liczebność	6	0	4	7	17
	Procent	3,09	0	2,06	3,61	8,76
	Proc. wier.	35,29	0	23,53	41,18	
	Proc. kol.	26,09	0	4,76	18,92	
Razem	Liczebność	23	50	84	37	194
	Procent	11,86	25,77	43,3	19,07	100

Źródło: opracowanie własne.

Tabela 5.44. Statystyki dla tabeli ATU_1B wg PEOU_1P

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**15**	**34,7104**	**0,0027**
Chi-kw. ilorazu wiarygodn.	**15**	**38,5138**	**0,0008**
Chi-kwadrat Mantela-Haenszela	1	0,2586	0,6111
Współczynnik FI		**0,423**	
Współczynnik wielodzielczości		0,3896	
V Cramera		0,2442	

Źródło: opracowanie własne.

Wnioski:

1. W przypadku uwierzytelnień opartych o hasła nie ma podstaw do odrzucenia hipotezy zerowej H^0_6; w przypadku uwierzytelnień w oparciu o przedmioty i biometrię należy odrzucić hipotezę zerową H^0_6 o niezależności badanych zmiennych, na korzyść hipotezy alternatywnej H^1_6.
2. **Zależność 12**: im korzystanie z przedmiotów uwierzytelniających jest postrzegane jako trudniejsze, tym bardziej negatywna postawa wobec uwierzytelnienia z użyciem przedmiotów – dodatni współczynnik korelacji.

   Siła zależności 12: słaba (wg badania korelacji Rang Spearmana; r = 0,18).
3. **Zależność 13**: im korzystanie z uwierzytelnienia biometrycznego jest postrzegane jako trudniejsze, tym bardziej negatywna postawa wobec uwierzytelnienia z użyciem biometrii - dodatni współczynnik korelacji.

   Siła zależności 13: niezbyt duża (wg badania korelacji Rang Spearmana; r = 0,26).

5.3.7. Badanie hipotezy statystycznej H7 (zależność FP od ATU)

Zbadano związek pomiędzy postrzeganiem wymuszenia (FP), a stosunkiem do metod uwierzytelnienia (ATU) i nie wykazano zależności istotnej statystycznie za pomocą testu Spearmana (tabela 5.45.).

Tabela 5.45. Współczynniki korelacji Spearmana (Rang Spearmana) PU i ATU

Współczynniki korelacji Spearmana					
Prawd. > |r| przy H0: Rho=0					
Liczba obserwacji					
	FP_1a	FP_1b	FP_1c	FP_1d	FP_1e
ATU_1H	0,09563	-0,118	-0,0516	0,09952	-0,041
	0,1882	0,1042	0,4784	0,1708	0,5734
	191	191	191	191	191
ATU_1P	-0,0365	-0,0996	0,01347	0,04419	-0,0202
	0,6207	0,1762	0,8552	0,5493	0,7839
	186	186	186	186	186
ATU_1B	0,08174	-0,0382	0,01329	0,0361	-0,0558
	0,2674	0,6052	0,8571	0,6247	0,4495
	186	186	186	186	186

Źródło: opracowanie własne.

Przeprowadzono analizę z wykorzystaniem testu Chi^2 i wykryto:

1. Zależność (**p = 0,02**) między konkretnymi działaniami przełożonego (FP_1d) a stosunkiem do haseł (ATU_1H). Wyniki analizy zawarte są w tabelach 5.46. i 5.47.

Tabela 5.46. Analiza statystyczna liczności odpowiedzi ATU_1H wg FP_1d

Tabela ATU_1H wg FP 1d						
FP_1d		ATU_1H				Razem
		1	2	3	4	
0	Liczebność	29	92	46	0	167
	Procent	15,18	48,17	24,08	0	87,43
	Proc. wier.	17,37	55,09	27,54	0	
	Proc. kol.	96,67	85,98	86,79	0	
1	Liczebność	1	15	7	1	24
	Procent	0,52	7,85	3,66	0,52	12,57
	Proc. wier.	4,17	62,5	29,17	4,17	
	Proc. kol.	3,33	14,02	13,21	100	
Razem	Liczebność	30	107	53	1	191
	Procent	15,71	56,02	27,75	0,52	100

Źródło: opracowanie własne.

Tabela 5.47. Statystyki dla tabeli ATU_1H wg FP_1d

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**3**	**9,5113**	**0,0232**
Chi-kw. ilorazu wiarygodn.	**3**	**7,5353**	**0,0567**
Chi-kwadrat Mantela-Haenszela	1	2,5528	0,1101
Współczynnik FI		**0,2232**	
Współczynnik wielodzielczości		0,2178	
V Cramera		0,2232	

Źródło: opracowanie własne.

Wnioski:

1. Należy odrzucić hipotezę zerową H^0_7 dotyczącą niezależności stosunku do uwierzytelnień za pomocą haseł od działań przełożonych, na korzyść hipotezy alternatywnej H^1_7. W pozostałych przypadkach nie ma podstaw do odrzucenia hipotezy H^0_7.
2. **Zależność 14**: Konkretne działania przełożonego wpływają na stosunek respondenta do haseł.
   Siła zależności 14: niezbyt duża (test Chi^2; r = 0,22).

5.3.8. Badanie hipotezy statystycznej H8 (zależność ATU od TA)

Zbadano związek pomiędzy świadomością zagrożeń (TA), a stosunkiem do tożsamości cyfrowych (ATU). Zarówno analiza z użyciem korelacji rang Spearmana, jak i testu Chi kwadrat nie wykazała związku istotnego statystycznie (tabela 5.48.).

Tabela 5.48. Współczynniki korelacji Spearmana (Rang Spearmana) ATU i TA

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	TA
ATU 1H	0,02177
	0,8158
	117
ATU 2P	0,02742
	0,7721
	114
ATU 3B	0,03257
	0,7308
	114

Źródło: opracowanie własne.

Wnioski:

1. Nie ma podstaw do odrzucenia hipotezy zerowej H^0_8 o niezależności badanych zmiennych, na korzyść hipotezy alternatywnej H^1_8.

5.3.9. Badanie hipotezy statystycznej H9 (zależność PEOU od DIC)

Zbadano związek pomiędzy postrzeganą łatwością użycia tożsamości cyfrowych w sposób bezpieczny (PEOU) i charakterystyką tożsamości cyfrowej (DIC) dla uwierzytelnień za pomocą haseł i przedmiotów (tabela 5.49.). W przypadku uwierzytelnienia biometrycznego liczba obserwacji nie pozwalała na przeprowadzenie wiarygodnych obliczeń statystycznych.

Tabela 5.49. Współczynniki korelacji Spearmana (Rang Spearmana) PEOU_1H i DIC w rozbiciu na pytania

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	PEOU_1H
DIC_1H	**r = -0,29685**
	p <0,0001
	n = 183
DIC_2Ha	-0,01256
	0,8829
	140
DIC_2Hb	-0,10607
	0,209
	142
DIC_2Hc	-0,00983
	0,9076
	142
DIC_2Hd	**r = -0,27032**
	p = 0,0011
	n = 142
DIC_3H	0,04441
	0,543
	190
DIC_4H	0,07988
	0,272
	191

Źródło: opracowanie własne.

W przypadku uwierzytelnień z wykorzystaniem haseł wykryto dwie zależności istotne statystycznie. Według testu Spearmana na postrzeganie łatwości stosowania haseł (PEOU_1H) wpływają: długość hasła (DIC_1H) z **p < 0,0001** oraz stosowanie w hasłach znaków specjalnych (DIC_2Hd).

Według testu Chi kwadrat istnieje zależność między postrzeganiem łatwości stosowania haseł (PEOU_1H) i stosowaniem w haśle znaków specjalnych (DIC_2Hd) z **p = 0,004** (tabela 5.50. i tabela 5.51.).

Tabela 5.50. Analiza statystyczna liczności odpowiedzi PEOU_1H wg DIC_2Hd

Tabela DIC_2Hd wg PEOU_1H							
DIC_2Hd		PEOU_1H					Razem
		1	2	3	4	5	
0	Liczebność	2	14	28	23	14	81
	Procent	1,41	9,86	19,72	16,2	9,86	57,04
	Proc. wier.	2,47	17,28	34,57	28,4	17,28	
	Proc. kol.	18,18	45,16	57,14	79,31	63,64	
1	Liczebność	9	17	21	6	8	61
	Procent	6,34	11,97	14,79	4,23	5,63	42,96
	Proc. wier.	14,75	27,87	34,43	9,84	13,11	
	Proc. kol.	81,82	54,84	42,86	20,69	36,36	
Razem	Liczebność	11	31	49	29	22	142
	Procent	7,75	21,83	34,51	20,42	15,49	100

Źródło: opracowanie własne.

Tabela 5.51. Statystyki dla tabeli PEOU_1H wg DIC_2Hd

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**4**	**14,8239**	**0,0051**
Chi-kw. ilorazu wiarygodn.	**4**	**15,5766**	**0,0036**
Chi-kwadrat Mantela-Haenszela	1	9,9857	0,0016
Współczynnik FI		**0,3231**	
Współczynnik wielodzielczości		0,3075	
V Cramera		0,3231	

Źródło: opracowanie własne.

Wykryto również zależność między postrzeganą łatwością bezpiecznego użycia przedmiotu (PEOU_1P) a stosowaniem tokenu – aplikacji na komórkę z **p = 0,017** (tabela 5.52. i tabela 5.53.).

Tabela 5.52. Analiza statystyczna liczności odpowiedzi PEOU_1P wg DIC_5Pf

Tabela DIC_5Pf wg PEOU_1P								
DIC_5Pf		PEOU_1P						Razem
		0	1	2	3	4	5	
0	Liczebność	2	12	32	17	13	4	80
	Procent	2,11	12,63	33,68	17,89	13,68	4,21	84,21
	Proc. wier.	2,5	15	40	21,25	16,25	5	
	Proc. kol.	100	100	80	70,83	100	100	
1	Liczebność	0	0	8	7	0	0	15
	Procent	0	0	8,42	7,37	0	0	15,79
	Proc. wier.	0	0	53,33	46,67	0	0	
	Proc. kol.	0	0	20	29,17	0	0	
Razem	Liczebność	2	12	40	24	13	4	95
	Procent	2,11	12,63	42,11	25,26	13,68	4,21	100

Źródło: opracowanie własne.

Tabela 5.53. Statystyki dla tabeli PEOU_1P wg DIC_5Pf

Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**5**	**9,5759**	**0,0882**
Chi-kw. ilorazu wiarygodn.	**5**	**13,8641**	**0,0165**
Chi-kwadrat Mantela-Haenszela	1	0,0047	0,9454
Współczynnik FI		**0,3175**	
Współczynnik wielodzielczości		0,3026	
V Cramera		0,3175	

Źródło: opracowanie własne.

Wnioski:

1. Należy odrzucić hipotezę zerową H^0_9 dotyczącą niezależności postrzeganej łatwości bezpiecznego stosowania tożsamości cyfrowych od charakterystyki uwierzytelnień za pomocą haseł, na korzyść hipotezy alternatywnej H^1_9. W pozostałych przypadkach nie ma podstaw do odrzucenia hipotezy H^0_9.
2. **Zależność 15**: im dłuższe hasło tym mniejsza postrzegana łatwość użycia haseł w sposób bezpieczny – korelacja ujemna.
   Siła zależności 15: dość duża (test Spearmana; r = -0,3).
3. **Zależność 16**: konieczność stosowania znaków specjalnych obniża postrzeganą łatwość użycia haseł w sposób bezpieczny – korelacja ujemna.
   Siła zależności 16: dość duża (test Spearmana; r = -0,27).

5.3.10. Badanie hipotezy statystycznej H10 (zależność TA od UC)

Zbadano związek pomiędzy samooceną wiedzy (UC_4) a świadomością zagrożeń (TA). Zarówno analiza z użyciem korelacji rang Spearmana jak i testu Chi kwadrat nie wykazała związku istotnego statystycznie. Dodatkowo zbadano, czy istnieje zależność między innymi charakterystykami użytkownika (UC) a świadomością zagrożeń. Nie wykryto takiej zależności. (tabela 5.54.)

Tabela 5.54. Współczynniki korelacji Spearmana (Rang Spearmana) UC i TA

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	TA
UC_3	-0,08495
	0,3798
	109
UC_4	-0,1196
	0,2155
	109
UC_6	0,08478
	0,3572
	120
UC_7	0,15033
	0,0998
	121
UC_8	0,11225
	0,2222
	120

Źródło: opracowanie własne.

Wnioski:

1. Nie ma podstaw do odrzucenia hipotezy zerowej H^0_{10} o niezależności badanych zmiennych, na korzyść hipotezy alternatywnej $H^1_{10.}$

5.3.11. Badanie hipotezy statystycznej H11 (zależność PG od MF)

Zbadano związek pomiędzy postrzeganymi korzyściami z bezpiecznego stosowania tożsamości cyfrowej (PG) a czynnikami zarządczymi (MF). Związek został zbadany zarówno pomiędzy zmiennymi reprezentującymi poszczególne pytania, jak i utworzonymi wskaźnikami (tabela 5.55.).

