2.8. Metody statystyczne

Materiał demonstracyjny opracowano na podstawie syntetycznej bazy danych obejmującej 100 pracowników administracji. OWszystkie obliczenia wykonano za pomocą pakietu statystycznego STATISTICA (StatSoft) w wersji 13.3.. Dane nie pochodzą z rzeczywistego badania ani ze zlecenia klienta.

Celem analizy była ocena znajomości zasad bezpieczeństwa cyfrowego i ochrony danych w zależności od trybu pracy, wieku, wykształcenia oraz rodzaju stanowiska. Wykorzystano analizę opisową, graficzną oraz test niezależności chi-kwadrat Pearsona.

Przyjęto poziom istotności $\alpha = 0,05$. Wyniki z $p \leq 0,05$ uznano za istotne statystycznie i oznaczono pogrubieniem. Sprawdzono liczebności oczekiwane (żadna poniżej 1, nie więcej niż 20% poniżej 5). Testy miały charakter eksploracyjny; nie stosowano korekty na wielokrotne porównania.

Wyniki prezentowano w tabelach zbiorczych dla każdej hipotezy, natomiast na odrębnych wykresach przedstawiono zależności istotne statystycznie. W pytaniach wielokrotnego wyboru każdą odpowiedź analizowano osobno. W przypadku zmiennych wielokategorialnych nie wykonywano porównań post hoc.

ROZDZIAŁ 3. WYNIKI BADAŃ WŁASNYCH

3.1. Charakterystyka badanej próby

W badaniu demonstracyjnym uwzględniono 100 pracowników administracji, spośród których ponad połowę (54%) stanowiły osoby pracujące hybrydowo. Rozkład poszczególnych grup wiekowych był równomierny – każda z nich stanowiła 25% badanych. Wśród respondentów dominowały osoby z wykształceniem do I stopnia (55%) oraz osoby zajmujące się obsługą klienta (57%). Badani najczęściej pracowali w urzędach gmin lub miast (25%), starostwach (24%) oraz urzędach wojewódzkich (22%). Pod względem stażu pracy największą grupę stanowiły osoby pracujące nie dłużej niż 3 lata (32%) (tab. 1).

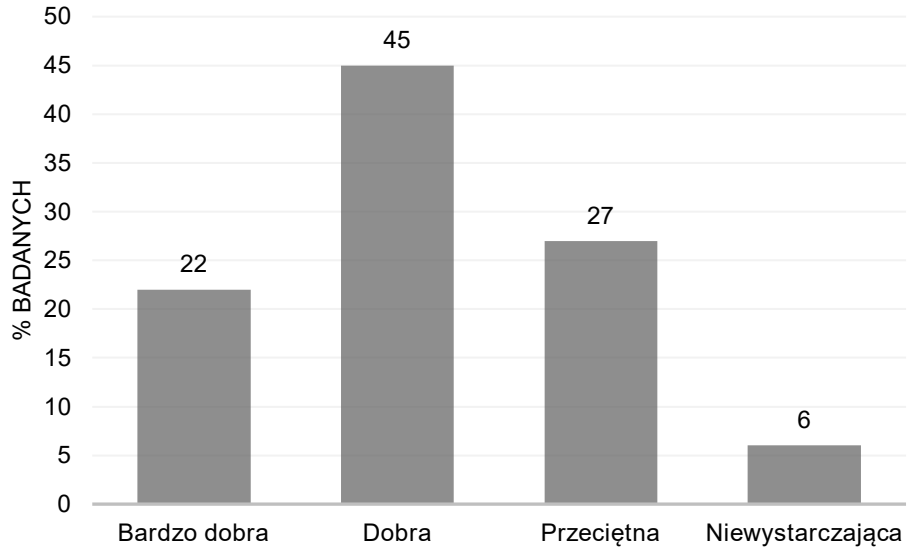
Tabela 1. Charakterystyka badanej grupy

Wyróżnik	Kategoria	n=%
Tryb pracy	Stacjonarny	46
	Hybrydowy	54
Wiek	do 29 lat	25
	30–39 lat	25
	40–49 lat	25
	50 lat i więcej	25
Wykształcenie	Do I stopnia, a w tym:	55
	Średnie	16
	Wyższe I stopnia	39
	II stopnia i wyższe, a w tym:	45
	Wyższe II stopnia	41
	Stopień naukowy	4
Stanowisko	Obsługa klienta	57
	Pozostałe, a w tym:	43
	Kadry i płace	18
	Księgowość	16
	Archiwizacja dokumentów	6
	Wsparcie IT	3
Miejsce pracy	Urząd gminy lub miasta	25
	Starostwo	24
	Urząd wojewódzki	22
	Jednostka oświatowa	10
	Instytucja kultury	11
	Inne jednostki	8
Staż pracy	do 3 lat	32
	4–8 lat	25
	9–15 lat	27
	powyżej 15 lat	16

Objaśnienia: n – liczebność, % – odsetek (procent)

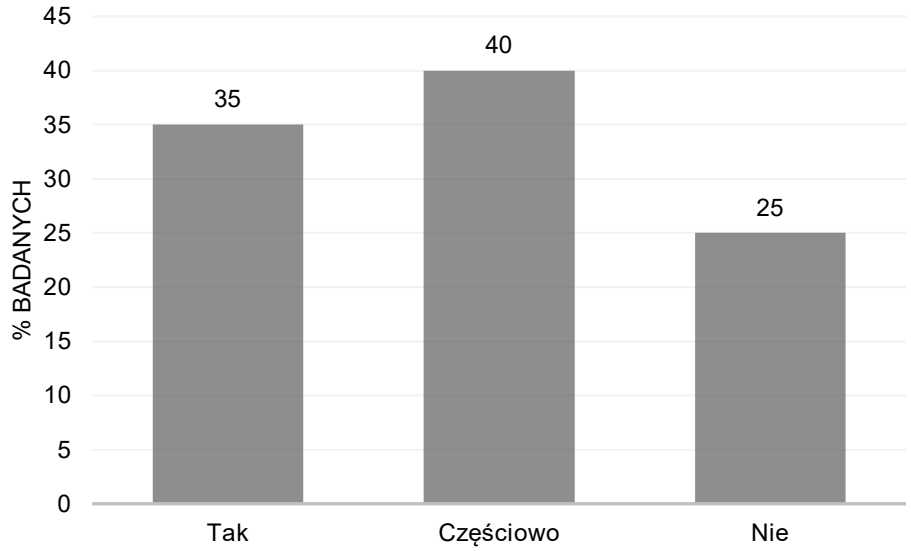
3.2. Wyniki ankiety

W pierwszej części analizy zajęto się oceną znajomości zasad bezpieczeństwa cyfrowego wśród pracowników administracji. Badanych poproszono o samoocenę wiedzy w tym zakresie. Najwięcej z nich oceniło ją jako dobrą (45%), a w dalszej kolejności jako przeciętną (27%). Bardzo dobrą znajomość tematu zadeklarowało 22% badanych, natomiast za niewystarczającą uznało ją 6% z nich (wykres 1).



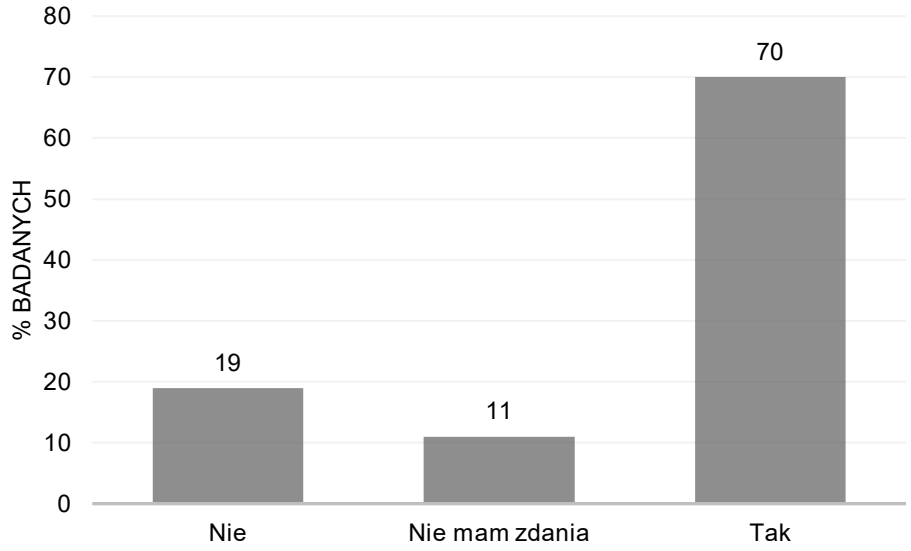
Wykres 1. Rozkład odpowiedzi na pytanie: *Jak oceniasz swoją znajomość zasad bezpieczeństwa cyfrowego?*

Kolejne pytanie dotyczyło dostępu do informacji i szkoleń z bezpieczeństwa cyfrowego w miejscu pracy. Wystarczający dostęp zadeklarowało 35% respondentów, a częściowy – 40%. Pozostali badani (25%) nie mieli dostępu do takich materiałów w wystarczającym zakresie (wykres 2).