Tabela 5.55. Współczynniki korelacji Spearmana (Rang Spearmana) PG i MF w rozbiciu na pytania

Współczynniki korelacji Spearmana					
Prawd. > |r| przy H0: Rho=0					
Liczba obserwacji					
	PG_1a	PG_1b	PG_1c	PG_1d	PG_1e
MF_1a	**r = 0.29049**	0,13466	0,13625	0,12211	**r = 0,19949**
	p = <.0001	0,0586	0,0563	0,0866	**p = 0,0047**
	n = 199	198	197	198	**n = 199**
MF_1b	**r = 0,19059**	**r = 0,1719**	0,01346	**r = 0,14416**	0,10668
	p = 0,007	**p = 0,0155**	0,8511	**p = 0,0427**	0,1337
	n = 199	**n = 198**	197	**n = 198**	199
MF_1c	0,04616	0,13309	**r = 0,15603**	**r = 0,14633**	0,13282
	0,5173	0,0616	**p = 0,0286**	**p = 0,0397**	0,0615
	199	198	**n = 197**	**n = 198**	199
MF_1d	0,07095	0,10285	**r = 0,18625**	0,13076	0,09455
	0,3193	0,1493	**p = 0,0088**	0,0663	0,1841
	199	198	**n = 197**	198	199
MF_1e	**r = 0,3082**	**r = 0,15211**	**r = 0,20567**	0,10549	**r = 0,20076**
	p <.0001	**p = 0,0324**	**p = 0,0037**	0,1391	**p = 0,0045**
	n = 199	**n = 198**	**n = 197**	198	**n = 199**
MF_1f	0,07524	0,00601	0,02908	0,08457	0,02627
	0,2909	0,9331	0,685	0,2362	0,7127
	199	198	197	198	199
MF_1g	**r = 0,23159**	0,09141	0,12024	0,08627	0,08524
	p = 0,001	0,2014	0,0932	0,228	0,2325
	n = 198	197	196	197	198
MF_1h	0,06902	-0,02099	0,08049	0,03191	0,01997
	0,3327	0,7691	0,2608	0,6554	0,7795
	199	198	197	198	199
MF_1i	**r =-0,16895**	-0,05732	0,00504	-0,02896	-0,09141
	p = 0,0171	0,4225	0,9439	0,6855	0,1991
	n = 199	198	197	198	199

Współczynniki korelacji Spearmana					
Prawd. > |r| przy H0: Rho=0					
Liczba obserwacji					
	PG_1a	PG_1b	PG_1c	PG_1d	PG_1e
MF_2a	**r = 0,25473**	**r = 0,29264**	**r = 0,25982**	**r = 0,2834**	**r = 0,30682**
	p = 0,0003	**p <0,0001**	**p = 0,0002**	**p <0,0001**	**p <0,0001**
	n = 200	**n = 199**	**n = 198**	**n = 199**	**n = 200**
MF_2b	**r = 0,29516**	**r = 0,26432**	**r = 0,20865**	**r = 0,24722**	**r = 0,32244**
	p <0,0001	**p = 0,0002**	**p = 0,0032**	**p = 0,0004**	**p <0,0001**
	n = 199	**n = 199**	**n = 198**	**n = 199**	**n = 199**
MF_2c	**r = 0,34965**	**r = 0,24919**	**r = 0,29864**	**r = 0,28234**	**r = 0,30261**
	p <0,0001	**p = 0,0004**	**p <0,0001**	**p <0,0001**	**p <0,0001**
	n = 198	**n = 198**	**n = 198**	**n = 199**	**n = 199**
MF_2d	**r = 0,23035**	**r = 0,23656**	**r = 0,17919**	**r = 0,19942**	**r = 0,26692**
	p = 0,0011	**p = 0,0008**	**p = 0,0118**	**p = 0,0049**	**p = 0,0001**
	n = 198	**n = 198**	**n = 197**	**n = 198**	**n = 198**
MF_2e	0,11456	**r = 0,16546**	0,12724	**r = 0,15767**	0,10045
	0,1071	**p = 0,0195**	0,074	**p = 0,0261**	0,158
	199	**n = 199**	198	**n = 199**	199
MF_3a	**r = 0,18681**	**r = 0,1746**	0,10124	**r = 0,1458**	**r = 0,23026**
	p = 0,0084	**p = 0,0139**	0,1569	**p = 0,0404**	**p = 0,0011**
	n = 198	**n = 198**	197	**n = 198**	**n = 198**
MF_3b	0,13467	**r = 0,22058**	**r = 0,20801**	**r = 0,20382**	**r = 0,26698**
	0,0592	**p = 0,0018**	**p = 0,0034**	**p = 0,0041**	**p = 0,0001**
	197	**n = 197**	**n = 196**	**n = 197**	**n = 197**
MF_3c	**r = 0,17073**	**r = 0,27286**	**r = 0,26369**	**r = 0,23972**	**r = 0,27384**
	p = 0,0162	**p = 0,0001**	**p = 0,0002**	**p = 0,0007**	**p <0,0001**
	n = 198	**n = 198**	**n = 197**	**n = 198**	**n = 198**
MF_3d	**r = 0,20269**	**r = 0,23329**	**r = 0,26708**	0,11277	**r = 0,2632**
	p = 0,0042	**p = 0,0009**	**p = 0,0001**	0,1137	**p = 0,0002**
	n = 198	**n = 198**	**n = 197**	198	**n = 198**
MF_3e	**r = 0,18349**	**r = 0,22376**	**r = 0,17671**	**r = 0,21653**	**r = 0,25231**
	p = 0,0095	**p = 0,0015**	**p = 0,013**	**p = 0,0022**	**p = 0,0003**
	n = 199	**n = 198**	**n = 197**	**n = 198**	**n = 199**
MF_4a	**r = 0,17409**	**r = 0,20959**	**r = 0,21386**	**r = 0,23243**	**r = 0,22983**
	p = 0,0144	**p = 0,0031**	**p = 0,0026**	**p = 0,001**	**p = 0,0012**
	n = 197	**n = 197**	**n = 196**	**n = 197**	**n = 197**
MF_4b	**r = 0,14759**	**r = 0,24978**	0,12212	0,16158	0,25706
	p = 0,0385	**p = 0,0004**	0,0882	0,0233	0,0003
	n = 197	**n = 197**	196	197	197
MF_4c	**r = 0,14315**	**r = 0,1875**	**r = 0,166**	0,13025	**r = 0,22674**
	p = 0,0453	**p = 0,0085**	**p = 0,0204**	0,0688	**p = 0,0014**
	n = 196	**n = 196**	**n = 195**	196	**n = 196**

Źródło: opracowanie własne.

Na podstawie analizy, określono jak działania, które mogą być podejmowane przez bezpośrednich przełożonych, są związane z postrzeganiem korzyści związanych z bezpiecznym korzystaniem z uwierzytelnienia.

Działania **zwiększające** (korelacja dodatnia) **znaczenie bezpieczeństwa danych** dla respondenta to:

1. Jasne wyznaczanie i komunikowanie zasad dotyczących korzystania z kont pracowniczych i narzędzi uwierzytelniania (MF_1e): **p < 0,0001**; r = 0,31.
2. Zapewnienie wsparcia technicznego i merytorycznego; gdy pracownik wie, do kogo się zwrócić w razie problemów (MF_1a): **p < 0,0001**; r = 0,29.
3. Bieżąca kontrola działań związanych z uwierzytelnieniem, reagowanie przełożonych na nieprzestrzeganie zasad (MF_1g): **p = 0,001**; r = 0,23.
4. Przeszkolenie z bezpieczeństwa uwierzytelniania się (MF_1b): **p = 0,007**; r = 0,19.

Działania **zmniejszające** (korelacja ujemna) **znaczenie bezpieczeństwa danych** dla respondenta:

1. Brak działań przełożonych (MF_1i): **p = 0,02**; r = -0,17.

Działania **zwiększające** (korelacja dodatnia) **znaczenie zmniejszenia ryzyka odpowiedzialności (np. karnej)** dla respondenta:

1. Przeszkolenie z bezpieczeństwa uwierzytelniania się (MF_1b): **p = 0,02**; r = 0,17.
2. Jasne wyznaczanie i komunikowanie zasad dotyczących korzystania z kont pracowniczych i narzędzi uwierzytelniania (MF_1e): **p = 0,03**; r = 0,15.

Działania **zwiększające** (korelacja dodatnia) **znaczenie świadomości dopełnienia obowiązków** dla respondenta:

1. Jasne wyznaczanie i komunikowanie zasad dotyczących korzystania z kont pracowniczych i narzędzi uwierzytelniania (MF_1e): **p = 0,004**; r = 0,21.
2. Włączenie pracownika w proces decydowania o zasadach i wyborze narzędzi uwierzytelniania (MF_1d): **p = 0,009**; r = 0,19.
3. Przeprowadzanie cyklicznych szkoleń, podczas których poruszane są kwestie związane z bezpieczeństwem uwierzytelniania się (MF_1c): **p = 0,03**; r = 0,16.

Działania **zwiększające** (korelacja dodatnia) **znaczenie uniknięcia problemów w pracy** dla respondenta:

1. Przeprowadzanie cyklicznych szkoleń, podczas których poruszane są kwestie związane z bezpieczeństwem uwierzytelniania się (MF_1c): **p = 0,04**; r = 0,15.
2. Przeszkolenie z bezpieczeństwa uwierzytelniania się (MF_1b): **p = 0,04**; r = 0,14.

Działania **zwiększające** (korelacja dodatnia) **znaczenie bezpieczeństwa komunikacji drogą elektroniczną** dla respondenta:

1. Jasne wyznaczanie i komunikowanie zasad dotyczących korzystania z kont pracowniczych i narzędzi uwierzytelniania (MF_1e): **p = 0,005**; r = 0,20.
2. Zapewnienie wsparcia technicznego i merytorycznego; gdy pracownik wie, do kogo się zwrócić w razie problemów (MF_1a): **p = 0,005**; r = 0,20.

Określono jaki związek parametrów zarządzania macierzystym przedsiębiorstwem i postrzegania przez respondenta istotności korzyści związanych z bezpiecznym korzystaniem z uwierzytelnienia. Parametry zostały podzielone na: przywództwo, styl zarządzania oraz kompetencje.

W ramach realizowanego w przedsiębiorstwie przywództwa, analizy statystyczne wykazywały następujące zależności:

1. Im bardziej respondent zgadzał się ze stwierdzeniem, że najwyższa kadra zarządzająca ma na uwadze możliwości oraz zagrożenia, jakie daje dostęp pracownika do zasobów informatycznych, tym ważniejsze były dla pracownika korzyści wynikające z bezpiecznego stosowania tożsamości cyfrowej (**p <= 0,0003**; 0,25< r <0,31).
2. Im bardziej respondent zgadzał się ze stwierdzeniem, że zapewnienie bezpieczeństwa dostępu do danych wpisuje się w ogólną strategię zakładu pracy, tym ważniejsze były dla pracownika korzyści wynikające z bezpiecznego stosowania tożsamości cyfrowej (**p <= 0,0032**; 0,20<r<0,323).
3. Im bardziej respondent zgadzał się ze stwierdzeniem, że w jego zakładzie pracy panuje kultura zabezpieczania informacji w ramach całej organizacji, tym ważniejsze były dla niego korzyści wynikające z bezpiecznego stosowania tożsamości cyfrowej (**p <= 0,0004**; 0,249<r<0,35).
4. Im bardziej respondent zgadzał się ze stwierdzeniem, że jego zakład pracy posiada jasno określoną i zaakceptowaną strategię rozwoju w zakresie bezpieczeństwa dostępu do systemów informatycznych, tym ważniejsze były dla niego korzyści wynikające z bezpiecznego stosowania tożsamości cyfrowej (**p < 0,012**; 0,179<r<0,267).
5. Im bardziej respondent zgadzał się ze stwierdzeniem, że w zakładzie pracy bezpieczeństwo danych jest ważniejsze niż efektywność pracy, tym ważniejsze były dla niego korzyści wynikające z redukcji ryzyka odpowiedzialności np. karnej (**p = 0,02**; r = 0,17) oraz uniknięcia problemów w pracy np. podszycia się (**p = 0,03**; r = 0,16).

W ramach badania stylu zarządzania przedsiębiorstwem, analizy statystyczne wykazywały następujące zależności:

1. Im bardziej respondent zgadzał się ze stwierdzeniem, że przedsiębiorstwo posiada standardowy proces administracyjny w zakresie zarządzania dostępem do systemów informatycznych, tym ważniejsze były dla niego: bezpieczeństwo komunikacji drogą elektroniczną (**p = 0,001**; r = 0,23), bezpie-

czeństwo danych (**p = 0,008**; r = 0,19), redukcja ryzyka odpowiedzialności karnej (**p = 0,014**; r = 0,18), uniknięcie problemów w pracy (**p = 0,04**; r = 0,15).

2. Im bardziej respondent zgadzał się ze stwierdzeniem, że przedsiębiorstwo posiada stabilne wskaźniki oceny kosztów/korzyści zabezpieczenia dostępu do systemów informatycznych, tym ważniejsze były dla niego bezpieczeństwo komunikacji drogą elektroniczną (**p = 0,0001**; r = 0,27), redukcja odpowiedzialności karnej (**p = 0,002**; r = 0,22), świadomość dopełnienia obowiązków (**p = 0,003**; r = 0,21) oraz uniknięcie problemów w pracy (**p = 0,004**; r = 0,20).
3. Im bardziej respondent zgadzał się ze stwierdzeniem, że funkcje, zakresy obowiązków, odpowiedzialności i kontroli w odniesieniu do kwestii związanych z dostępem do systemów informatycznych są jasno sprecyzowane, tym ważniejsze były dla niego korzyści wynikające z bezpiecznego stosowania tożsamości cyfrowej (**p < 0,016**; 0,17 < r < 0,274).
4. Im bardziej respondent zgadzał się ze stwierdzeniem, że kierownicy są kompetentni i dobrze motywowani do zabezpieczenia dostępu do systemów informatycznych oraz egzekwowania bezpiecznego ich użycia przez ich podwładnych, tym ważniejsze były dla niego świadomość dopełnienia obowiązków (**p = 0,0001**; r = 0,27), bezpieczna komunikacja droga elektroniczną (**p = 0,0002**; r = 0,26), redukcja odpowiedzialności np. karnej (**p = 0,0009**; r = 0,23) oraz bezpieczeństwo danych (**p = 0,004**; r = 0,20).
5. Im bardziej respondent zgadzał się ze stwierdzeniem, że dział IT (wsparcie techniczne) udziela szybkiego i kompleksowego wsparcia, a współpraca z nim przebiega bez zakłóceń, tym ważniejsze były dla niego korzyści wynikające z bezpiecznego stosowania tożsamości cyfrowej (**p <= 0,013**; 0,17 < r < 0,25).

W ramach badania kompetencji w zarządzaniu przedsiębiorstwem, analizy statystyczne wykazywały następujące zależności:

1. Im bardziej respondent zgadzał się ze stwierdzeniem, że zakład pracy jest w stanie funkcjonować w otoczeniu szybkich i wciąż zachodzących zmian, tym ważniejsze były dla niego korzyści wynikające z bezpiecznego stosowania tożsamości cyfrowej (**p < 0,015**; 0,17 < r < 0,253).
2. Im bardziej respondent zgadzał się ze stwierdzeniem, że dostęp do odpowiednich zasobów systemów informatycznych jest udzielany niezwłocznie i właściwie (np. w przypadku przyjęcia nowego pracownika), tym ważniejsze były dla niego redukcja odpowiedzialności np. karnej (**p = 0,0004**; r = 0,25) oraz bezpieczeństwo danych (**p = 0,04**; r = 0,15).
3. Im bardziej respondent zgadzał się ze stwierdzeniem, że osoby zarządzające biznesem mają wiedzę technologiczną, a osoby zarządzające technologią mają wiedzę biznesową, tym ważniejsze były dla niego komunikacja drogą elektroniczną (**p = 0,001**; r = 0,23), redukcja ryzyka odpowiedzialności np.

karnej (**p = 0,009**; r = 0,19), świadomość dopełnienia obowiązków (**p = 0,02**; r = 0,17) oraz bezpieczeństwo danych (**p = 0,05**; r = 0,14).

Zbadano zależności między czynnikami zarządczymi (pojedyncze pytania oraz zbudowane wskaźniki) a wskaźnikiem PG. Wyniki ukazano w tabeli 5.56.

Tabela 5.56. Współczynniki korelacji Spearmana (Rang Spearmana) PG i MF w rozbiciu na pytania

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	PG
MF_1a	**r = 0,20948**
	p = 0,0029
	n = 200
MF_1b	0,1274
	0,0722
	200
MF_1c	0,13188
	0,0627
	200
MF_1d	0,13243
	0,0616
	200
MF_1e	**r = 0,21626**
	p = 0,0021
	n = 200
MF_1f	0,07511
	0,2905
	200
MF_1g	**r = 0,14329**
	p = 0,0435
	n = 199
MF_1h	0,04291
	0,5463
	200
MF_1i	-0,07149
	0,3144
	200
MF_5	**r = 0,38214**
	p <0,0001
	n = 201
MF_6	**r = 0,3401**
	p <0,0001
	n = 200
MF_7	**r = 0,28769**
	p <0,0001
	n = 198
MF	**r =0.37845**
	p <0,0001
	n=202

Źródło: opracowanie własne.

Na podstawie analizy określono, że największy związek z postrzeganiem korzyści z bezpiecznego stosowania uwierzytelnienia miały następujące działania przełożonych:

1. Wyznaczenie i jasne komunikowanie zasad dotyczących korzystania z kont pracowniczych i narzędzi uwierzytelniania (**p = 0,002**; r = 0,22).
2. Zapewnienie wsparcia technicznego i merytorycznego, by pracownik wiedział do kogo się zwrócić w razie kłopotów (**p = 0,003**; r = 0,21).
3. Bieżąca kontrola działań związanych z uwierzytelnieniem, reagowanie przełożonych na nieprzestrzeganie zasad (**p = 0,44**; r = 0,14).

Na podstawie analizy określono następującą hierarchię związku parametrów zarządzania w macierzystym zakładzie pracy z postrzeganiem korzyści z bezpiecznego stosowania uwierzytelnienia:

1. Przywództwo (**p < 0,0001**; r = 0,38).
2. Styl zarządzania (**p < 0,0001**; r = 0,34).
3. Kompetencje (**p < 0,0001**; r = 0,29).

Obliczono siłę związku między wskaźnikiem MF a wskaźnikiem PG jako r = 0,38, przy **p < 0,0001**.

Wnioski:

1. Należy odrzucić hipotezę zerową H^0_{11} dotyczącą niezależności postrzegania korzyści z tytułu bezpiecznego stosowania tożsamości cyfrowych i czynników zarządczych, na korzyść hipotezy alternatywnej H^1_{11}.
2. **Zależność 17**: Wyznaczenie i jasne komunikowanie zasad dotyczących korzystania z kont pracowniczych i narzędzi uwierzytelniania zwiększa postrzeganie korzyści z bezpiecznego stosowania tożsamości cyfrowej – dodatni współczynnik korelacji.
   Siła zależności 17: niezbyt duża (test Spearmana; r = 0,22).
3. **Zależność 18**: Zapewnienie wsparcia technicznego i merytorycznego, by pracownik wiedział do kogo się zwrócić w razie kłopotów zwiększa postrzeganie korzyści z bezpiecznego stosowania tożsamości cyfrowej – dodatni współczynnik korelacji.
   Siła zależności 18: niezbyt duża (test Spearmana; r = 0,21).
4. **Zależność 19**: Bieżąca kontrola działań związanych z uwierzytelnieniem, reagowanie przełożonych na nieprzestrzeganie zasad zwiększa postrzeganie korzyści z bezpiecznego stosowania tożsamości cyfrowej – dodatni współczynnik korelacji.
   Siła zależności 19: słaba (test Spearmana; r = 0,14).
5. **Zależność 20**: Wysoki poziom zarządzania zwiększa postrzeganie korzyści z bezpiecznego stosowania tożsamości cyfrowej – dodatni współczynnik korelacji.
   Siła zależności 20: dość duża (test Spearmana 0,38).

5.3.12. Badanie hipotezy statystycznej H12 (zależność PL od MF)

Zbadano związek pomiędzy postrzeganymi stratami z tytułu bezpiecznego stosowania tożsamości cyfrowej (PL) i czynnikami zarządczymi (MF). Związek został zbadany zarówno pomiędzy zmiennymi reprezentującymi poszczególne pytania, jak i utworzonymi wskaźnikami (tabela 5.57.).

Tabela 5.57. Współczynniki korelacji Spearmana (Rang Spearmana) PL i MF w rozbiciu na pytania

Współczynniki korelacji Spearmana				
Prawd. > |r| przy H0: Rho=0				
Liczba obserwacji				
	PL_1H	PL_1P	PL_1B	PL_2
MF_1a	-0.05134	**r = -0,155**	**r = -0,158**	0,12387
	0.4726	**p = 0,030**	**p = 0,026**	0,0798
	198	**n = 197**	**n = 198**	201
MF_1b	0,053	-0,074	-0,008	0,09746
	0,462	0,300	0,912	0,1709
	198	197	198	199
MF_1c	0,008	0,011	-0,051	0,09816
	0,906	0,877	0,472	0,1678
	198	197	198	199
MF_1d	-0,109	-0,078	-0,009	005018
	0,125	0,274	0,900	0,4815
	198	197	198	199
MF_1e	**r = -0,163**	-0,081	0,044	0,00838
	p = 0,021	0,256	0,538	0,9065
	n = 198	197	198	199
MF_1f	0,105	0,045	-0,023	0,04905
	0,141	0,527	0,751	0,4915
	198	197	198	199
MF_1g	-0,117	-0,101	r = -0,162	0,01838
	0,102	0,160	p = 0,023	0,7967
	197	196	n = 197	199
MF_1h	0,019	-0,008	0,046	-0,0382
	0,791	0,907	0,519	0,5931
	198	197	198	198
MF_1i	-0,090	0,014	-0,013	0,00426
	0,206	0,842	0,860	0,9524
	198	197	198	199
MF_2a	-0,005	-0,008	-0,017	-0,05339
	0,944	0,908	0,814	0,4539
	199	198	199	199

Współczynniki korelacji Spearmana				
Prawd. > |r| przy H0: Rho=0				
Liczba obserwacji				
	PL_1H	PL_1P	PL_1B	PL_2
MF_2b	0,037	0,014	-0,018	**r = 0,14979**
	0,601	0,844	0,796	**p = 0,0343**
	199	197	198	**n = 200**
MF_2c	-0,052	-0,059	-0,023	0,0999
	0,465	0,412	0,745	0,1603
	198	196	197	199
MF_2d	-0,044	-0,036	0,025	0,11422
	0,537	0,618	0,729	0,1091
	198	196	197	198
MF_2e	0,092	0,057	0,106	0,12933
	0,196	0,426	0,139	0,0694
	199	197	198	198
MF_3a	-0,033	-0,018	-0,040	0,07899
	0,643	0,802	0,580	0,2674
	198	196	197	199
MF_3b	-0,022	**r = -0,214**	-0,084	0,074
	0,759	**p = 0,003**	0,243	0,3002
	197	**n = 196**	196	198
MF_3c	-0,004	**r = -0,175**	0,001	**r = 0,14812**
	0,955	**p = 0,014**	0,987	**p = 0,0378**
	198	**n = 196**	197	**n = 197**
MF_3d	-0,052	-0,090	-0,046	**r = 0,15947**
	0,469	0,212	0,519	**p = 0,0248**
	198	196	197	**n = 198**
MF_3e	-0,023	-0,120	-0,072	0,06881
	0,747	0,093	0,310	0,3354
	198	197	198	198
MF_4a	-0,117	-0,132	**r = -0,188**	0,06586
	0,101	0,067	**p = 0,008**	0,3554
	197	195	**n = 196**	199
MF_4b	**r = -0,169**	-0,119	-0,093	0,01179
	p = 0,018	0,098	0,195	0,8693
	n = 197	195	196	197
MF_4c	**r = -0,191**	-0,134	**r = -0,145**	0,07984
	p = 0,007	0,063	**p = 0,043**	0,2648
	n = 196,000	194,000	**n = 195,000**	197

Źródło: opracowanie własne.

Wykazano zależności istotne statystycznie między (tabela 5.57.):

1. Zapewnieniem wsparcia technicznego i merytorycznego, by pracownik wiedział do kogo się zwrócić w razie kłopotów (MF_1a), a postrzeganiem strat na efektywności pracy ponoszonymi z tytułu bezpiecznego korzystania z przedmiotów uwierzytelniających (PL_1P) oraz korzystania

z uwierzytelnienia biometrycznego (PL_1B): odpowiednio **p = 0,30**; r = -0,16 oraz **p = 0,26**; r = -0,16.

2. Wyznaczeniem i jasnym komunikowaniem zasad dotyczących korzystania z kont pracowniczych i narzędzi uwierzytelniania (MF_1e) a postrzeganiem strat na efektywności pracy ponoszonymi z tytułu bezpiecznego korzystania z haseł (PL_1H): **p = 0,21**; r = -0,16.
3. Posiadaniem stabilnych wskaźników oceny kosztów/korzyści zabezpieczenia dostępu do systemów informatycznych (MF_3b) oraz posiadanie jasno sprecyzowanych funkcji, zakresów obowiązków, odpowiedzialności i kontroli w odniesieniu do kwestii związanych z dostępem do systemów informatycznych (MF_3c), a postrzeganiem strat na efektywności pracy ponoszonymi z tytułu bezpiecznego korzystania z przedmiotów uwierzytelniających (PL_1P): odpowiednio **p = 0,003**; r = -0,21 oraz **p = 0,014**; r = -0,175.
4. Postrzeganiem zakładu pracy jako zdolnego funkcjonować w otoczeniu szybkich i wciąż zachodzących zmian (MF_4a), a postrzeganymi stratami z tytułu korzystania z uwierzytelnienia biometrycznego (PL_1B): **p = 0,008**; r = -0,188.
5. Niezwłocznym i właściwym udzielaniem dostępu do odpowiednich zasobów systemów informatycznych (MF_1b) a postrzeganymi stratami z tytułu bezpiecznego korzystania z haseł (PL_1H): **p = 0,018**; r = -0,169.
6. Posiadaniem wiedzy technologicznej przez osoby zarządzające biznesem, wiedzy biznesowej przez osoby zarządzające technologią (MF_4c), a postrzeganymi stratami na efektywności pracy z tytułu korzystania w sposób bezpieczny z haseł (PL_1H) oraz korzystania z uwierzytelnienia biometrycznego (PL_1B): odpowiednio **p = 0,007**; r = -0,191 oraz **p = 0,043**; r = -0,145.
7. Faktem, że zapewnienie bezpieczeństwa dostępu do danych wpisuje się w ogólną strategię zakładu pracy (MF_2b), posiadaniem jasno sprecyzowanych funkcji, zakresów obowiązków, odpowiedzialności i kontroli w odniesieniu do kwestii związanych z dostępem do systemów informatycznych (MF_3c), oraz kompetencjami i dobrą motywacją kierowników do zabezpieczenia dostępu do systemów informatycznych oraz egzekwowaniem bezpiecznego ich użycia przez ich podwładnych (MF_3d), a poziomem poczucia zagrożenia związanego z uwierzytelnieniem się: odpowiednio **p = 0,034**; r = 0,15 oraz **p = 0,038**; r = 0,15 oraz **p = 0,025**; r = 0,16.

Zbadano zależności między poziomem zarządzania MF a postrzeganiem ryzyka związanego z uwierzytelnieniem się (PL_2a do PL_2h). Wykryto jedną zależność między poziomem zarządzania a obawą związaną z zagrożeniem osobistym przy próbie dotarcia do zasobów chronionych cechami biometrycznymi (np. rozbój): **p = 0,046**, r = -0,14.

Wnioski:

1. Należy odrzucić hipotezę zerową H^0_{12} dotyczącą niezależności postrzegania strat z tytułu bezpiecznego stosowania tożsamości cyfrowych i czynników zarządczych, na korzyść hipotezy alternatywnej H^1_{12}.
2. **Zależność 21**: Zapewnienie wsparcia technicznego i merytorycznego, by pracownik wiedział do kogo się zwrócić w razie kłopotów zmniejsza postrzegane straty na efektywności z tytułu bezpiecznego stosowania przedmiotów oraz stosowania metod biometrycznych – ujemny współczynnik korelacji.
   Siła zależności 21: słaba (test Spearmana; r = -0,16).
3. **Zależność 22**: Wyznaczenie i jasne komunikowanie zasad dotyczących korzystania z kont pracowniczych i narzędzi uwierzytelniania zmniejsza postrzegane straty na efektywności z tytułu bezpiecznego stosowania haseł – ujemny współczynnik korelacji.
   Siła zależności 22: słaba (test Spearmana, r = -0,16).
4. **Zależność 23**: Posiadanie stabilnych wskaźników oceny kosztów/korzyści zabezpieczenia dostępu do systemów informatycznych zmniejsza postrzegane straty na efektywności z tytułu bezpiecznego stosowania przedmiotów – ujemny współczynnik korelacji.
   Siła zależności 23: niezbyt duża (test Spearmana; r = -0,21)
5. **Zależność 24**: Posiadanie jasno sprecyzowanych funkcji, zakresów obowiązków, odpowiedzialności i kontroli w odniesieniu do kwestii związanych z dostępem do systemów informatycznych, zmniejsza postrzegane straty na efektywności z tytułu bezpiecznego stosowania przedmiotów – ujemny współczynnik korelacji.
   Siła zależności 24: słaba (test Spearmana; r = -0,18).
6. **Zależność 25**: Postrzeganie zakładu pracy jako zdolnego funkcjonować w otoczeniu szybkich i wciąż zachodzących zmian zmniejsza postrzegane straty na efektywności z tytułu korzystania z uwierzytelnienia biometrycznego – ujemny współczynnik korelacji.
   Siła zależności 25: słaba (test Spearmana; r = -0,19).
7. **Zależność 26**: Niezwłoczne i właściwe udzielanie dostępu do odpowiednich zasobów systemów informatycznych zmniejsza postrzegane straty na efektywności z tytułu bezpiecznego stosowania haseł – ujemny współczynnik korelacji.
   Siła zależności 26: słaba (test Spearmana; r = -0,17).
8. **Zależność 27**: Posiadanie wiedzy technologicznej przez osoby zarządzające biznesem, a wiedzy biznesowej przez osoby zarządzające technologią zmniejsza postrzegane straty na efektywności z tytułu bezpiecznego stosowania haseł – ujemny współczynnik korelacji.
   Siła zależności 27: słaba (Test Spearmana; r = -0,19).
9. **Zależność 28**: Posiadanie wiedzy technologicznej przez osoby zarządzające biznesem, a wiedzy biznesowej przez osoby zarządzające technologią zmnie-

jsza postrzegane straty na efektywności z tytułu stosowania uwierzytelnienia biometrycznego – ujemny współczynnik korelacji.

Siła zależności 28: słaba (Test Spearmana; r = -0,15).

10. **Zależność 29**: Fakt, że zapewnienie bezpieczeństwa dostępu do danych wpisuje się w ogólną strategię zakładu pracy zwiększa poziom poczucia zagrożenia związanego z uwierzytelnieniem się – dodatni współczynnik korelacji.

    Siła zależności 29: słaba (Test Spearmana; r = 0,15).
11. **Zależność 30**: Posiadanie jasno sprecyzowanych funkcji, zakresów obowiązków, odpowiedzialności i kontroli w odniesieniu do kwestii związanych z dostępem do systemów informatycznych, zwiększa poziom poczucia zagrożenia związanego z uwierzytelnieniem się – dodatni współczynnik korelacji.

    Siła zależności 30: słaba (Test Spearmana; r = 0,15).
12. **Zależność 31**: Kompetencje i dobra motywacja kierowników do zabezpieczenia dostępu do systemów informatycznych oraz egzekwowanie bezpiecznego ich użycia przez ich podwładnych zwiększa poziom poczucia zagrożenia związanego z uwierzytelnieniem się – dodatni współczynnik korelacji.

    Siła zależności 31: słaba (Test Spearmana; r = 0,16).
13. **Zależność 32**: Im wyższy poziom zarządzania, tym mniejsze obawy związane z zagrożeniem osobistym podczas próby dotarcia do zasobów chronionych cechami biometrycznymi – współczynnik korelacji ujemny.

    Siła zależności 32: słaba (Test Spearmana; r = -0,14.