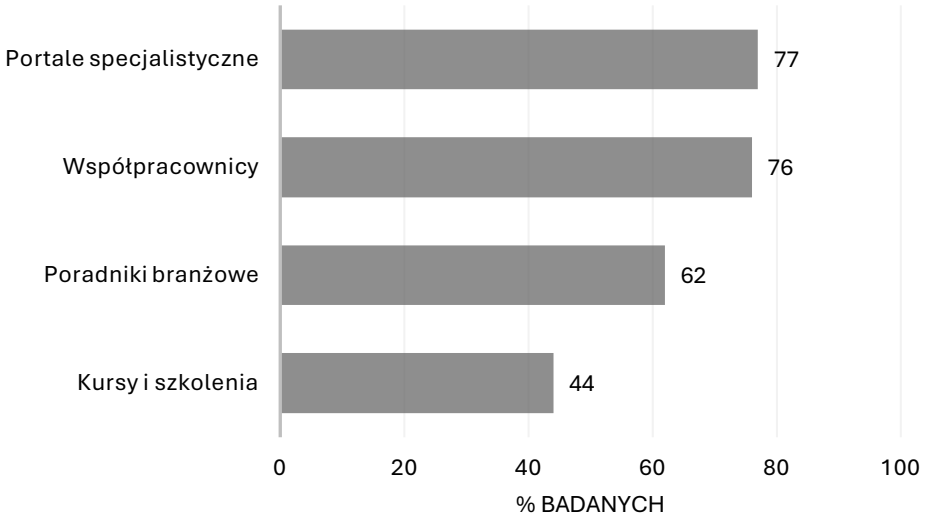
Wykres 2. Rozkład odpowiedzi na pytanie: *Czy masz w pracy dostęp do informacji i szkoleń z bezpieczeństwa cyfrowego?*

Badani w większości (70%) widzieli potrzebę dalszych szkoleń w zakresie ochrony danych. Odmiennego zdania było 19% respondentów, a brak zdania wyraziło 11% z nich (wykres 3).



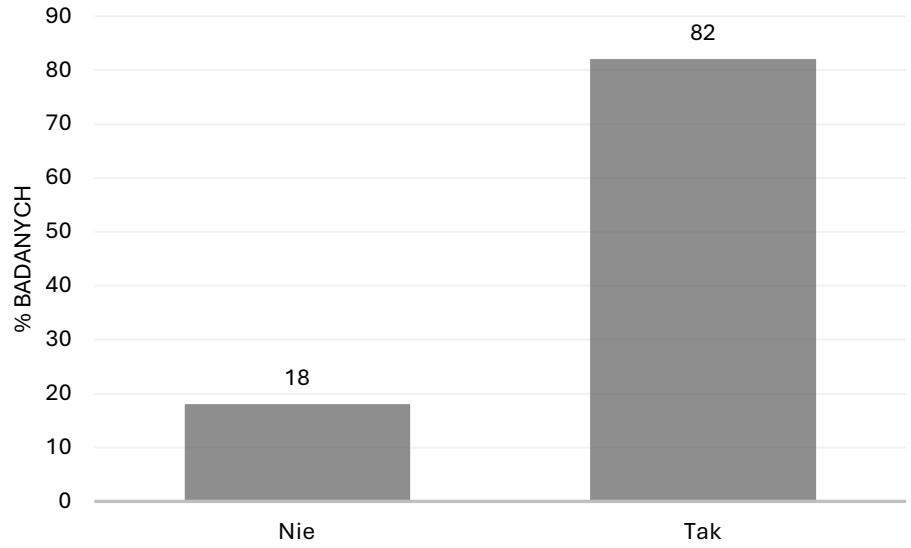
Wykres 3. Rozkład odpowiedzi na pytanie: *Czy widzisz potrzebę dalszych szkoleń w zakresie ochrony danych?*

Pod względem źródeł wiedzy o bezpieczeństwie cyfrowym najczęściej wskazywano na portale specjalistyczne (77%) oraz współpracowników (76%). Rzadziej badani korzystali z poradników branżowych (62%) oraz kursów i szkoleń (44%) (wykres 4).



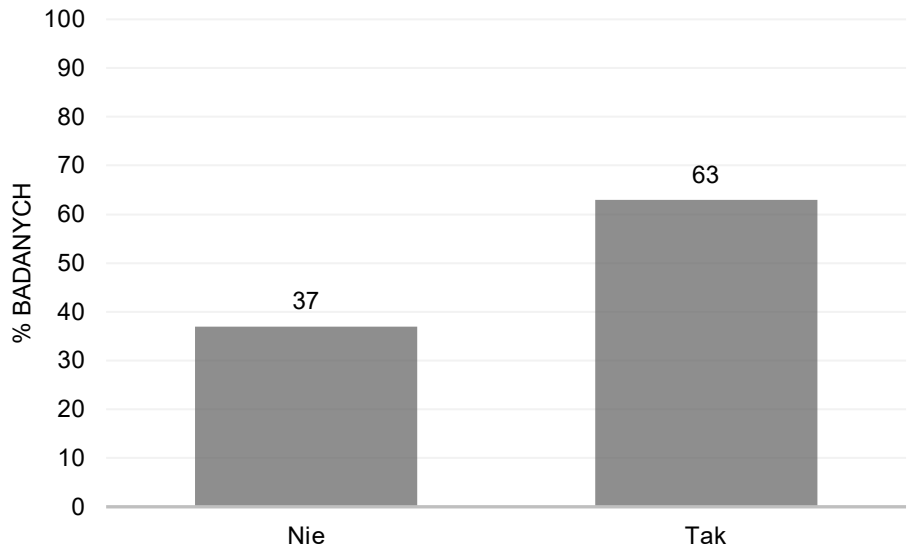
Wykres 4. Rozkład odpowiedzi na pytanie: *Skąd najczęściej czerpiesz informacje o bezpieczeństwie cyfrowym?* (wielokrotny wybór)

Zdecydowana większość badanych (82%) wyraziła chęć otrzymania dodatkowych materiałów edukacyjnych dotyczących ochrony danych. Takiej potrzeby nie deklarowało 18% uczestników badania (wykres 5).



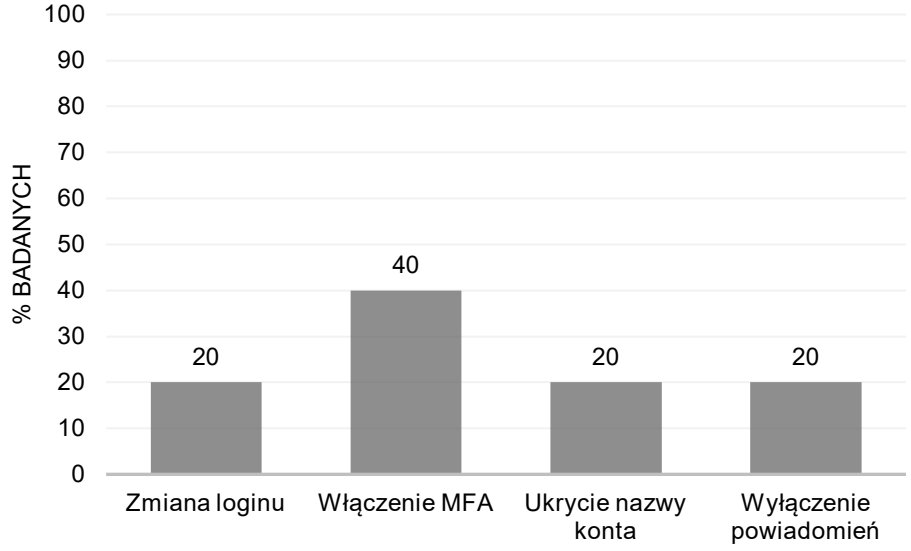
Wykres 5. Rozkład odpowiedzi na pytanie: *Czy chciałbyś/chciałabyś otrzymać więcej materiałów edukacyjnych o ochronie danych?*

W kolejnej części ankiety oceniono znajomość zagrożeń cyfrowych oraz zasad ochrony danych, uwzględniając zarówno odpowiedzi na pytania merytoryczne, jak i samoocenę wiedzy. Znajomość pojęcia uwierzytelniania wieloskładnikowego zadeklarowało 63% badanych. Pozostali (37%) przyznali, że nie znają tego pojęcia (wykres 6).