5.3.13. Badanie hipotezy statystycznej H13 (zależność FP od MF)

Analiza danych (wyniki w tabeli 5.58.) nie wykazała zależności między czynnikami zarządczymi (MF) a postrzeganiem wymuszenia (FP).

Tabela 5.58. Współczynniki korelacji Spearmana (Rang Spearmana) MF i FP

Współczynniki korelacji Spearmana, N = 191	
Prawd. > |r| przy H0: Rho=0	
	MF
FP 1a	0,00093
	0,9898
FP 1b	0,00127
	0,9861
FP 1c	0,01961
	0,7877
FP 1d	0,093
	0,2007
FP 1e	0,05258
	0,4701

Źródło: opracowanie własne.

Współczynniki korelacji FP_1e i MF znalazły się blisko granicy uznania za istotne statystycznie.

Wnioski:

1. Nie ma podstaw do odrzucenia hipotezy zerowej H^0_{13} o niezależności badanych zmiennych, na korzyść hipotezy alternatywnej H^1_{13}.

5.3.14. Badanie hipotezy statystycznej H14 (zależność DIC od MF)

Zbadano związek pomiędzy charakterystyką tożsamości cyfrowej (DIC), a czynnikami zarządczymi (MF). Związek ten został zbadany zarówno pomiędzy zmiennymi reprezentującymi poszczególne pytania a utworzonym wskaźnikiem MF (tabela 5.59.).

Tabela 5.59. Współczynniki korelacji Spearmana (Rang Spearmana) MF i DIC w rozbiciu na pytania

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	MF
DIC_1H	0,07733
	0,2954
	185
DIC_2Ha	0,0506
	0,5527
	140
DIC_2Hb	**r = 0,16619**
	p = 0,0481
	n = 142
DIC_2Hc	0,15192
	0,0711
	142
DIC_2Hd	-0,00573
	0,9461
	142
DIC_3H	0,05784
	0,4406
	180
DIC_4H	0,13197
	0,0638
	198
DIC_5Pa	0,10174
	0,1496
	202
DIC_5Pb	**r = 0,16597**
	p = 0,0182
	n = 202
DIC_5Pc	0,08458
	0,2314
	202
DIC_5Pd	0,12572
	0,0746
	202

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	MF
DIC_5Pf	**r = 0,18188**
	p = 0,0096
	n = 202
DIC_5Pg	**r = 0,21401**
	p = 0,0022
	n = 202
DIC_6P	**r = 0,1622**
	p = 0,0211
	n = 202
DIC_7Pa	0,06481
	0,3619
	200
DIC_7Pb	0,11947
	0,092
	200
DIC_7Pc	0,10881
	0,1251
	200
DIC_7Pd	0,1109
	0,118
	200
DIC_7Pe	0,10312
	0,1472
	199
DIC_7Pf	0,13176
	0,0629
	200
DIC_7Pg	**r = 0,16325**
	p = 0,0209
	n = 200

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	MF
DIC_5Pe	0,06419
	0,3641
	202
DIC_8B	0,07779
	0,2736
	200

Źródło: opracowanie własne.

Wykazano zależności istotne statystycznie między poziomem zarządzania (MF) a:

- stosowaniem dużych liter w hasłach (**p = 0,0481**; r = 0,16619**)**,
- stosowaniem karty elektronicznej zabezpieczonej dodatkowo numerem PIN (**p = 0,0182**; r = 0,16597),
- stosowaniem tokena – aplikacji na komórkę (**p = 0,0096**; r = 0,18188),
- stosowaniem kart kodów jednorazowych (**p = 0,0022**; r = 0,21401),
- częstotliwością stosowania przedmiotów uwierzytelniających w ciągu dnia (**p = 0,0211**; r = 0,1622),
- częstotliwości stosowania kart kodów jednorazowych w ciągu dnia (**p = 0.0209**; r = 0,16325).

Zbadano związek między czynnikami zarządczymi a częstotliwością użycia hasła (tabela 5.60.).

Tabela 5.60. Współczynniki korelacji Spearmana (Rang Spearmana) MF w rozbiciu na i DIC_3H

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	DIC_3H
MF	0,13197
	0,0638
	198
MF_1a	**r = 0,22337**
	p = 0,0016
	n = 196
MF_1b	0,12745
	0,0751
	196
MF_1c	0,06193
	0,3885
	196

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	DIC_3H
MF_2d	0,09076
	0,207
	195
MF_2e	-0,07482
	0,2973
	196
MF_3a	0,06555
	0,3626
	195
MF_3b	0,00718
	0,9208
	194

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	DIC_3H
MF_1d	-0,00598
	0,9337
	196
MF_1e	0,04373
	0,5428
	196
MF_1f	0,09894
	0,1677
	196
MF_1g	**r = 0,14965**
	p = 0,0368
	n = 195
MF_1h	-0,13192
	0,0653
	196
MF_1i	-0,03276
	0,6485
	196
MF_2a	0,0055
	0,9389
	197
MF_2b	0,12324
	0,0853
	196
MF_2c	0,13656
	0,057
	195

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	DIC_3H
MF_3c	0,01502
	0,835
	195
MF_3d	0,11375
	0,1133
	195
MF_3e	**r = 0,14424**
	p = 0,0437
	n = 196
MF_4a	0,08933
	0,2155
	194
MF_4b	0,05748
	0,426
	194
MF_4c	0,04488
	0,5355
	193
MF_5	0,06898
	0,3354
	197
MF_6	0,06247
	0,3844
	196
MF_7	0,05844
	0,4183
	194

Źródło: opracowanie własne.

Wykazano zależności istotne statystycznie między częstotliwością użycia hasła a:

- zapewnieniem wsparcia merytorycznego i technicznego (**p = 0,0016**; r = 0,22337),
- bieżącym kontrolowaniem działań związanych z uwierzytelnieniem i reagowaniem przełożonych na nieprzestrzeganie zasad (**p = 0,0368**; r = 0,14965),
- szybkim i kompleksowym wsparciem technicznym, którym współpraca przebiega bez zakłóceń (**p = 0,0437**; r = 0,14424).

Wnioski:

1. W przypadku uwierzytelnień opartych o biometrię nie ma podstaw do odrzucenia hipotezy zerowej H^0_{14}; w przypadku uwierzytelnień opartych o hasła i przedmioty należy odrzucić hipotezę zerową H^0_{14} o niezależności badanych zmiennych, na korzyść hipotezy alternatywnej H^1_{14}.
2. **Zależność 33**: Im lepsze zarządzanie, tym częściej stosowane są wielkie litery w hasłach – dodatni współczynnik korelacji.
   Siła zależności 33: słaba (test Spearmana; r = 0,17).
3. **Zależność 34**: Im lepsze zarządzanie, tym wyższa jest częstotliwość stosowania w ciągu dnia pracy uwierzytelnienia opartego o przedmioty – dodatnia korelacja.
   Siła zależności 34: słaba (test Spearmana; r = 0,16).
4. **Zależność 35**: Im lepsze zarządzanie, tym częściej stosowane są karty elektroniczne zabezpieczone numerem PIN, tokeny w postaci aplikacji oraz karty kodów jednorazowych – dodatnia korelacja.
   Siła zależności 35: słaba (test Spearmana; odpowiednio r = 0,18, r = 0,21; r = 0,16).
5. **Zależność 36**: Im lepsze jest zarządzanie przedsiębiorstwem, tym częściej w ciągu dnia pracy wykorzystywane są kart kodów jednorazowych – dodatnia korelacja.
   Siła zależności 36: słaba (test Spearmana; r = 0,16).
6. **Zależność 37**: Im lepsze wsparcie merytoryczne i techniczne, tym częściej używane są hasła – dodatnia korelacja.
   Siła zależności 37: nieduża (Test Spearmana; r = 0,22).
7. **Zależność 38**: im większa kontrola bieżących działań związanych z uwierzytelnieniem i reagowanie na uchybienia w tej kwestii, tym większa częstotliwość uwierzytelnienia – korelacja dodatnia.
   Siła zależności 38: słaba (Test Spearmana; r = 0,15).
8. **Zależność 39**: im lepsza współpraca z działem IT (wsparciem technicznym), tym większa częstotliwość uwierzytelniania się – korelacja dodatnia.
   Siła zależności 39: słaba (Test Spearmana; r = 0,14).

5.3.15. Badanie hipotezy statystycznej H15 (zależność UC od MF)

W ramach charakterystyki użytkownika zbadano wyłącznie związek samooceny wiedzy (UC_4) z czynnikami zarządczymi (MF).

Tabela 5.61. Współczynniki korelacji Spearmana (Rang Spearmana) MF w rozbiciu i UC_4

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	UC_4
MF 1a	0,02503
	0,7416
	176
MF 1b	**r = 0,22799**
	p = 0,0023
	n = 176
MF 1c	**r = 0,29358**
	p <0,0001
	n = 176
MF 1d	0,12706
	0,0929
	176
MF 1e	0,03734
	0,6227
	176
MF 1f	0,03124
	0,6806
	176
MF 1g	**r = 0,15858**
	p = 0,0361
	n = 175
MF 1h	-0,01974
	0,7948
	176
MF 1i	0,06621
	0,3827
	176
MF 2a	0,08271
	0,2738
	177
MF 2b	**r = 0,17287**
	p = 0,0218
	n = 176
MF 2c	**r = 0,26252**
	p = 0,0004
	n = 176

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	UC_4
MF 2d	**r = 0,1745**
	p = 0,0209
	n = 175
MF 2e	**r = 0,15266**
	p = 0,0431
	n = 176
MF 3a	**r = 0,22814**
	p = 0,0023
	n = 176
MF 3b	**r = 0,2245**
	p = 0,0028
	n = 175
MF 3c	**r = 0,2785**
	p = 0,0002
	n = 176
MF 3d	**r = 0,18035**
	p = 0,0166
	n = 176
MF 3e	**r = 0,28558**
	p = 0,0001
	n = 177
MF 4a	**r = 0,15054**
	p = 0,0461
	n = 176
MF 4b	0,14027
	0,0633
	176
MF 4c	**r = 0,15863**
	p = 0,036
	n = 175
MF	**r = 0,32806**
	p = 0,000008
	n = 178

Źródło: opracowanie własne.

Zaobserwowano liczne zależności (tabela 5.61.). Najbardziej istotne z nich dotyczyły związku samooceny wiedzy, dokonanej przez respondenta z:

- faktem odbywania cyklicznych szkoleń (**p < 0,0001**; r = 0,29),
- szybkim i kompleksowym wsparciem ze strony działu IT (**p = 0,0001**; r = 0,29),

- jasnym sprecyzowaniem funkcji, zakresów obowiązków, odpowiedzialności i kontroli w odniesieniu do kwestii związanych z dostępem do systemów informatycznych (**p = 0,0002**; r = 0,28),
- kulturą zapewnienia bezpieczeństwa informacji w całym przedsiębiorstwie (**p = 0,0004**; r = 0,26),
- faktem odbycia wstępnego szkolenia z uwierzytelniania się (**p = 0,0023**; r = 0,23),
- stosowaniem standardowego procesu administracyjnego w zakresie zarządzania dostępem do systemów informatycznych (**p = 0,0023**; r = 0,23),
- stosowaniem stabilnych wskaźników oceny kosztów/korzyści zabezpieczenia dostępu do systemów informatycznych (**p = 0,0028**; r = 0,225),

Wnioski:

1. Należy odrzucić hipotezę zerową H^0_{15} o niezależności badanych zmiennych, na korzyść hipotezy alternatywnej H^1_{15}.
2. **Zależność 40**: im lepiej zarządzanie przedsiębiorstwo (MF) tym wyższa samoocena wiedzy respondenta dotycząca bezpieczeństwa uwierzytelnienia się – korelacja dodatnia.

   Siła zależności 40: średnia, ale wysoko istotny statystycznie współczynnik korelacji Rang Spearmana r = 0,33.

5.3.16. Badanie hipotezy statystycznej H16 (zależność TA od MF)

Zbadano związek pomiędzy postrzeganiem zagrożeń (TA) a czynnikami zarządczymi (MF) z wykorzystaniem testu Spearmana oraz testu Chi kwadrat. W obu przypadkach nie wykryto związku między poszczególnymi zmiennymi (tabela 5.62.).

Tabela 5.62. Współczynniki korelacji Spearmana (Rang Spearmana) MF w rozbiciu na pytania i TA

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	TA
MF 1a	-0,14186
	0,1175
	123
MF 1b	-0,03247
	0,7214
	123
MF 1c	-0,04174
	0,6467
	123
MF 1d	0,05347
	0,5569
	123
MF 1e	-0,07132
	0,4331
	123
MF 1f	0,1044
	0,2505
	123
MF 1g	-0,09819
	0,2799
	123
MF 1h	-0,02438
	0,789
	123
MF 1i	0,14139
	0,1188
	123
MF 2a	-0,02012
	0,8245
	124
MF 2b	-0,09685
	0,2846
	124

Współczynniki korelacji Spearmana	
Prawd. > |r| przy H0: Rho=0	
Liczba obserwacji	
	TA
MF 2c	-0,03434
	0,7049
	124
MF 2d	0,01036
	0,9091
	124
MF 2e	-0,02309
	0,7991
	124
MF 3a	-0,04567
	0,6145
	124
MF 3b	0,00935
	0,9182
	123
MF 3c	-0,12454
	0,1682
	124
MF 3d	-0,14468
	0,1089
	124
MF 3e	-0,11715
	0,1951
	124
MF 4a	-0,06547
	0,4719
	123
MF 4b	-0,02443
	0,7885
	123
MF 4c	-0,00503
	0,9559
	123

Źródło: opracowanie własne.

Wnioski:

1. Nie ma podstaw do odrzucenia hipotezy zerowej H^0_{16} o niezależności badanych zmiennych.

5.3.17. Badanie hipotezy statystycznej H17 (zależność U od BI)

Zbadano zależność bezpieczeństwa obecnego użycia tożsamości cyfrowych przez respondentów (U) i intencji użycia tożsamości cyfrowych w sposób bezpieczny (BI). Nie wykazano takiej zależności (tabela 5.63.).

Tabela 5.63.Współczynniki korelacji Spearmana (Rang Spearmana) BI i U

Współczynniki korelacji Spearmana		
Prawd. > |r| przy H0: Rho=0		
Liczba obserwacji		
	U_1H	U_1P
BI_1H	-0,13728	-0,09191
	0,0544	0,3944
	197	88
BI_2P	-0,10512	-0,0522
	0,1457	0,6291
	193	88
BI_3B	-0,02112	0,00839
	0,7718	0,9385
	191	87

Źródło: opracowanie własne.

Zbadano zatem zależności między intencją użycia tożsamości cyfrowych w sposób bezpieczny (BI_1H, BI_1P oraz BI_1B) a faktycznym użyciem, czyli działaniami użytkownika składającymi się na użycie narzędzia uwierzytelnienia w obszarze parametrów haseł, zachowania użytkownika oraz rozwiązań.