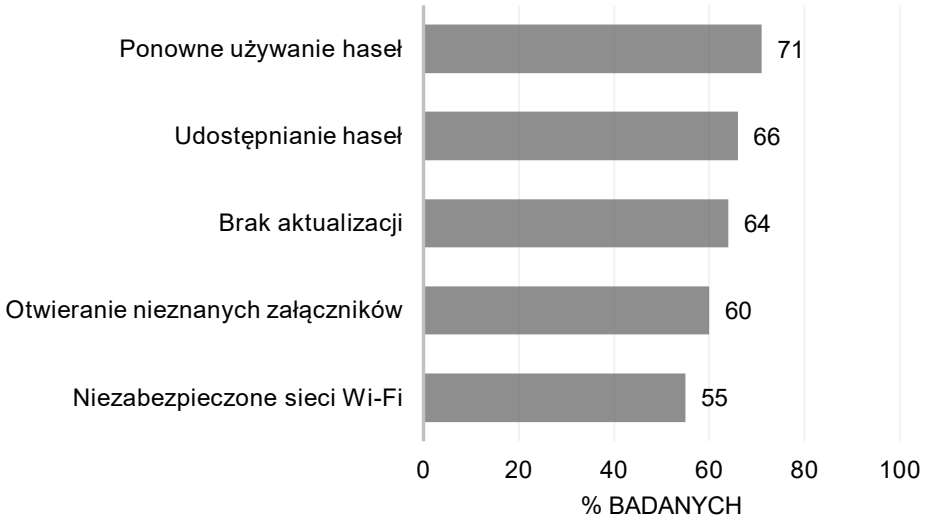
Wykres 6. Rozkład odpowiedzi na pytanie: *Czy wiesz, czym jest uwierzytelnianie wieloskładnikowe?*

W pytaniu dotyczącym ograniczania ryzyka przejęcia konta 40% badanych wskazało prawidłową odpowiedź – włączenie uwierzytelniania wieloskładnikowego (MFA). Na każdą z pozostałych, błędnych odpowiedzi (zmianę loginu, ukrycie nazwy konta oraz wyłączenie powiadomień) wskazało po 20% respondentów (wykres 7).



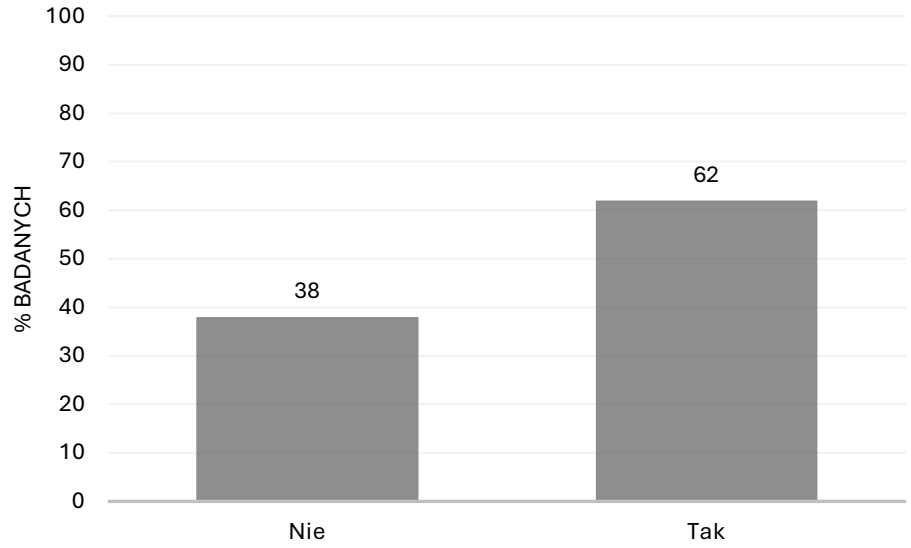
Wykres 7. Rozkład odpowiedzi na pytanie: *Które działanie najskuteczniej ogranicza ryzyko przejęcia konta?*

Wśród zachowań zwiększających ryzyko incydentów cyfrowych najczęściej wskazywano na ponowne używanie haseł (71%) oraz udostępnianie haseł (66%). W dalszej kolejności wymieniano brak aktualizacji (64%) oraz otwieranie nieznanych załączników (60%), natomiast najrzadziej wskazywano na niezabezpieczone sieci Wi-Fi (55%) (wykres 8).



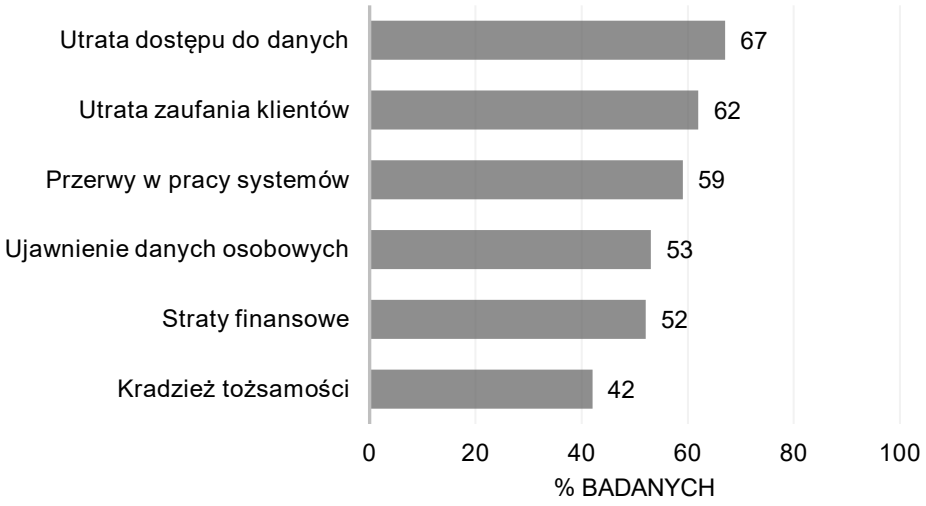
Wykres 8. Rozkład odpowiedzi na pytanie: *Jakie zachowania zwiększają ryzyko incydentów cyfrowych?* (wielokrotny wybór)

Badanych zapytano również o znajomość możliwych skutków naruszenia bezpieczeństwa danych. Odpowiedzi twierdzącej udzieliło 62% respondentów, natomiast 38% przyznało, że nie posiada takiej wiedzy (wykres 9).



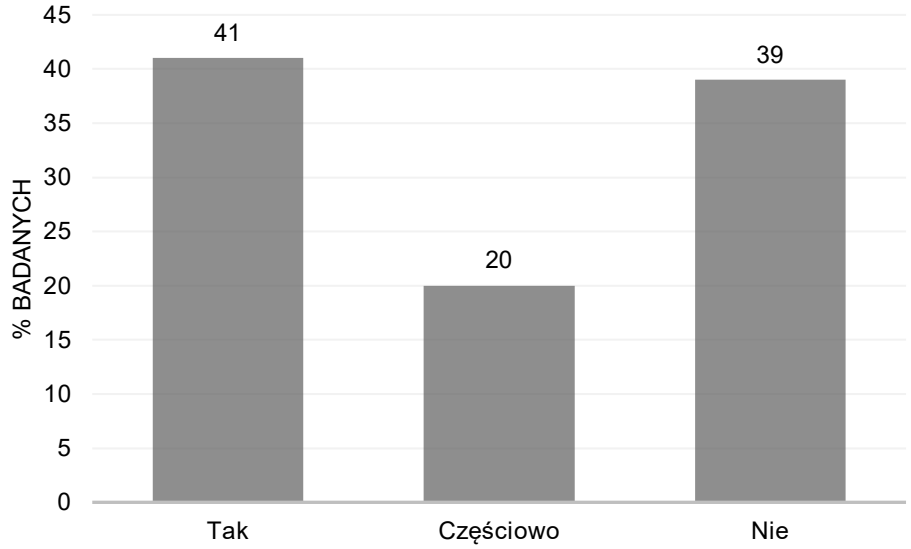
Wykres 9. Rozkład odpowiedzi na pytanie: *Czy wiesz, jakie mogą być skutki naruszenia bezpieczeństwa danych?*

Wśród możliwych konsekwencji naruszenia bezpieczeństwa danych najczęściej wskazywano na utratę dostępu do danych (67%) oraz utratę zaufania klientów (62%). W dalszej kolejności wymieniano przerwy w pracy systemów (59%), ujawnienie danych osobowych (53%) oraz straty finansowe (52%), natomiast najrzadziej wskazywano na kradzież tożsamości (42%) (wykres 10).