Zależności jakie udało się wykazać:

1. Chęć bezpiecznego stosowania biometrii (BI_1B) i stosowanie w hasłach ryzykownych treści np. prostych sekwencji czy ważnych dat (U_3H) – **p = 0,025** (tabela 5.64., tabela 5.65.).
2. Chęć stosowania przedmiotów uwierzytelniających w sposób bezpieczny (BI_1P) i stosowanie w hasłach ryzykownych treści np. prostych sekwencji czy ważnych dat (U_3H) – **p = 0,028** (tabela 5.66., tabela 5.67.).
3. Chęć stosowania przedmiotów uwierzytelniających w sposób bezpieczny (BI_1P) i stosowanie tego samego hasła do różnych aplikacji (U_7H) – **p = 0,036** (tabela 5.68., tabela 5.69.).
4. Chęć stosowania przedmiotów uwierzytelniających w sposób bezpieczny (BI_1P) i poziom zapewnionej ochrony dostępu do przedmiotu uwierzytelniającego (U_1P) – **p = 0,041** (tabela 5.70., tabela 5.71.).

Tabela 5.64. Analiza statystyczna liczności odpowiedzi U_3H wg BI_1B

Tabela U_3H wg BI_1B					
U_3H		BI_1B			Razem
		1	2	3	
0	Liczebność	6	1	17	24
	Procent	3,55	0,59	10,06	14,2
	Proc. wier.	25	4,17	70,83	
	Proc. kol.	24	2,78	15,74	
1	Liczebność	19	35	91	145
	Procent	11,24	20,71	53,85	85,8
	Proc. wier.	13,1	24,14	62,76	
	Proc. kol.	76	97,22	84,26	
Razem	Liczebność	25	36	108	169
	Procent	14,79	21,3	63,91	100

Źródło: opracowanie własne.

Tabela 5.65. Statystyki dla tabeli U_3H wg BI_1B

Statystyki dla tabeli U_3H wg BI_1B			
Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**2**	**6,0357**	**0,0489**
Chi-kw. ilorazu wiarygodn.	**2**	**7,3787**	**0,025**
Chi-kwadrat Mantela-Haenszela	1	0,0548	0,8149
Współczynnik FI		**0,189**	
Współczynnik wielodzielczości		0,1857	
V Cramera		0,189	

Źródło: opracowanie własne.

Tabela 5.66. Analiza statystyczna liczności odpowiedzi U_3H wg BI_1P

Tabela U_3H wg BI_1P					
U_3H		BI_1P			Razem
		1	2	3	
0	Liczebność	5	1	18	24
	Procent	2,91	0,58	10,47	13,95
	Proc. wier.	20,83	4,17	75	
	Proc. kol.	35,71	3,85	13,64	
1	Liczebność	9	25	114	148
	Procent	5,23	14,53	66,28	86,05
	Proc. wier.	6,08	16,89	77,03	
	Proc. kol.	64,29	96,15	86,36	
Razem	Liczebność	14	26	132	172
	Procent	8,14	15,12	76,74	100

Źródło: opracowanie własne.

Tabela 5.67. Statystyki dla tabeli U_3H wg BI_1P

Statystyki dla tabeli U_3H wg BI_1P			
Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**2**	**7,7448**	**0,0208**
Chi-kw. ilorazu wiarygodn.	**2**	**7,1372**	**0,0282**
Chi-kwadrat Mantela-Haenszela	1	1,5285	0,2163
Współczynnik FI		**0,2122**	
Współczynnik wielodzielczości		0,2076	
V Cramera		0,2122	

Źródło: opracowanie własne.

Tabela 5.68. Analiza statystyczna liczności odpowiedzi U_7H wg BI_1P

Tabela U_7H wg BI_1P					
U_7H		BI_1P			Razem
		1	2	3	
1	Liczebność	3	14	64	81
	Procent	1,67	7,78	35,56	45
	Proc. wier.	3,7	17,28	79,01	
	Proc. kol.	17,65	53,85	46,72	
2	Liczebność	14	12	73	99
	Procent	7,78	6,67	40,56	55
	Proc. wier.	14,14	12,12	73,74	
	Proc. kol.	82,35	46,15	53,28	
Razem	Liczebność	17	26	137	180
	Procent	9,44	14,44	76,11	100

Źródło: opracowanie własne.

Tabela 5.69. Statystyki dla tabeli U_7H wg BI_1P

Statystyki dla tabeli U_7H wg BI_1P			
Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**2**	**6,124**	**0,0468**
Chi-kw. ilorazu wiarygodn.	**2**	**6,6657**	**0,0357**
Chi-kwadrat Mantela-Haenszela	1	2,6605	0,1029
Współczynnik FI		**0,1845**	
Współczynnik wielodzielczości		0,1814	
V Cramera		0,1845	

Źródło: opracowanie własne.

Tabela 5.70. Analiza statystyczna liczności odpowiedzi U_1P wg BI_1P

Tabela U_1P wg BI_1P					
U_1P		BI_1P			Razem
		1	2	3	
1	Liczebność	3	4	26	33
	Procent	4,84	6,45	41,94	53,23
	Proc. wier.	9,09	12,12	78,79	
	Proc. kol.	75	100	48,15	
2	Liczebność	1	0	28	29
	Procent	1,61	0	45,16	46,77
	Proc. wier.	3,45	0	96,55	
	Proc. kol.	25	0	51,85	
Razem	Liczebność	4	4	54	62
	Procent	6,45	6,45	87,1	100

Źródło: opracowanie własne.

Tabela 5.71. Statystyki dla tabeli U_1P wg BI_1P

Statystyki dla tabeli U_1P wg BI_1P			
Statystyka	St. sw.	Wartość	Prawd.
Chi-kwadrat	**2**	**4,8361**	**0,0891**
Chi-kw. ilorazu wiarygodn.	**2**	**6,4075**	**0,0406**
Chi-kwadrat Mantela-Haenszela	1	2,9181	0,0876
Współczynnik FI		**0,2793**	
Współczynnik wielodzielczości		0,269	
V Cramera		0,2793	

Źródło: opracowanie własne.

Wnioski:

1. Należy odrzucić hipotezę zerową H^0_{17} o niezależności badanych zmiennych, na korzyść hipotezy alternatywnej H^1_{17}.
2. **Zależność 41**: chęć stosowania biometrii jest związana ze sposobem budowania haseł (zawieranie prostych ciągów znaków, ważnych dat itp.).
   Siła zależności 41: słaba (wg badania Chi kwadrat; fi = 0,189).
3. **Zależność 42**: chęć stosowania przedmiotów w sposób bezpieczny jest związana z tymi działaniami użytkownika dotyczącymi haseł, które można kontrolować tylko do pewnego stopnia tj. sposobem budowania haseł (zawieranie prostych ciągów znaków, ważnych dat itp.) oraz unikalnością stosowanych haseł w ramach różnych aplikacji.
   Siła zależności 42: słaba (wg badania Chi kwadrat; odpowiednio fi = 0,212 oraz fi = 0,185).
4. **Zależność 43**: chęć stosowania przedmiotów w sposób bezpieczny jest związana z zabezpieczeniem przedmiotu przed nieuprawnionym użyciem (użyczanie przedmiotu innym osobom).
   Siła zależności 43: dość słaba (wg badania Chi kwadrat; fi = 0,279).

6. Bezpieczeństwo użycia tożsamości cyfrowej przez kierowników i pracowników zatrudnionych na stanowiskach wykonawczych

Głównym ograniczeniem wiarygodności analizy porównawczej grup pracowników na stanowiskach kierowniczych i wykonawczych jest liczebność próby badawczej: osób deklarujących zajmowanie kierowniczego stanowiska było 51 (25% odpowiedzi), natomiast wykonawczego stanowiska – 141 (70% odpowiedzi). Pozostali respondenci nie udzielili odpowiedzi na to pytanie. Dodatkowo liczba respondentów korzystających z urządzeń uwierzytelniających jest stosunkowo niska. Z uwagi na dużą różnicę w liczności grup, porównywano procent udzielonych odpowiedzi.

6.1. Poziom bezpieczeństwa użycia tożsamości cyfrowych przez kierowników i pracowników niższych szczebli zarządzania

Bezpieczeństwo użycia tożsamości cyfrowej zostało zdefiniowane w oparciu o bezpieczeństwo użycia narzędzi uwierzytelnienia (U): loginów i haseł oraz przedmiotów uwierzytelniających.

Na pytania pozwalające określić poziom bezpieczeństwa użycia haseł odpowiedziało w sumie 175 osób: 48 kierowników (25% użytkowników haseł) oraz 127 (65% użytkowników haseł) pracowników na stanowiskach wykonawczych. Generalnie osoby na stanowiskach kierowniczych korzystają w haseł w sposób bardziej bezpieczny tj. mniej osób na stanowisku kierowniczym charakteryzowało się niskim bezpieczeństwem stosowania haseł (vide tabela 6.1.).

Tabela 6.1. Porównanie poziomu bezpieczeństwa użycia haseł (U_H) przez kierowników i pracowników na stanowiskach wykonawczych

	Stanowisko				**Różnica (R%)**
	Kierownicze		**Wykonawcze**		
	Liczba odpowiedzi (L)	**Procent odpowiedzi (%)**	**Liczba odpowiedzi (L)**	**Procent odpowiedzi (%)**	
Niskie	22	46%	75	59%	-13%
Średnie	22	46%	44	35%	11%
Wysokie	4	8%	8	6%	2%

Źródło: opracowanie własne.

Zbadano ile osób używa haseł w sposób zwiększający bezpieczeństwo zasobów systemów informacyjnych. Między badanymi grupami zaobserwowano brak lub niewielką różnicę (na korzyść osób zajmujących stanowisko kierownicze)

w przypadku większości parametrów (vide tabela 6.2.). Jednak osoby na stanowisku wykonawczym znacząco rzadziej zmieniali hasła oraz częściej wykorzystywali jedno hasło do różnych aplikacji.

Tabela 6.2. Porównanie elementów pozytywnie wpływających na bezpieczeństwo użycia haseł przez kierowników i pracowników na stanowiskach wykonawczych

Elementy pozytywnie wpływające na bezpieczeństwo haseł		Stanowisko				Różnica (R%)
		Kierownicze		Wykonawcze		
		Liczba odpowiedzi (L)	Procent odpowiedzi (%)	Liczba odpowiedzi (L)	Procent odpowiedzi (%)	
Parametry haseł	Właściwa długość	38	78%	96	75%	3%
	Właściwa liczba grup znaków wykorzystywanych w haśle	23	66%	64	66%	0%
	Nie stosowanie ważnych dat, imion, sekwencji itp.	44	86%	106	81%	5%
	Minimalna częstotliwość zmiany hasła na rok	32	63%	60	47%	16%
Zachowanie użytkownika	Właściwe przechowywanie hasła	40	80%	108	84%	-4%
	Nieudostępnianie hasła innym osobom	22	45%	54	42%	3%
	Niewykorzystywanie jednego hasła do różnych aplikacji	27	53%	58	44%	9%
	Zmiana hasła zgodnie z zaleceniami	27	56%	64	53%	3%
	Właściwa reakcja na sytuację, gdy mogła nastąpić kompromitacja hasła	28	93%	47	92%	1%
Rozwiązania organizacyjne	Sposób uzyskiwania dostępu do zasobów systemów informatycznych zapewniający większe bezpieczeństwo	41	84%	110	81%	3%
	Zabezpieczenie przed podejrzeniem wprowadzanego hasła	44	100%	141	100%	0%

Źródło: opracowanie własne.

Wśród przebadanych pracowników, osoby na stanowiskach kierowniczych korzystały z przedmiotów uwierzytelniających znacząco częściej (23 osoby

tj. 46% grupy kierowników), niż pracownicy zatrudnieni na stanowiskach wykonawczych (38 osób tj. 27% tej grupy). Kierownicy mieli częściej konta indywidualne (o 21%), jednak też częściej (18%) udostępniali swój przedmiot uwierzytelniający innym (vide tabela 6.3.).

Tabela 6.3. Porównanie elementów wpływających na bezpieczeństwo użycia przedmiotów przez kierowników i pracowników na stanowiskach wykonawczych

Element	Stanowisko				Różnica (R%)
	Kierownicze		Wykonawcze		
	Liczba odpowiedzi (L)	Procent odpowiedzi (%)	Liczba odpowiedzi (L)	Procent odpowiedzi (%)	
Udostępnianie przedmiotu innym osobom	7	30%	18	49%	-18%
Przestrzeganie zasad związanych z przechowywaniem przedmiotu	16	76%	28	76%	1%
Reakcja na sytuację, gdy mogło nastąpić przejęcie przedmiotu przez osobę postronną	6	86%	6	86%	0%
Sposób uzyskiwania dostępu do zasobów systemów informatycznych	22	100%	30	79%	21%

Źródło: opracowanie własne.

Porównano, jak te dwie grupy oceniają swoją wiedzę (tabela 6.4.). Kierownicy deklarowali wyższą wiedzę dotyczącą bezpiecznego uwierzytelniania się niż osoby na stanowiskach wykonawczych.

Tabela 6.4. Porównanie samooceny respondentów w obszarze bezpieczeństwa stosowania uwierzytelnienia przez kierowników i pracowników na stanowiskach wykonawczych

	Samoocena wiedzy dotyczącej bezpieczeństwa uwierzytelniania		
	Niska	Przeciętna	Wysoka
Kierownicy	0%	28%	72%
Pracownicy wykonawczy	1%	44%	56%

Źródło: opracowanie własne.

Porównano obie grupy w kwestii posiadania kompetencji informatycznych nabytych formalnie (przeszkolenie informatyczne) lub poprzez praktykę (praca

w branży IT). Więcej osób pracujących na stanowiskach wykonawczych wykazywało związek z informatyką (tabela 6.5.).

Tabela 6.5. Porównanie respondentów w obszarze formalnego lub praktycznego związku z obszarem IT

	Profesjonalista IT	
	Nie	Tak
Kierownicy	32%	68%
Pracownicy wykonawczy	28%	72%

Źródło: opracowanie własne.

6.2. Ocena siły wpływu działań przełożonych na motywację podwładnych do bezpiecznego korzystania z tożsamości cyfrowych

Na pytanie dotyczące znaczenia działań przełożonych w motywowaniu do bezpiecznego korzystania z tożsamości cyfrowej, odpowiedzi udzieliło średnio ok. 49 (97%) kierowników oraz 135 (96%) osób na stanowisku wykonawczym. Porównano średnie wagi przypisane poszczególnym działaniom przełożonych przez obie badane grupy. Każde z działań motywujących do bezpiecznego korzystania z tożsamości cyfrowych było oceniane jako ważniejsze przez grupę pracowników wykonawczych, a w szczególności: motywacja finansowa, szkolenia cykliczne, wyznaczanie i komunikowanie zasad oraz bieżąca kontrola. Stąd można wysnuć wniosek, że kierownicy nie doceniają znaczenia ich działań dla polepszenia bezpieczeństwa zasobów ich zakładu pracy (vide tabela 6.6.).

Tabela 6.6. Porównanie średnich ocen znaczenia poszczególnych działań przełożonych w motywowaniu do bezpiecznego korzystania z tożsamości cyfrowych

Działania przełożonych oceniane w skali 1 (nieważne) do 5 (bardzo ważne)	Stanowisko		Różnica
	Kierownicze	Wykonawcze	
Znaczenie w motywowaniu do bezpiecznego korzystania z dostępu do danych - zapewnienie wsparcia technicznego i merytorycznego	3,53	3,89	-0,36
Szkolenie dot. zasad bezpiecznego korzystania z systemów informatycznych podczas wdrażania do pracy	3,20	3,54	-0,34
Szkolenia cykliczne (utrwalające) dot. zasad bezpiecznego korzystania z systemów informatycznych	2,59	2,98	-0,39
Konsultacje dotyczące zasad i narzędzi uwierzytelniania	3,08	3,22	-0,14
Wyznaczanie i komunikowanie zasad dot. bezpiecznego korzystania z systemów informatycznych	3,12	3,50	-0,38
Ocena pracy pracownika w aspekcie bezpiecznego użytkowania systemów informatycznych	2,71	2,89	-0,18
Bieżąca kontrola i reagowanie na nieprzestrzeganie zasad	3,08	3,46	-0,38
Motywacja finansowa	3,20	3,67	-0,48

Źródło: opracowanie własne.

6.3. Preferencje dotyczące metod i parametrów uwierzytelnienia

Na pytanie, dotyczące preferowanej głównej metody uwierzytelnienia, odpowiedzi udzieliło 188 (93%) respondentów. Większość z nich (85%) wybrała loginy i hasła (tabela 6.7.). W tej kwestii nie zaobserwowano znaczących statystycznie różnic między pracownikami na stanowiskach kierowniczych i wykonawczych. Pracownicy wykonawczy chętniej wybierali rozwiązania oparte o posiadanie przedmiotu (prawie 9% wobec 4% wyborów kierowników), natomiast kierownicy bardziej preferowali symbol odblokowania (6% wobec 3,6% wyborów pracowników wykonawczych). Jednak wnioski należałoby wysnuwać z zachowaniem ostrożności z uwagi na liczebność próby i małe różnice wyników.

Tabela 6.7. Rozkład odpowiedzi respondentów dotyczących preferowanej metody uwierzytelnienia wybranej przez nich jako optymalnej

	Główna metoda uwierzytelnienia	Liczba odpowiedzi (L)	Procent odpowiedzi (%)
Stanowisko kierownicze	Loginy i hasła	43	86%
	symbol odblokowania	3	6%
	Przedmiot	1	2%
	Przedmiot + PIN	1	2%
	Biometria	2	4%
Stanowisko wykonawcze	Loginy i hasła	116	84,1%
	Symbol odblokowania	5	3,6%
	Przedmiot	4	2,9%
	Przedmiot + PIN	8	5,8%
	Biometria	5	3,6%

Źródło: opracowanie własne.

Respondentów poproszono o określenie wytycznych dotyczących haseł, które byłyby optymalne dla ich zakładów pracy (vide tabela 6.8.). Badani najczęściej określali długość hasła (86% respondentów, którzy udzielili odpowiedzi na pytanie dotyczące charakteru ich stanowiska) i jego skład (87% z nich). Rzadziej deklarowano chęć ustalenia daty ważności hasła (60%), zakaz stosowania ryzykownych treści w hasłach (40%) czy wykorzystywania jednego hasła do wielu aplikacji (30%).

Tabela 6.8. Rozkład odpowiedzi dotyczących optymalnych wytycznych dotyczących haseł, które byłyby optymalne według respondentów w rozbiciu na kierowników i pracowników wykonawczych

	Stanowisko				
	Kierownicze		Wykonawcze		
	Liczba odpowiedzi (L)	Procent odpowiedzi (%)	Liczba odpowiedzi (L)	Procent odpowiedzi (%)	Różnica (R%)
Długość hasła	42	82%	123	87%	-5%
Liczba grup znaków w haśle	44	86%	123	87%	-1%
min. 1 duża i 1 mała litera	36	71%	88	62%	8%
min. 1 cyfra	40	78%	107	76%	3%
min. 1 znak specjalny	25	49%	55	39%	10%
Częstotliwość zmian hasła w ciągu roku	30	59%	85	60%	-1%
Zakaz stosowania haseł w różnych aplikacjach	16	31%	42	30%	2%
Zakaz stosowania w hasłach ważnych dat, imion, prostych słów czy sekwencji (np. 12345)	19	37%	58	41%	-4%

Źródło: opracowanie własne.

Respondenci na stanowiskach kierowniczych preferowali większą minimalną długość haseł oraz ich większą złożoność, podczas gdy pracownicy na stanowiskach wykonawczych preferowali hasła o krótszym okresie ważności (tabela 6.9.).

Tabela 6.9. Porównanie optymalnych parametrów haseł określonych przez respondentów zajmujących stanowiska kierownicze i wykonawcze

	Stanowisko		
	Kierownicze	**Wykonawcze**	
	Wartość średnia	**Wartość średnia**	**Różnica**
Długość hasła	8,57	8,24	0,33
Liczba grup znaków w haśle	3,11	2,75	0,37
Częstotliwość zmian hasła w ciągu roku	5,93	8,71	-2,77

Źródło: opracowanie własne.

Zbadano bezpieczeństwo haseł tworzonych w oparciu o wytyczne dotyczące parametrów haseł podane przez respondentów. Przyjęto, że hasła spełniające minimalne wymogi bezpieczeństwa charakteryzują się długością min. 8 znaków, składają się z min. 3 grup znaków oraz są zmieniane min. 2 razy na rok. Wytyczne, które wymuszają na użytkowniku stworzenie hasła spełniającego minimalne wymogi bezpieczeństwa, zostały podane przez 43% respondentów należących do grupy kierowników oraz 33% pracowników wykonawczych (tabela 6.10.).

Tabela 6.10. Ocena haseł tworzonych w oparciu o wymogi dotyczące parametrów haseł podane przez respondentów

Spełnienie minimalnych wymogów bezpieczeństwa	**Stanowisko**			
	Kierownicze		**Wykonawcze**	
	Liczba odpowiedzi (L)	**Procent odpowiedzi (%)**	**Liczba odpowiedzi (L)**	**Procent odpowiedzi (%)**
Tak	22	43%	47	33%
Nie	29	57%	94	67%

Źródło: opracowanie własne.

6.4. Luka w podejściu do tożsamości cyfrowych w grupach stanowisk kierowniczych i podwładnych

Osoby zajmujące kierownicze stanowiska generalnie korzystają ze swojej tożsamości cyfrowej w sposób bardziej bezpieczny. Hasła ponad połowy z nich charakteryzują się średnim lub wysokim poziomem bezpieczeństwa (vide rozdz. 6.1).

Również wytyczne dotyczące optymalnych haseł częściej spełniają minimalne wymogi bezpieczeństwa, niż wytyczne pracowników zajmujących stanowiska wykonawcze (rozdz. 6.3).

Jednakże kierownicy przypisują mniejszą wagę działaniom przełożonych, które mogą wpłynąć pozytywnie na bezpieczeństwo zasobów informatycznych (rozdz. 6.2).

Stąd wynikają dwie luki kompetencyjne (rozumiane jako niedostosowanie kompetencji pracowników do wymagań w zakresie wdrażania strategii rozwoju organizacji [33]):

1. Luka kompetencji pracownika w obszarze wiedzy dotyczącej bezpieczeństwa.
2. Luka kompetencji kierownika w obszarze motywacji pracowników.

[33] Manuszak, M., (2019). *Profile kompetencyjne menedżerów sektora publicznego*. Studia i prace Kolegium zarządzania i Finansów, Zeszyt naukowy nr 172, Oficyna Wydawnicza SGH, s. 126.

7. Podsumowanie badań

W rozdziale zawarto ostateczną postać modelu DIAM wraz z jego interpretacją, wnioski wynikające z analizy wykorzystania tożsamości cyfrowych w małych i średnich przedsiębiorstwach, oraz proponowane rekomendacje dla kadry menedżerskiej. Nakreślono także obszary, których eksploracja może być wartościowa pod względem naukowym.

7.1. Wnioski dotyczące praktyki stosowania tożsamości cyfrowych w małych i średnich przedsiębiorstwach oraz dalsze kierunki badań

Wniosek 1. Polityka bezpieczeństwa nie jest wdrożona w wielu przedsiębiorstwach.

Nie ma możliwości kompleksowego zabezpieczenia dostępu do zasobów przedsiębiorstwa bez przygotowania i wdrożenia polityki bezpieczeństwa, a tej brakowało w około 40% badanych przedsiębiorstw.

Brak wdrożenia polityki bezpieczeństwa niesie ze sobą skutki w co najmniej dwóch obszarach:

1. W razie wystąpienia incydentu naruszenia bezpieczeństwa – narażenie na konsekwencje prawne (odpowiedzialność karna i z powództwa cywilnego), finansowe, wizerunkowe, utrata potencjalnych korzyści do bankructwa włącznie.
2. Słabość przedsiębiorstwa, polegająca na braku procedur, niedookreślenia obowiązków zarówno przełożonych, jak i ich podwładnych, która może dezorganizować pracę i prowokować incydenty naruszenia bezpieczeństwa, zwiększając wpływ tzw. czynnika ludzkiego na systemy informatyczne. Jest to także niedostosowanie do warunków konkurowania i może stanowić czynnik powodujący utratę udziału w rynku.

Brak polityki bezpieczeństwa pozostawia wiele kwestii w gestii pracownika (tylko niecała połowa respondentów deklarowała istnienie wytycznych dotyczących zabezpieczania zasobów za pomocą haseł); i to od jego wiedzy i chęci (lub ich braku) uzależnione jest bezpieczeństwo informacyjne przedsiębiorstwa.

Fakt, że badana była wiedza pracowników (niekoniecznie top managementu), obnaża w tej sferze braki np. brak świadomości czy przedsiębiorstwo posiada w ogóle jakąś politykę bezpieczeństwa. Zastanawiający jest stosunkowo duży odsetek tych osób. Taka sytuacja jest niebezpieczna, ponieważ daje fałszywe poczucie bezpieczeństwa zarządowi.

W ramach dalszych badań warto rozważyć następujące kwestie:

1. Jakie są przyczyny braku skutecznego wdrożenia polityki bezpieczeństwa w małych i średnich przedsiębiorstwach?
2. Jakie etapy wdrożenia polityki bezpieczeństwa są najbardziej problematyczne i jak można je wspomóc?
3. Jaka jest sprawność delegowania obowiązków związanych z bezpieczeństwem w przedsiębiorstwach?

Wniosek 2. ***Hasła są nadal najpopularniejszym sposobem zabezpieczenia zasobów, na drugim miejscu są przedmioty. Rozwiązania biometryczne są nadal nowością. Jednak ponad 40% badanych przedsiębiorstw stosuje także przedmioty uwierzytelniające i biometrię.***

Hasła są podstawowym narzędziem zabezpieczenia dostępu do zasobów systemów informatycznych przedsiębiorstwa.

Wniosek 3. ***Narzędzia uwierzytelnienia o różnej charakterystyce są stosowane w odmienny sposób.***

Częstotliwość stosowania poszczególnych metod zabezpieczenia tożsamości cyfrowych jest znacząco różna. Najczęściej stosowane w czasie przeciętnego dnia pracy narzędzia to symbol odblokowania oraz czytnik linii papilarnych. Duże odchylenie standardowe sugeruje, że istnieje dodatkowy czynnik różnicujący. Może nim być np. urządzeń mobilnych (np. telefonów), które nie są w użyciu ciągłym i mogą wymagać odblokowania przed każdym użyciem.

Na drugim końcu skali częstotliwości użycia są karty kodów jednorazowych (stosowane często w bakowości) oraz karty elektroniczne zabezpieczone numerem PIN. Te odpowiedzi mają jednocześnie najniższą wartość odchylenia standardowego, stąd można domniemywać, że są używane w podobny sposób przez respondentów.

Hasła są wykorzystywane w zróżnicowany sposób, na co wskazuje wysoka wartość odchylenia standardowego, a sposób ich stosowania wart jest dalszego badania.

Warto zatem zbadać następujące założenia:

1. Liczba stosowanych haseł koreluje z poziomem bezpieczeństwa, które należy zapewnić.
2. Hasła są stosowane domyślnie do wielu aplikacji, bez analizy potrzeb w zakresie ich ochrony.
3. Dla bezpieczeństwa zasobów systemów informatycznych lepsze jest stosowanie haseł o zróżnicowanej uciążliwości (liczba, skład i liczba wprowadzeń do systemu w ciągu dnia) niż standardowe, ujednolicone wytyczne dla haseł dostępu do newralgicznych i wspomagających danych/aplikacji.

4. Tam, gdzie stosowane są różne metody uwierzytelnienia, przedmioty służą zabezpieczeniu dostępu do kluczowych danych/aplikacji, a hasła do pozostałych celów.

Wniosek 4. Konstrukcja haseł wielu respondentów nie spełnia standardów bezpieczeństwa.

Respondenci deklarują znaczną dowolność w kwestii haseł - niemal co trzeci respondent sam decydował o zastosowaniu haseł oraz ich składzie. Stąd niska jakość wielu haseł (zbyt krótkie, zbyt proste).

Warto zbadać w jakim stopniu przedsiębiorstwa stosują strategie ochrony zasobów za pomocą haseł (np. ochrona tylko zasobów kluczowych, zróżnicowane standardy haseł dla różnych zasobów, delegowanie uprawnień do ustalania parametrów haseł na bezpośrednich przełożonych itp.).

Wniosek 5. Indywidualne narzędzia uwierzytelniające są niewystarczająco chronione przed nieautoryzowanym dostępem.

Ponad połowa respondentów udostępnia swoje hasła i przedmioty innym, co stanowi naruszenie bezpieczeństwa.

Warto zbadać czym jest to spowodowane: niefrasobliwością pracowników, którzy chcą ułatwić sobie pracę czy też koniecznością, wynikającą z niewłaściwego przyporządkowania zasobów do pracowników, którzy, aby wykonać swoje obowiązki muszą korzystać z haseł lub przedmiotów innych pracowników. Być może jest też pozytywny aspekt tej sytuacji np. lepsza kooperacja i praca zespołowa wynikająca z zaufania?

Blisko połowa respondentów nie ma wytycznych co do częstotliwości zmiany hasła, co zwiększa prawdopodobieństwo złamania hasła podczas cyberataku.

Warto zbadać czy jest to wynikiem niezarządzania hasłami pracowników w ogóle, czy też ustawienia maksymalnej daty ważności hasła jest celowo pomijane.

7.2. Model DIAM

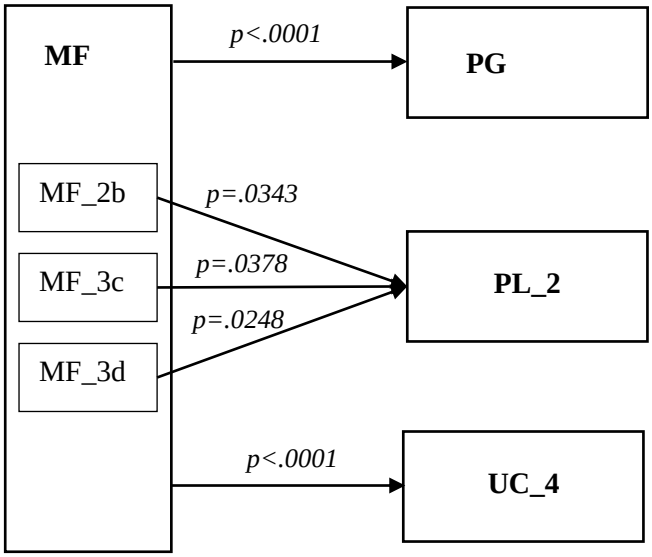
Badanie rzetelności skali i spójności pytań za pomocą współczynnika Alfa-Cronbacha potwierdziło, że metoda uwierzytelnienia stanowi istotny czynnik różnicujący odpowiedzi. Stąd wyodrębniono cztery obszary modelu DIAM:

- niezróżnicowany narzędziem uwierzytelniającym (DIAM-0),
- dotyczący uwierzytelnień za pomocą hasła (DIAM-H),
- dotyczący uwierzytelnień za pomocą przedmiotu (DIAM-P),
- dotyczący uwierzytelnień za pomocą biometrii (DIAM-B).