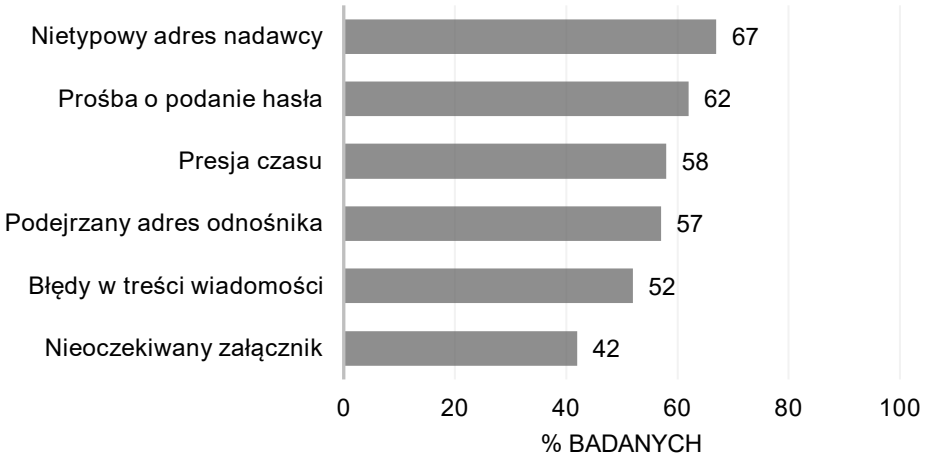
Wykres 10. Rozkład odpowiedzi na pytanie: *Jakie mogą być konsekwencje naruszenia bezpieczeństwa danych?* (wielokrotny wybór)

Umiejętność rozpoznania próby wyłudzenia danych zadeklarowało 41% badanych. Częściową znajomość tego zagadnienia wskazało 20% z nich, a brak znajomości – 39% (wykres 11).



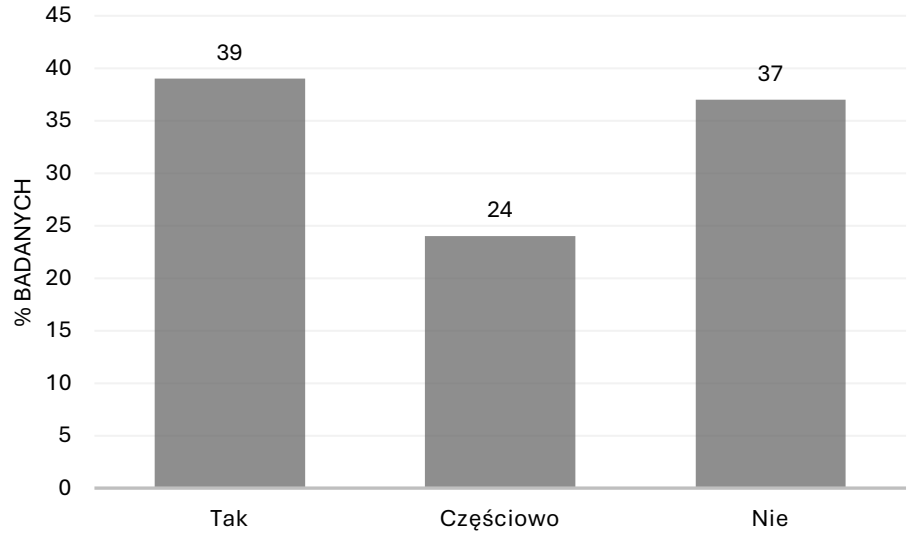
Wykres 11. Rozkład odpowiedzi na pytanie: *Czy potrafisz rozpoznać próbę wyłudzenia danych?*

Pod względem sygnałów mogących świadczyć o próbie wyłudzenia danych najczęściej wskazywano na nietypowy adres nadawcy (67%) oraz prośbę o podanie hasła (62%). W dalszej kolejności wymieniano presję czasu (58%), podejrzany adres odnośnika (57%) oraz błędy w treści wiadomości (52%), natomiast najrzadziej wskazywano na nieoczekiwany załącznik (42%) (wykres 12).



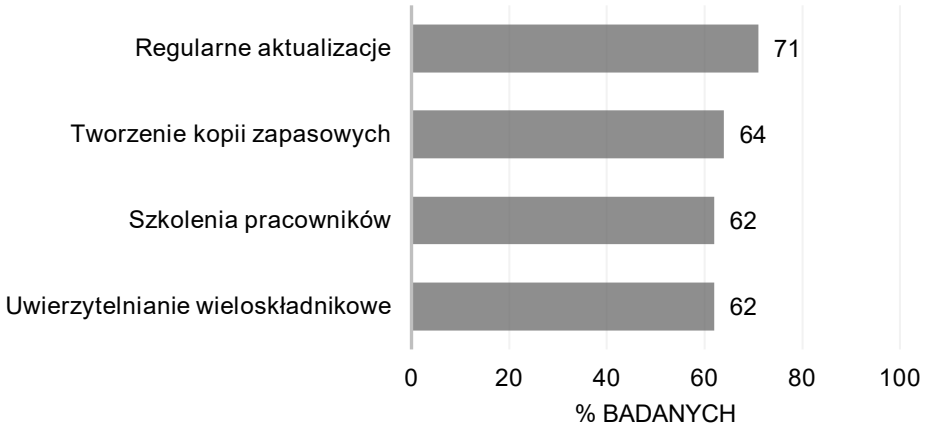
Wykres 12. Rozkład odpowiedzi na pytanie: *Jakie sygnały mogą świadczyć o próbie wyłudzenia danych?* (wielokrotny wybór)

Znajomość zasad zgłaszania incydentów w miejscu pracy zadeklarowało 39% badanych. Częściową znajomość tego zagadnienia wskazało 24% z nich, a brak znajomości – 37% (wykres 13).



Wykres 13. Rozkład odpowiedzi na pytanie: *Czy znasz zasady zgłaszania incydentów w miejscu pracy?*

Wśród działań ograniczających ryzyko incydentów cyfrowych najczęściej wskazywano na regularne aktualizacje (71%) oraz tworzenie kopii zapasowych (64%). Rzadziej wymieniano uwierzytelnianie wieloskładnikowe (62%) oraz szkolenia pracowników (62%) (wykres 14).

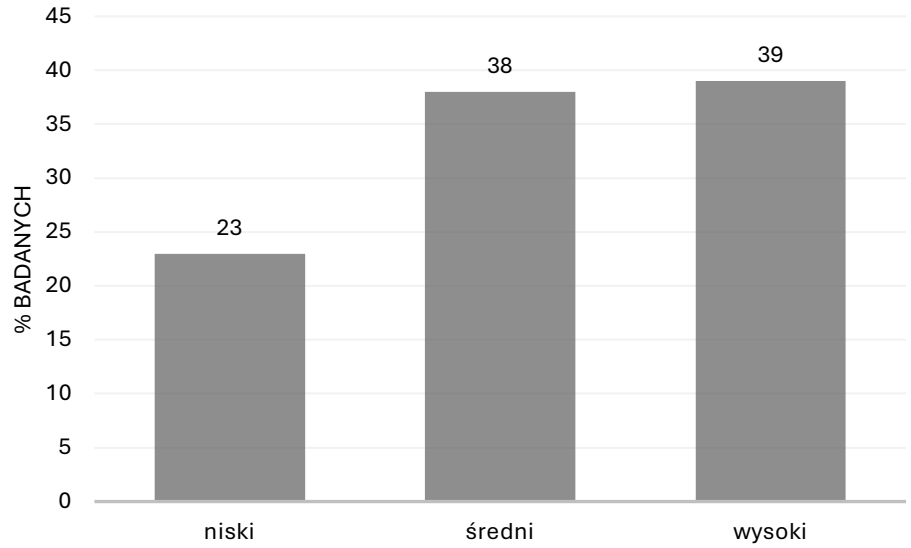


Wykres 14. Rozkład odpowiedzi na pytanie: *Jakie działania pomagają ograniczyć ryzyko incydentów cyfrowych?* (wielokrotny wybór)

Na podstawie pytań 7–15 opracowano wskaźnik znajomości zasad bezpieczeństwa cyfrowego, łączący rozpoznawanie prawidłowych odpowiedzi i samoocenę wiedzy. Za każdą prawidłową odpowiedź w pytaniu testowym, każde wskazanie prawidłowej opcji w pytaniach wielokrotnego wyboru oraz odpowiedź „tak" w pytaniach o znajomość zagadnienia przyznawano 1 punkt. Za odpowiedź „częściowo" przyznawano 0,5 punktu. Możliwe było uzyskanie od 0 do 26 punktów. Przyjęto następujące umowne przedziały:

- od 0 do 8 punktów – niski poziom znajomości zasad,
- powyżej 8 do 17 punktów – średni poziom znajomości zasad,
- powyżej 17 do 26 punktów – wysoki poziom znajomości zasad.

Największa część respondentów charakteryzowała się wysokim poziomem znajomości zasad bezpieczeństwa cyfrowego (39%). Średni poziom dotyczył 38% badanych, a niski – 23% z nich (wykres 15).



Wykres 15. Ogólny poziom znajomości zasad bezpieczeństwa cyfrowego

3.3. Statystyczna weryfikacja hipotez

3.3.1. Wyniki badań i ich omówienie – weryfikacja pierwszej hipotezy badawczej

Oceniając zależności między trybem pracy a znajomością poszczególnych aspektów bezpieczeństwa cyfrowego, istotne ($p < 0,05$) zależności wykazano w 11 przypadkach, w tym dla ogólnego poziomu znajomości zasad (tab. 2). Wyniki istotne statystycznie zaprezentowano na wykresach 16–21.

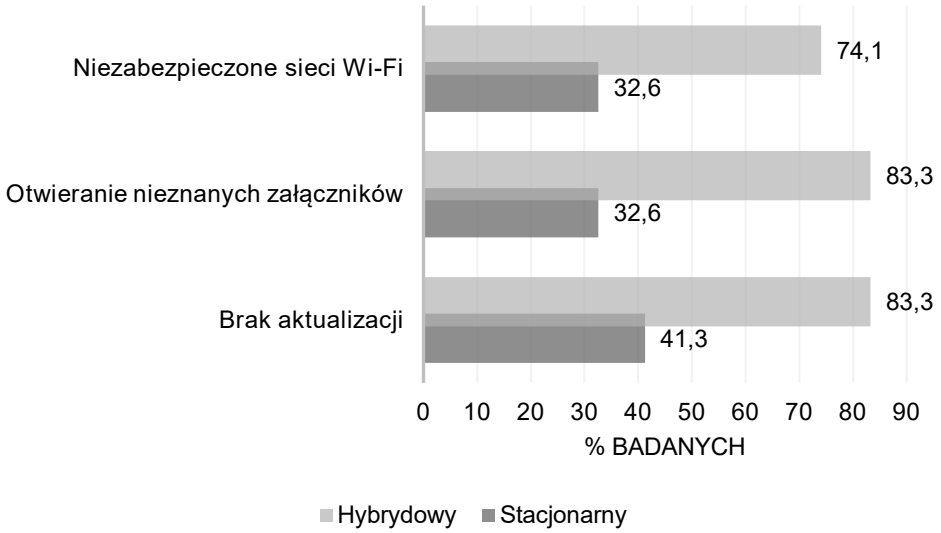
Tabela 2. Wartości testu niezależności χ^2 między trybem pracy a znajomością zasad bezpieczeństwa cyfrowego

Pytanie	Chi^2	p
7. Czy wiesz, czym jest uwierzytelnianie wieloskładnikowe?	<0,01	0,993
8. Które działanie najskuteczniej ogranicza ryzyko przejęcia konta?	2,88	0,411
9. Jakie zachowania zwiększają ryzyko incydentów cyfrowych?		
Brak aktualizacji	**19,04**	**<0,001**
Ponowne używanie haseł	0,09	0,770
Otwieranie nieznanych załączników	**26,63**	**<0,001**
Udostępnianie haseł	0,33	0,565
Niezabezpieczone sieci Wi-Fi	**17,26**	**<0,001**
10. Czy wiesz, jakie mogą być skutki naruszenia bezpieczeństwa danych?	**9,66**	**0,002**
11. Jakie mogą być konsekwencje naruszenia bezpieczeństwa danych?		
Utrata dostępu do danych	**14,16**	**<0,001**
Ujawnienie danych osobowych	0,42	0,515
Przerwy w pracy systemów	**16,18**	**<0,001**
Straty finansowe	**12,83**	**<0,001**
Utrata zaufania klientów	1,09	0,298
Kradzież tożsamości	0,08	0,782

Pytanie	Chi^2	p
12. Czy potrafisz rozpoznać próbę wyłudzenia danych?	1,22	0,544
13. Jakie sygnały mogą świadczyć o próbie wyłudzenia danych?		
Nietypowy adres nadawcy	0,60	0,437
Prośba o podanie hasła	**22,68**	**<0,001**
Presja czasu	0,08	0,782
Błędy w treści wiadomości	0,59	0,441
Podejrzany adres odnośnika	2,93	0,087
Nieoczekiwany załącznik	0,08	0,782
14. Czy znasz zasady zgłaszania incydentów w miejscu pracy?	2,09	0,351
15. Jakie działania pomagają ograniczyć ryzyko incydentów cyfrowych?		
Regularne aktualizacje	0,54	0,463
Uwierzytelnianie wieloskładnikowe	**9,66**	**0,002**
Tworzenie kopii zapasowych	0,03	0,854
Szkolenia pracowników	**12,40**	**<0,001**
Ogólny poziom znajomości zasad bezpieczeństwa cyfrowego	**9,47**	**0,009**

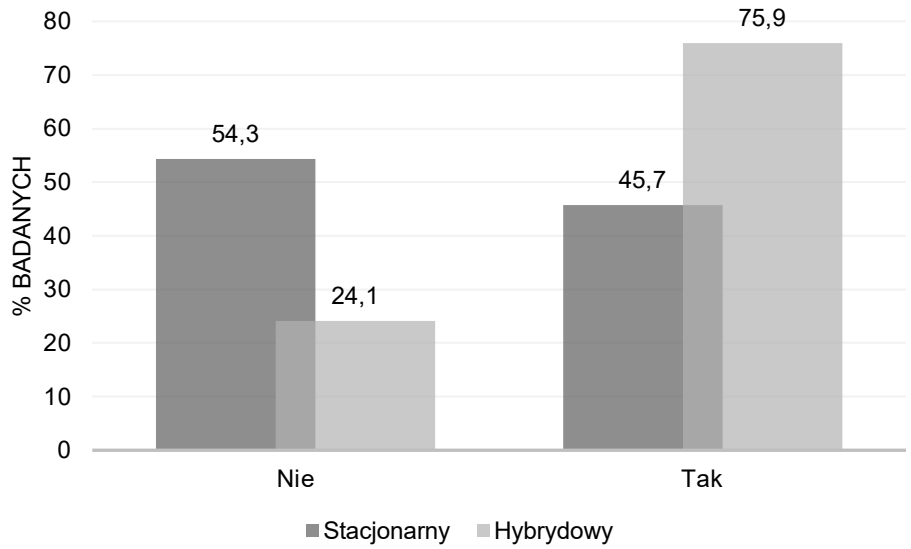
Objaśnienia: Chi^2 – wartość testu niezależności Chi^2, p – istotność

Wykazano, że osoby pracujące hybrydowo istotnie częściej niż osoby pracujące stacjonarnie wskazywały brak aktualizacji (83,3% wobec 41,3%), otwieranie nieznanych załączników (83,3% wobec 32,6%) oraz niezabezpieczone sieci Wi-Fi (74,1% wobec 32,6%) jako zachowania zwiększające ryzyko incydentów cyfrowych (wykres 16).