Wyciągnięto wnioski dotyczące wpływu zarządzania lub poszczególnych działań na pracowników i uwierzytelnienie w małych i średnich przedsiębiorstwach.

7.2.1. DIAM-0

Ta część modelu, której elementy nie odnoszą się do konkretnych narzędzi uwierzytelnienia, opisuje wpływ czynników zarządczych (MF) na postrzegane korzyści (PG), straty (PL_2) z tytułu bezpiecznego uwierzytelniania się, oraz postrzeganie własnej wiedzy dotyczące bezpieczeństwa uwierzytelnienia (UC_4).



Rysunek 7.1. Model DIAM-0
Źródło: opracowanie własne.

Wniosek 6. ***Odpowiednie zarządzanie kształtuje postrzeganie zalet bezpiecznego korzystania z uwierzytelnienia.***

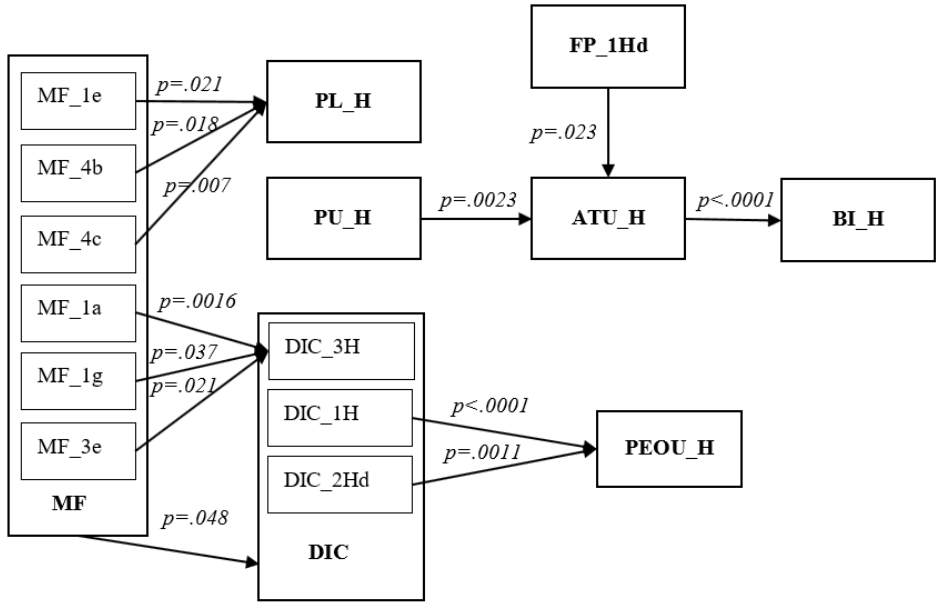
Wniosek 7. ***Szczególnie znaczenie ma kształtowanie bezpieczeństwa na poziomie strategicznym (podejście top managementu, budowa strategii oraz kultura organizacyjna) – działania w tym obszarze przekładają się na większą świadomość korzyści płynących z bezpiecznego uwierzytelnienia u pracowników.***

Wniosek 8. ***Jasne ustalenie kwestii związanych z dostępem do systemów informatycznych i ich egzekwowanie przez dobrze zmotywowanych***

kierowników, oraz wpisanie bezpieczeństwa dostępu do danych w strategię przedsiębiorstwa, zmniejszają postrzeganą stratę związaną z bezpiecznym uwierzytelnieniem się.

Wniosek 9. ***Dobre zarządzanie przekłada się na większą wiedzę dotyczącą bezpieczeństwa uwierzytelniania się pracowników.***

7.2.2. DIAM-H



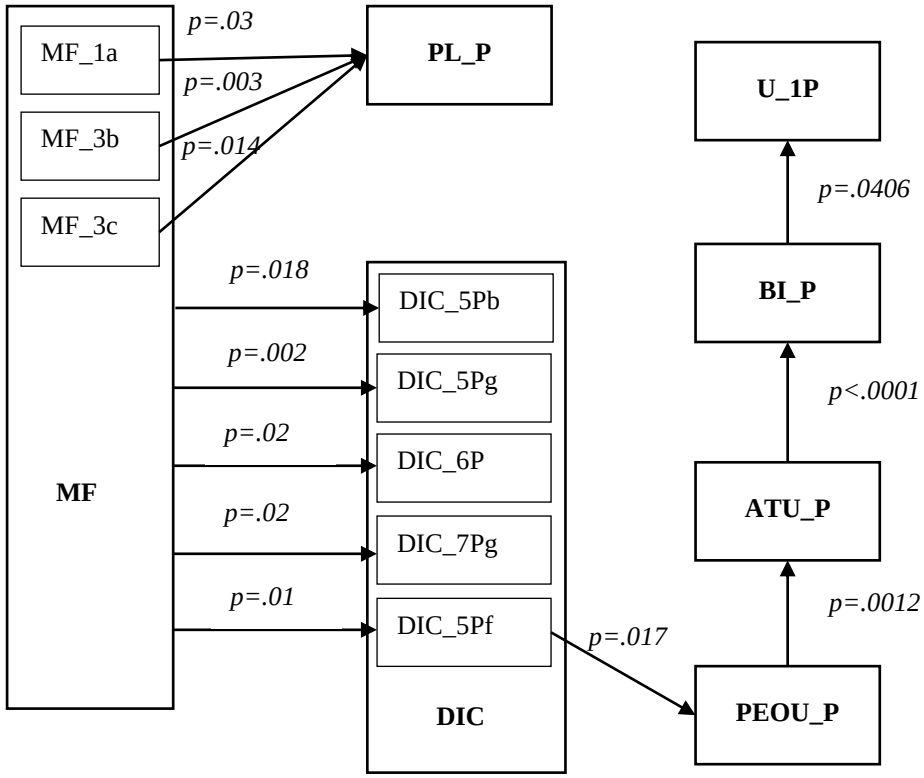
Rysunek 7.2. Model DIAM-H

Źródło: opracowanie własne.

Wniosek 10. ***Dobra organizacja pracy oraz szerokie kompetencje kadry technicznej i kierowniczej, zmniejszają postrzeganą stratę wynikającą z bezpiecznego uwierzytelniania się za pomocą haseł.***

Wniosek 11. ***Zapewnienie pracownikom łatwego do uzyskania wsparcia technicznego oraz kontrola ich działań wspiera częstsze stosowanie haseł w czasie codziennej pracy.***

7.2.3. DIAM-P



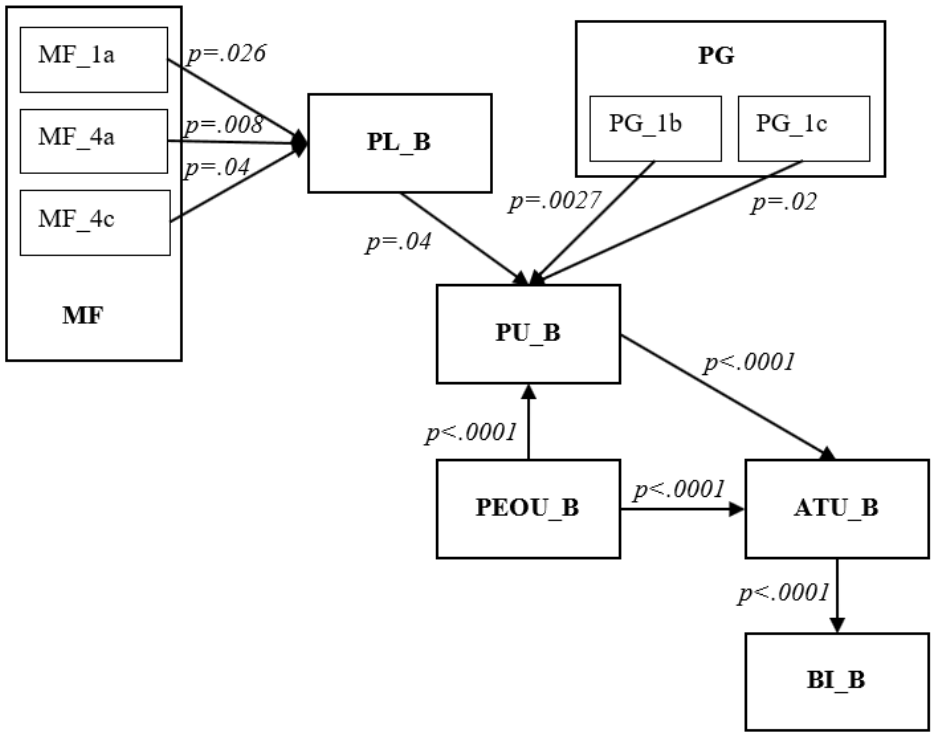
Rysunek 7.3. Model DIAM-P

Źródło: opracowanie własne.

Wniosek 12. ***Jasne określenie kwestii związanych z bezpieczeństwem uwierzytelniania się oraz stosowanie wskaźników oceny kosztów i korzyści zabezpieczenia dostępu do danych, zmniejszają postrzeganą stratę z tytułu korzystania z przedmiotów uwierzytelniających w sposób bezpieczny.***

Wniosek 13. ***W dobrze zarządzanych przedsiębiorstwach częściej stosowane są przedmioty uwierzytelniające.***

7.2.4. DIAM-B



Rysunek 7.4. Model DIAM-B

Źródło: opracowanie własne.

Wniosek 14. ***Świadomość konieczności dostosowania się do nowych wyzwań rynku, a także łatwość uzyskania wsparcia technicznego i szerokie kompetencje kadry biznesowej i technicznej zmniejszają poczucie straty z tytułu wykorzystania uwierzytelnienia biometrycznego.***

7.3. Interpretacja luki między podejściem do tożsamości cyfrowej reprezentowanym przez pracowników wykonawczych i kierowników

Wniosek 15. ***Na podstawie wniosków z rozdziału 6 można przyjąć, że w badanej grupie kierownicy są generalnie bardziej kompetentni w kwestii stosowania uwierzytelnień, niż pracownicy na stanowiskach wykonawczych. Wynika to zarówno ze sposobu, w jaki stosują uwierzytelnienia, jak i wyboru optymalnych wytycznych (luka kompetencji).***

Obszarem wartym dalszego badania jest przyczyna, dla której kierownicy wybrali rozwiązania bardziej bezpieczne. Warto podkreślić, że działo się tak pomimo faktu, że więcej respondentów na stanowiskach wykonawczych deklarowało bycie profesjonalistą w obszarze IT. Z drugiej strony to kierownicy lepiej oceniali swoją wiedzę dotyczącą bezpieczeństwa uwierzytelniania się.

Przyczyny tego stanu rzeczy, które są godne rozważenia to m.in.:

- wiedza – nabyta poprzez szkolenia, uświadomienie sobie skutków kompromitacji danych (np. podczas szkolenia podwładnych), współtworzenie polityki bezpieczeństwa itp.;
- odpowiedzialność – włączenie kwestii związanych z polityką bezpieczeństwa w sferę odpowiedzialności kierownika (planowanie i organizowanie zasobów, kontrolowanie oraz motywowanie pracowników), podobnie jak świadomość odpowiedzialności za działania podwładnych w obszarze uwierzytelnień (także karnej);
- spójność – zachowanie spójności wymagań wobec innych i własnego postępowania;
- uznanie autorytetu – przyjęcie wytycznych dotyczących bezpieczeństwa opracowanych przez osoby, które uznane zostały za specjalistów w ob.-szarze, w którym kierownicy nie czuli się kompetentni.

Wniosek 16. ***Na podstawie wniosków z rozdziału 6 można wywnioskować, że kierownicy nie doceniają roli, jaką pełnią w kształtowaniu zachowań swoich podwładnych związanych z uwierzytelnieniem się (luka oczekiwań).***

Stąd, w ramach dalszych badań warto określić:

- W jakim stopniu kierownicy są świadomi możliwości kształtowania postaw pracowników w obszarze bezpieczeństwa?
- W jaki sposób można tę świadomość zmienić?
- Na ile bezpieczeństwo zasobów jest postrzegane jako priorytet w bieżącym funkcjonowaniu przedsiębiorstwa?

Wniosek 17. ***Przełożeni mają wpływ na kształtowanie samych pracowników, nie tylko na efekty ich pracy. Może to być uzupełnieniem zabezpieczeń w warstwie technicznej i organizacyjnej.***

Warto określić:

- W jakim stopniu pozytywna postawa wobec bezpiecznego uwierzytelnienia się zwiększa bezpieczeństwo zasobów?

7.4. Zalecenia dla kadry menedżerskiej

Na podstawie badań sformułowano szereg rekomendacji dla osób zarządzających przedsiębiorstwem, które mogą być przydatne zarówno na wyższym jak i niższym szczeblu zarządzania, a dotyczą różnych aspektów zabezpieczenia zasobów przedsiębiorstwa.

Rekomendacje (tabela 7.1.) oparto o sformułowane uprzednio zalecenia (rozdział 5.3) i wnioski (rozdziały 6.1 – 6.3).

Tabela 7.1. Źródła rekomendacji na potrzeby managementu

Obszar	Nr rekomendacji	Podstawa sformułowania zalecenia
Projektowanie systemu bezpieczeństwa informacji	1	W1, W7, W8, Z23, Z29
	2	W2, W3, W4, W5, W12, W13, Z34, Z35, Z36
	3	W5, W8, W10, W12, Z17, Z22, Z24, Z36
	4	W11, W14, Z18, Z21, Z26, Z34, Z37, Z39
	5	W2, W4, W8, W15, Z17, Z33
	6	W4, W5
Działania i kompetencje przełożonych	7	W5, W8, W11, W12, Z17, Z22, Z24
	8	W8, W11, W14, Z14, Z19, Z38
	9	W16, Z14
	10	W10, W14, W15, Z14, Z18, Z21, Z27, Z28, Z31, Z37
	11	W9, Z17, Z40
Kształtowanie postaw pracowników	12	Z9, Z10, Z11
	13	Z15, Z16
	14	Z14, Z22, Z26
	15	Z8
	16	Z12
Zalecenia dot. wprowadzania uwierzytelnienia biometrycznego	17	W13, Z2, Z6, Z9
	18	Z13, Z21, Z28
	19	Z3, Z4
	20	Z5, Z7

W – wnioski (rozdz. 6.1-6.3), Z – zależności (rozdz. 5.3)

Źródło: opracowanie własne.

Projektowanie systemu bezpieczeństwa informacji:

Rekomendacja 1. Należy bezwzględnie opracować i wdrożyć politykę bezpieczeństwa, a kwestie bezpieczeństwa traktować priorytetowo.

Rekomendacja 2. Należy stosować narzędzia uwierzytelnienia adekwatne do znaczenia chronionych zasobów i ryzyka, które powodowałoby ich skompromitowanie; w miarę możliwości, należy wprowadzić silniejsze zabezpieczenia oparte o przedmioty lub biometrię.