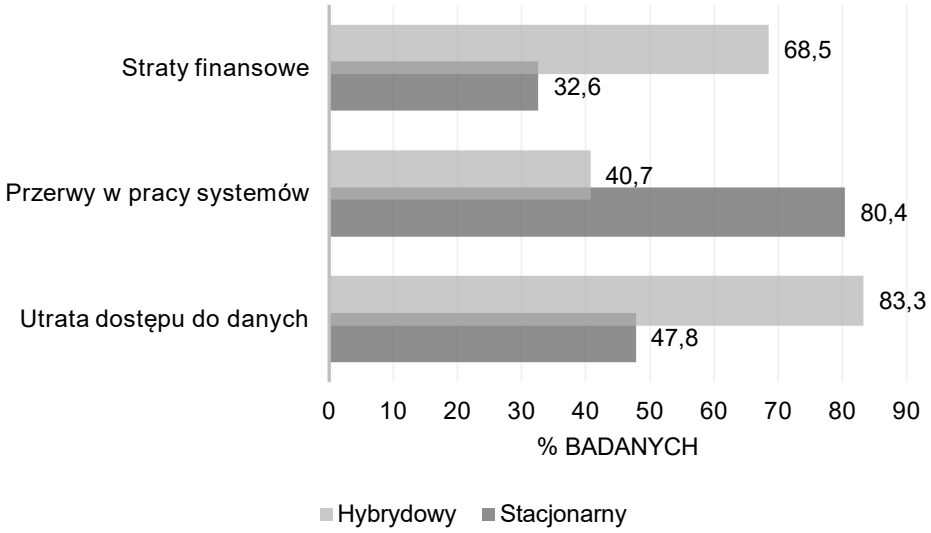
Wykres 16. Rozkład odpowiedzi na pytanie: *Jakie zachowania zwiększają ryzyko incydentów cyfrowych?* (wielokrotny wybór) w zależności od trybu pracy, dla odpowiedzi z istotnością statystyczną

Wykazano także, że osoby pracujące hybrydowo częściej niż osoby pracujące stacjonarnie deklarowały znajomość możliwych skutków naruszenia bezpieczeństwa danych (75,9% wobec 45,7%) (wykres 17).



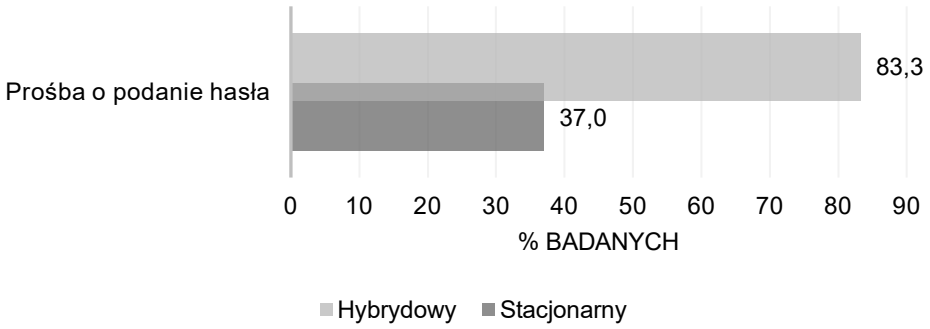
Wykres 17. Rozkład odpowiedzi na pytanie: *Czy wiesz, jakie mogą być skutki naruszenia bezpieczeństwa danych?* w zależności od trybu pracy

Wykazano, że osoby pracujące stacjonarnie istotnie częściej niż osoby pracujące hybrydowo wskazywały przerwy w pracy systemów (80,4% wobec 40,7%) jako możliwe skutki naruszenia bezpieczeństwa danych. Natomiast osoby pracujące hybrydowo istotnie częściej niż osoby pracujące stacjonarnie wskazywały utratę dostępu do danych (83,3% wobec 47,8%) oraz straty finansowe (68,5% wobec 32,6%) jako możliwe skutki naruszenia bezpieczeństwa danych (wykres 18).



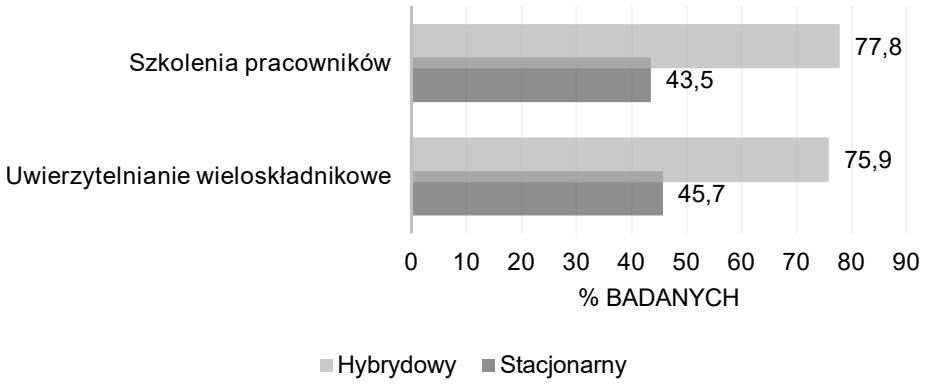
Wykres 18. Rozkład odpowiedzi na pytanie: *Jakie mogą być konsekwencje naruszenia bezpieczeństwa danych?* (wielokrotny wybór) w zależności od trybu pracy, dla odpowiedzi z istotnością statystyczną

Wykazano, że osoby pracujące hybrydowo istotnie częściej niż osoby pracujące stacjonarnie wskazywały prośbę o podanie hasła (83,3% wobec 37,0%) jako sygnał mogący świadczyć o próbie wyłudzenia danych (wykres 19).



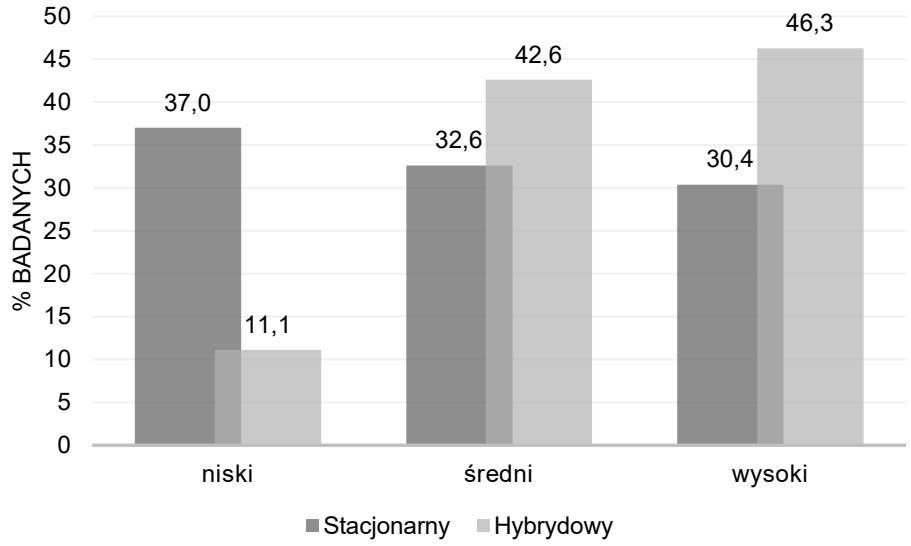
Wykres 19. Rozkład odpowiedzi na pytanie: *Jakie sygnały mogą świadczyć o próbie wyłudzenia danych?* (wielokrotny wybór) w zależności od trybu pracy, dla odpowiedzi z istotnością statystyczną

Wykazano, że osoby pracujące hybrydowo istotnie częściej niż osoby pracujące stacjonarnie wskazywały uwierzytelnianie wieloskładnikowe (75,9% wobec 45,7%) oraz szkolenia pracowników (77,8% wobec 43,5%) jako działania ograniczające ryzyko incydentów cyfrowych (wykres 20).



Wykres 20. Rozkład odpowiedzi na pytanie: *Jakie działania pomagają ograniczyć ryzyko incydentów cyfrowych?* (wielokrotny wybór) w zależności od trybu pracy, dla odpowiedzi z istotnością statystyczną

Wykazano istotne ($p < 0,05$) różnice pomiędzy osobami pracującymi stacjonarnie i hybrydowo pod względem ogólnego poziomu znajomości zasad bezpieczeństwa cyfrowego. Osoby pracujące hybrydowo częściej prezentowały wysoki (46,3% wobec 30,4%) lub średni poziom znajomości zasad (42,6% wobec 32,6%), natomiast osoby pracujące stacjonarnie – niski (37,0% wobec 11,1%) (wykres 21).



Wykres 21. Ogólny poziom znajomości zasad bezpieczeństwa cyfrowego w zależności od trybu pracy

Na podstawie przeprowadzonych analiz uzyskano podstawy do potwierdzenia hipotezy pierwszej, zgodnie z którą osoby pracujące hybrydowo charakteryzują się wyższym ogólnym poziomem znajomości zasad bezpieczeństwa cyfrowego niż osoby pracujące stacjonarnie.

3.3.2. Wyniki badań i ich omówienie – weryfikacja drugiej hipotezy badawczej

Oceniając zależności między wiekiem a znajomością poszczególnych aspektów bezpieczeństwa cyfrowego, istotne ($p < 0,05$) zależności wykazano w 3 przypadkach, przy czym nie wykazano istotności statystycznej dla ogólnego poziomu znajomości zasad (tab. 3). Wyniki istotne statystycznie zaprezentowano na wykresach 22–24.

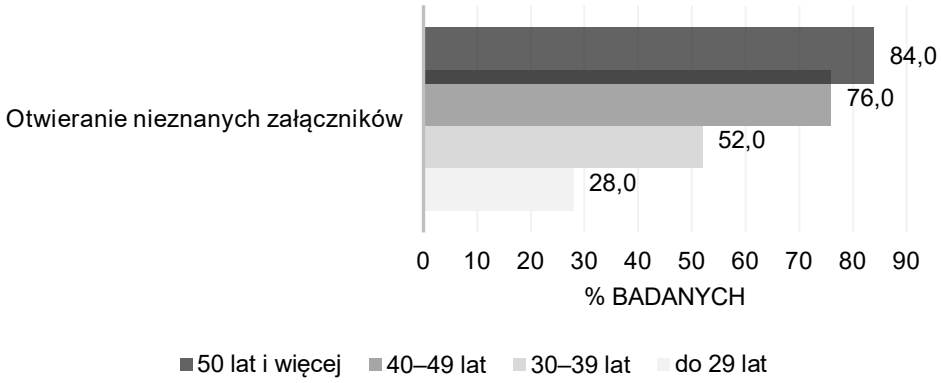
Tabela 3. Wartości testu niezależności χ^2 między wiekiem a znajomością zasad bezpieczeństwa cyfrowego

Pytanie	Chi^2	p
7. Czy wiesz, czym jest uwierzytelnianie wieloskładnikowe?	6,65	0,084
8. Które działanie najskuteczniej ogranicza ryzyko przejęcia konta?	9,80	0,367
9. Jakie zachowania zwiększają ryzyko incydentów cyfrowych?		
Brak aktualizacji	3,47	0,324
Ponowne używanie haseł	1,70	0,637
Otwieranie nieznanych załączników	**20,00**	**<0,001**
Udostępnianie haseł	6,60	0,086
Niezabezpieczone sieci Wi-Fi	5,62	0,132
10. Czy wiesz, jakie mogą być skutki naruszenia bezpieczeństwa danych?	**19,86**	**<0,001**
11. Jakie mogą być konsekwencje naruszenia bezpieczeństwa danych?		
Utrata dostępu do danych	4,12	0,249
Ujawnienie danych osobowych	2,37	0,500
Przerwy w pracy systemów	3,76	0,288

Pytanie	Chi^2	p
Straty finansowe	2,88	0,410
Utrata zaufania klientów	2,89	0,409
Kradzież tożsamości	2,79	0,425
12. Czy potrafisz rozpoznać próbę wyłudzenia danych?	**28,05**	**<0,001**
13. Jakie sygnały mogą świadczyć o próbie wyłudzenia danych?		
Nietypowy adres nadawcy	5,56	0,135
Prośba o podanie hasła	3,57	0,312
Presja czasu	4,76	0,190
Błędy w treści wiadomości	2,24	0,523
Podejrzany adres odnośnika	4,04	0,257
Nieoczekiwany załącznik	4,11	0,250
14. Czy znasz zasady zgłaszania incydentów w miejscu pracy?	10,72	0,097
15. Jakie działania pomagają ograniczyć ryzyko incydentów cyfrowych?		
Regularne aktualizacje	4,03	0,258
Uwierzytelnianie wieloskładnikowe	6,96	0,073
Tworzenie kopii zapasowych	4,51	0,211
Szkolenia pracowników	6,96	0,073
Ogólny poziom znajomości zasad bezpieczeństwa cyfrowego	8,26	0,219

Objaśnienia: Chi^2 – wartość testu niezależności Chi^2, p – istotność

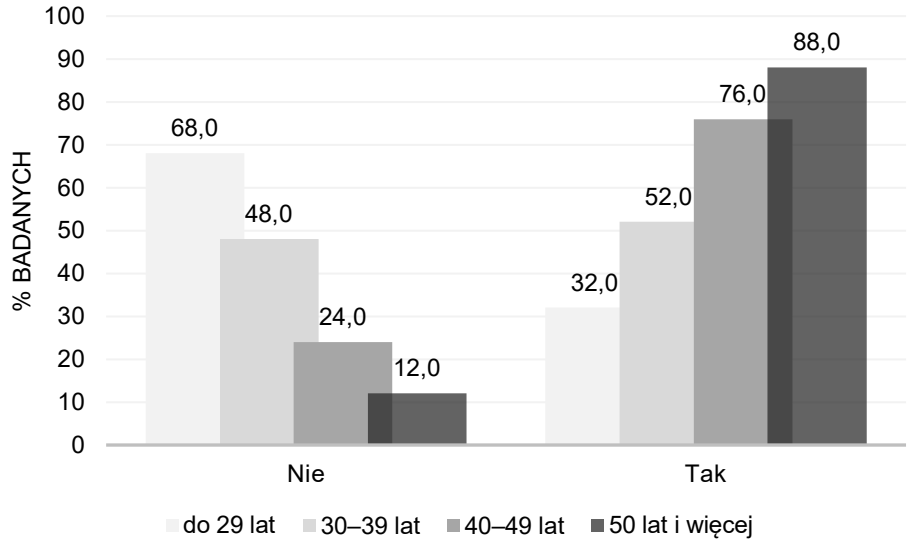
Wykazano istotną ($p < 0,05$) zależność między wiekiem a wskazaniem na otwieranie nieznanych załączników jako czynnik ryzyka. Najczęściej wskazywały na otwieranie nieznanych załączników osoby z grupy 50 lat i więcej (84,0%), najrzadziej natomiast osoby z grupy do 29 lat (28,0%). W pozostałych grupach odsetki wynosiły 52,0% (grupa 30–39 lat) oraz 76,0% (grupa 40–49 lat) (wykres 22).