Rekomendacja 3. Należy jasno określić kwestie związane z dostępem pracowników do zasobów systemów informatycznych na podstawie ich ról biznesowych (tj. określić dostępne zasoby, uprawnienia, narzędzia uwierzytelnienia i zasady związane z ich używaniem).

Rekomendacja 4. Należy zapewnić dobrze działający system wsparcia procesu uzyskiwania dostępu do zasobów (przypisanie odpowiednich obowiązków przełożonym i/lub powołanie działu wsparcia IT).

Rekomendacja 5. Należy zaimplementować rozwiązania techniczne wymuszające stosowanie bezpiecznych haseł (długość i skład hasła oraz jego maksymalna data ważności).

Rekomendacja 6. Należy aktywnie identyfikować użytkowników stanowiących zagrożenie dla bezpieczeństwa zasobów systemów informatycznych (np. wprowadzić test kompetencji w ob.-szarze bezpieczeństwa) i poprzez oddziaływanie przełożonych dążyć do podniesienia ich kompetencji lub/i zintensyfikować kontrolę ich pracy.

Działania i kompetencje przełożonych:

Rekomendacja 7. Należy precyzyjnie zakomunikować podwładnemu kwestie związane z dostępem do systemów informatycznych (tj. obowiązki, zasady bezpieczeństwa i konsekwencje ich łamania).

Rekomendacja 8. Należy kontrolować działania pracowników w kwestii uwierzytelnienia się i budować kulturę organizacyjną wspierającą bezpieczeństwo zasobów systemów informatycznych.

Rekomendacja 9. Należy zintensyfikować wykorzystanie już posiadanych przez kierowników uprawnień i narzędzi wpływu w celu poprawy bezpieczeństwa zasobów.

Rekomendacja 10. Należy dążyć do zwiększenia kompetencji kierowników, także w obszarze bezpieczeństwa informatycznego.

Rekomendacja 11. Należy włączyć kwestie dotyczące uwierzytelnień do szkoleń wstępnych i cyklicznych, w celu podniesienia samooceny wiedzy pracowników oraz postrzeganie przez nich korzyści z tytułu bezpiecznego stosowania uwierzytelnień.

Kształtowanie postaw pracowników wobec bezpiecznego uwierzytelniania się:

Rekomendacja 12. Jednym z kierunków działań, mających na celu zapewnienie bezpieczeństwa zasobów systemów informatycznych, powinno być zwiększenie akceptacji stosowanych metod uwierzytelnienia poprzez kształtowanie pozytywnej postawy.

Rekomendacja 13. Podczas ustalania wytycznych dotyczących budowy haseł należy uwzględnić ograniczone możliwości człowieka w kwestii zapamiętywania ciągów znaków. Czynnikami, które w największym stopniu zwiększają postrzeganą trudność stosowania haseł w sposób bezpieczny są długość hasła oraz konieczność stosowania w haśle znaków specjalnych.

Rekomendacja 14. Należy jasno określić zasady dotyczące kont pracowniczych oraz zapewnić szybkie i właściwe przydzielanie dostępu do koniecznych zasobów w celu zmniejszenia postrzegania przez pracownika strat na efektywności z tytułu bezpiecznego stosowania haseł.

Rekomendacja 15. Należy położyć nacisk na przekonanie pracowników, że stosowanie haseł w sposób bezpieczny jest dla nich użyteczne.

Rekomendacja 16. Wybierając przedmioty uwierzytelniające należy uwzględnić wygodę i łatwość ich użytkowania.

Zalecenia dotyczące zmniejszania oporu pracowników podczas wprowadzania uwierzytelnienia biometrycznego:

Rekomendacja 17. Warto zaadaptować rozwiązania oparte o przedmioty uwierzytelniające, ponieważ pozytywne doświadczenia pracowników w pracy z przedmiotami zwiększają otwartość pracowników na metody biometryczne.

Rekomendacja 18. Wybierając metody biometryczne służące uwierzytelnieniu należy uwzględnić wygodę i łatwość ich użytkowania, a także zapewnić wsparcie techniczne i merytoryczne.

Rekomendacja 19. Warto informować pracowników o zaletach uwierzytelnienia biometrycznego (szczególnie o redukcji odpowiedzialności np. karnej oraz świadomość dopełnienia obowiązków).

Rekomendacja 20. Warto podkreślać wady haseł i ich uciążliwość by przekonać pracownika do stosowania metod biometrycznych, ponieważ największymi zwolennikami metody biometrycznych są osoby niezadowolone z haseł (wskazujące na ich uciążliwość, nisko oceniające ich przydatność oraz posiadające relatywnie najmniej pozytywną postawę wobec haseł).

Zakończenie

W toku prac okazało się, że narzędzie uwierzytelnienia stanowi istotny czynnik wpływający na postrzeganie uwierzytelnienia przez pracowników. Wyniki zdają się potwierdzać również, że stosunek do danego narzędzia uwierzytelnienia przekłada się na chęć wykorzystywania go w sposób bezpieczny. Stąd istotne znaczenie i potrzeba kształtowania postawy pracownika.

Narzędziem, które może być do tego wykorzystane jest model DIAM, którego kwantyfikacja była **głównym celem pracy**. Wyodrębniono cztery obszary modelu DIAM: zależności uniwersalne oraz dotyczące uwierzytel-nienia za pomocą hasła, przedmiotu i biometrii. Dzięki temu udało się zidenty-fikować, jaki wpływ na pracowników wywiera sposób zarządzania, jakie czynniki i w jakim stopniu kształtują ich postawę.

Analiza materiału badawczego pozwoliła wysnuć wnioski na temat **sposobu wykorzystania tożsamości cyfrowych przez pracowników małych i średnich przedsiębiorstw (pierwszy cel poznawczy).** Zatrważające jest, że tylko 60% badanych deklarowało, że ich przedsiębiorstwa posiadały politykę bezpieczeństwa. W tym kontekście nie dziwi fakt, że ponad 30% respondentów samodzielnie decydowało o stosowaniu haseł, a prawie 60% udostępnia je innym. Oznacza to także, że przedsiębiorstwa sektora MSP nie były gotowe na zmiany, jakie niesie ogólne rozporządzenie o ochronie danych (RODO), które weszło w życie 25 maja 2018 r.

Badanie preferencji pracowników (drugi cel poznawczy) ujawniło, że respondenci preferowali bezpieczniejsze hasła niż te, których używali obecnie. Jednak, mimo, iż 40% respondentów deklarowało stosowanie narzędzi uwierzytelniających, które charakteryzują się wyższym poziomem bezpieczeństwa niż hasła, nie były one preferowane jako główne narzędzie uwierzytelnienia przez pracowników. W przypadku rozwiązań biometrycznych użytkownicy byli bardzo podzieleni.

Ciekawe wnioski wysnuć można z **porównania odpowiedzi osób na stanowiskach kierowniczych i wykonawczych (trzeci cel poznawczy).** Zestawiono wyniki tych dwóch grup w kwestii preferowanych narzędzi i zasad uwierzytelnienia, obecnego sposobu korzystania z tożsamości cyfrowej, a także siły wpływu działań przełożonych na pracowników. Pomimo faktu, że większym odsetkiem osób związanych z IT charakteryzowała się grupa pracowników wykonawczych, to kierownicy lepiej chronili swoją tożsamość cyfrową. Stosowali oni silniejsze hasła, które częściej zmieniali oraz częściej korzystali z przedmiotów uwierzytelniających. Podobne zależności ujawnia porównanie preferencji co do stosowanych zabezpieczeń. Pokrywało się to również z samo-oceną wiedzy dotyczącej bezpieczeństwa uwierzytelnienia, która była znacząco wyższa w przypadku osób na stanowisku kierowniczym. Przeczy to zatem intuicyjnemu założeniu, że osoby z wykształceniem informatycznym lub/i pracujące w branży związanej z wykorzystaniem komputerów, a przez to,

wydawałoby się, świadome zagrożeń i ich skutków, lepiej dbają o bezpieczeństwo tożsamości cyfrowych. W dobie rosnących zagrożeń systemów informatycznych jest to istotna przesłanka do wzbogacenia programów nauczania informatyki o treści związane z zapewnieniem bezpieczeństwa teleinformatycznego.

Zidentyfikowano także lukę związaną z relacjami między przełożonym a podwładnym. Według kierowników, siła wpływu przełożonych na podwładnych była niższa, niż w ocenie pracowników na stanowisku wykonawczym. Może to wskazywać na potrzebę refleksji kadry kierowniczej co jej do znaczenia w organizacji.

W pracy postawiono jeden **cel utylitarny: sporządzenie rekomendacji dla kadry zarządzającej**. Cel ten został zrealizowany poprzez przygotowanie czterech zestawów rekomendacji, przydatnych w następujących obszarach: projektowanie systemu bezpieczeństwa informacji, działania i kompetencje przełożonych, kształtowanie postaw pracowników wobec bezpiecznego uwierzytelniania się oraz wprowadzanie uwierzytelnienia biometrycznego.

Wnioskowanie z niniejszej pracy jest ograniczone z jednej strony próbą badawczą, a konkretnie jej doborem (przypadkowa nie losowa), lokalizacją badanych przedsiębiorstw (duży udział województwa lubelskiego i świętokrzyskiego), charakterystyką użytkowników (nadreprezentacja osób młodych i związanych z branżą IT). Z drugiej strony, mamy do czynienia z dynamicznym rozwojem narzędzi uwierzytelnienia (w szczególności biometrycznych) oraz nasileniem zagrożeń, co może przełożyć się na dezaktualizację zarówno rekomendacji jak i samego modelu za jakiś czas.

Bibliografia

1. *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: 30.11.2021.
2. Aczel, A.D. (2007). *Statystyka w zarządzaniu*, Warszawa: Wydawnictwo Naukowe PWN, s. 269.
3. *Analiza rzetelności i pozycji*. StatSoft. Online: http://www.statistica.pl/textbook/stathome_stat.html?http%3A%2F%2Fwww.statistica.pl%2Ftextbook%2Fstreliab.html, dostęp, dostęp: 30.11.2021.
4. Azhar, M.I. (2017). *Systematic Review of Identity Access Management in Information Security*. International Journal Of Innovations In Engineering Research And Technology [IJIERT], Vol. 4, Iss. 7.
5. Brar, H.S., Kumar, G. (2018). *Cybercrimes: A Proposed Taxonomy and Challenges.* Journal of Computer Networks and Communications, Vol. 2018.
6. Chen, D.Q., Liang, H. (2019). *Wishful Thinking and IT Threat Avoidance: An Extension to the Technology Threat Avoidance Theory*. IEEE Transactions on Engineering Management, Volume 66, Issue 4, s. 552–567.
7. Chmielarz, W. (2015). *Determinanty rozwoju serwisów dystrybucji treści komercyjnych w Polsce*. Problemy Zarządzania, Vol. 13, Nr 2 (52), T. 1, s. 52.
8. Davis, F.D. (1986). *Technology Acceptance Model for Empirically Testing New End-user Information Systems Theory and Results.* Unpublished Doctoral Dissertation, MIT.
9. *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representtations* (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.
10. Deming, W.E. (1993). *The New Economicst*. Cambridge: MIT Press s. 135.
11. *Dz.U. 1997 Nr 133 poz. 883 USTAWA z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.*
12. Fincher, M., Hadnagy, Ch. (2016). Mroczne odmęty phishingu. Nie daj się złowić!. Gliwice: Wydawnictwo Helion.
13. German, R.L., Barber, K.S. (2018). *Consumer Attitudes About Biometric Authentication.* UT CID Biometrics Report. Online: https://identity.utexas.edu/sites/default/files/202009/Consumer%20Attitudes%20About%20Biometrics.pdf, dostęp: 30.11.2021.
14. Jasiewicz, J. i in. (2014). *Ramowy katalog kompetencji cyfrowych*. Warszawa: Centrum Cyfrowe, 68 s. Online: https://www.academia.edu/12624330/Ramowy_Katalog_Kompetencji_Cyfrowych, dostęp: 2021.11.30.
15. Juszczyk, M. (2020). *Rozbudowa modelu akceptacji technologii dla potrzeb bezpiecznego wykorzystania tożsamości cyfrowej w małych i średnich przedsiębiorstwach. Cz. I Modelowanie*. Wydawnictwo Politechniki Lubelskiej. Lublin.
16. Kostka, G., Steinacker, L., Meckel, M. (2020). *Between Privacy and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the UK and the US*, SSRN, doi: http://dx.doi.org/10.2139/ssrn.3518857.

17. Król, K. (2015) *Organizacyjne aspekty zarządzania bezpieczeństwem danych z perspektywy zagrożeń phishingu*. Organizacja i Zarządzanie, Wyd. Kwartalnik naukowy 2 (30), Politechniki Śląskiej, s. 23–24.
18. Kumar M., Kumar N. (2020). *Cancelable Biometrics: a comprehensive survey.* Artificial Intelligence Review, Vol. 53, Iss. 5, s. 3403–3446.
19. Liu, C., Wang, N., Liang, H. (2020). *Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment*. International Journal of Information Management, Vol. 54.
20. Lu, S. i in. (2021). *Do larger audiences generate greater revenues under pay what you want? Evidence from a live streaming platform.* Marketing Science, Vol. 40, Iss. 5, s. 964-984.
21. Manuszak, M., (2019). *Profile kompetencyjne menedżerów sektora publicznego*. Studia i prace Kolegium zarządzania i Finansów, Zeszyt naukowy nr 172, Oficyna Wydawnicza SGH, s. 123-141.
22. McLeodal, A., Dolezel, D. (2022) *Information security policy non-compliance: Can capitulation theory explain user behaviors?*. Computers and Security, Vol. 112.
23. Meng, J. (2022). *Information acquisition, persuasion, and group conformity of online tribalism: Does user activeness matter?*. International Journal of e-Business Research, Vol. 18, Iss. 2.
24. 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.
25. Mitnick, K.D., Simon, W. (2016). *Sztuka podstępu. Łamałem ludzi, nie hasła*. Wyd. II. Gliwice: Wydawnictwo Helion.
26. Ogbanufe, O. (2021). *Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity*. Computers and Security, Vol. 108.
27. Ogbanufe, O., Pavur, R. (2022). *Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection*. International Journal of Information Management, Vol. 62.
28. Opitek, P. (2015). *Przestępstwo skimmingu*. Prokuratura i prawo 11, s. 66–82.
29. Pasławski, K. (2020). *Z czym nie radzą sobie MŚP*. CRN Polska. Online: https://crn.pl/aktualnosci/z-czym-nie-radza-sobie-msp/, 2021-05-21.
30. *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.*
31. Wendzel, S., Mazurczyk, W., Caviglione, L., Houmansadr, A. (2022). *Emerging topics in defending networked systems*. Future Generation Computer Systems, Vol. 128, s. 317–319.
32. Wodo, W., Ławniczak, K. (2016). *Bezpieczeństwo i biometria urządzeń mobilnych w Polsce. Badanie użytkowników 2016*. Wrocław: Wydawnictwo Politechniki Wrocławskiej, s. 9. Online: https://dbc.wroc.pl/Content/36335/Wodo_raport-bezpieczenstwo-urzadzenia-mobilne-polska-2016.pdf, dostęp 2021.11.30.