Wykres 22. Rozkład odpowiedzi na pytanie: *Jakie zachowania zwiększają ryzyko incydentów cyfrowych?* (wielokrotny wybór) w zależności od wieku, dla odpowiedzi z istotnością statystyczną

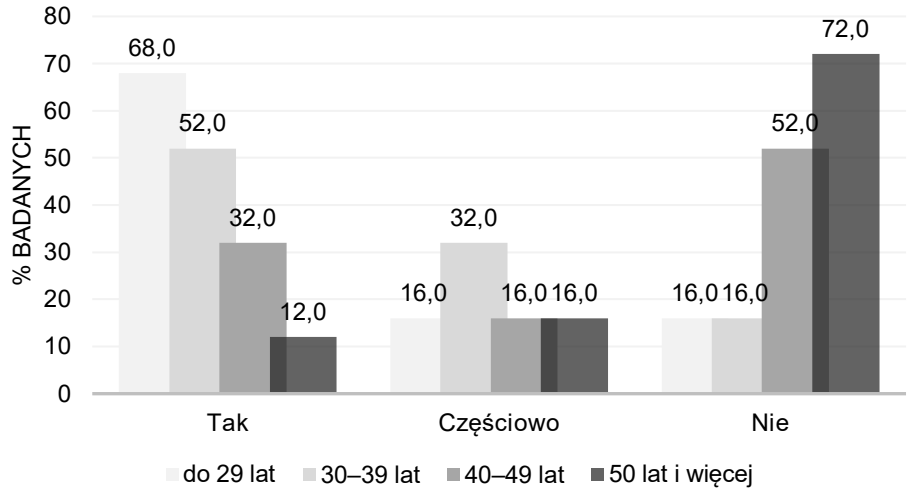
Wykazano istotną ($p < 0,05$) zależność między wiekiem a deklarowaną znajomością skutków naruszenia bezpieczeństwa danych. Najczęściej deklarowały znajomość skutków naruszenia bezpieczeństwa danych osoby z grupy 50 lat i więcej (88,0%), najrzadziej natomiast

osoby z grupy do 29 lat (32,0%). W pozostałych grupach odsetki wynosiły 52,0% (grupa 30–39 lat) oraz 76,0% (grupa 40–49 lat) (wykres 23).



Wykres 23. Rozkład odpowiedzi na pytanie: *Czy wiesz, jakie mogą być skutki naruszenia bezpieczeństwa danych?* w zależności od wieku

Wykazano istotną ($p < 0,05$) zależność między wiekiem a deklarowaną umiejętnością rozpoznawania prób wyłudzenia danych. Najczęściej deklarowały umiejętność rozpoznania próby wyłudzenia danych osoby z grupy do 29 lat (68,0%), najrzadziej natomiast osoby z grupy 50 lat i więcej (12,0%). W pozostałych grupach odsetki wynosiły 52,0% (grupa 30–39 lat) oraz 32,0% (grupa 40–49 lat) (wykres 24).



Wykres 24. Rozkład odpowiedzi na pytanie: *Czy potrafisz rozpoznać próbę wyłudzenia danych?* w zależności od wieku

Przeprowadzone analizy nie pozwoliły potwierdzić hipotezy drugiej mówiącej o tym, że ogólny poziom znajomości zasad bezpieczeństwa cyfrowego różni się w zależności od wieku. Wykazano natomiast zależności dla wybranych aspektów wiedzy i jej samooceny.

3.3.3. Wyniki badań i ich omówienie – weryfikacja trzeciej hipotezy badawczej

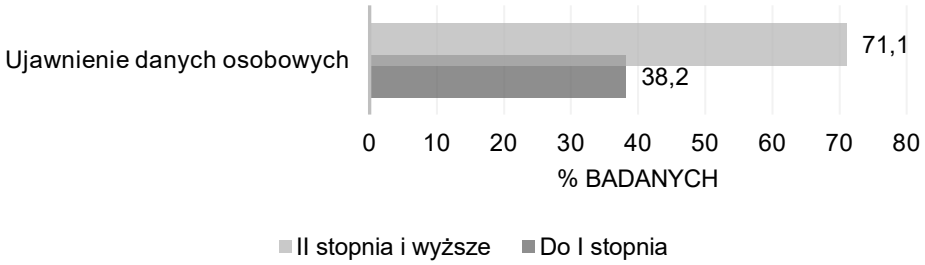
Oceniając zależności między wykształceniem a znajomością poszczególnych aspektów bezpieczeństwa cyfrowego, istotne ($p < 0,05$) zależności wykazano w 2 przypadkach, przy czym nie wykazano istotności statystycznej dla ogólnego poziomu znajomości zasad (tab. 4). Wyniki istotne statystycznie zaprezentowano na wykresach 25–26.

Tabela 4. Wartości testu niezależności χ^2 między wykształceniem a znajomością zasad bezpieczeństwa cyfrowego

Pytanie	Chi^2	p
7. Czy wiesz, czym jest uwierzytelnianie wieloskładnikowe?	0,47	0,492
8. Które działanie najskuteczniej ogranicza ryzyko przejęcia konta?	5,15	0,161
9. Jakie zachowania zwiększają ryzyko incydentów cyfrowych?		
Brak aktualizacji	0,11	0,738
Ponowne używanie haseł	0,82	0,364
Otwieranie nieznanych załączników	2,69	0,101
Udostępnianie haseł	1,96	0,161
Niezabezpieczone sieci Wi-Fi	1,23	0,267
10. Czy wiesz, jakie mogą być skutki naruszenia bezpieczeństwa danych?	<0,01	0,967
11. Jakie mogą być konsekwencje naruszenia bezpieczeństwa danych?		
Utrata dostępu do danych	0,13	0,716
Ujawnienie danych osobowych	**10,77**	**0,001**
Przerwy w pracy systemów	0,03	0,854
Straty finansowe	1,09	0,296
Utrata zaufania klientów	<0,01	0,967
Kradzież tożsamości	<0,01	0,968
12. Czy potrafisz rozpoznać próbę wyłudzenia danych?	1,06	0,590
13. Jakie sygnały mogą świadczyć o próbie wyłudzenia danych?		
Nietypowy adres nadawcy	<0,01	0,949
Prośba o podanie hasła	0,14	0,709
Presja czasu	<0,01	0,968
Błędy w treści wiadomości	1,09	0,296
Podejrzany adres odnośnika	1,85	0,174
Nieoczekiwany załącznik	<0,01	0,968
14. Czy znasz zasady zgłaszania incydentów w miejscu pracy?	1,74	0,420
15. Jakie działania pomagają ograniczyć ryzyko incydentów cyfrowych?		
Regularne aktualizacje	1,83	0,177
Uwierzytelnianie wieloskładnikowe	0,76	0,384
Tworzenie kopii zapasowych	**16,84**	**<0,001**
Szkolenia pracowników	0,14	0,709
Ogólny poziom znajomości zasad bezpieczeństwa cyfrowego	1,72	0,424

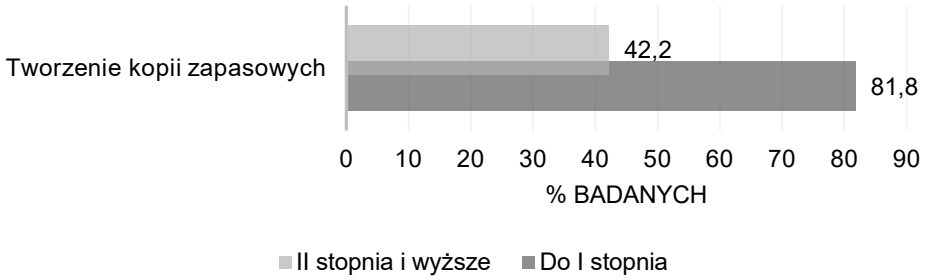
Objaśnienia: Chi^2 – wartość testu niezależności Chi^2, p – istotność

Wykazano, że osoby z wykształceniem II stopnia lub wyższym istotnie częściej niż osoby z wykształceniem do I stopnia wskazywały ujawnienie danych osobowych (71,1% wobec 38,2%) jako możliwe skutki naruszenia bezpieczeństwa danych (wykres 25).



Wykres 25. Rozkład odpowiedzi na pytanie: *Jakie mogą być konsekwencje naruszenia bezpieczeństwa danych?* (wielokrotny wybór) w zależności od wykształcenia, dla odpowiedzi z istotnością statystyczną

Wykazano, że osoby z wykształceniem do I stopnia istotnie częściej niż osoby z wykształceniem II stopnia lub wyższym wskazywały tworzenie kopii zapasowych (81,8% wobec 42,2%) jako działania ograniczające ryzyko incydentów cyfrowych (wykres 26).



Wykres 26. Rozkład odpowiedzi na pytanie: *Jakie działania pomagają ograniczyć ryzyko incydentów cyfrowych?* (wielokrotny wybór) w zależności od wykształcenia, dla odpowiedzi z istotnością statystyczną

Nie uzyskano podstaw do potwierdzenia hipotezy trzeciej, zgodnie z którą osoby z wykształceniem II stopnia lub wyższym charakteryzują się wyższym ogólnym poziomem znajomości zasad bezpieczeństwa cyfrowego. Istotne zależności stwierdzono jedynie w odniesieniu do dwóch odpowiedzi szczegółowych.

3.3.4. Wyniki badań i ich omówienie – weryfikacja czwartej hipotezy badawczej

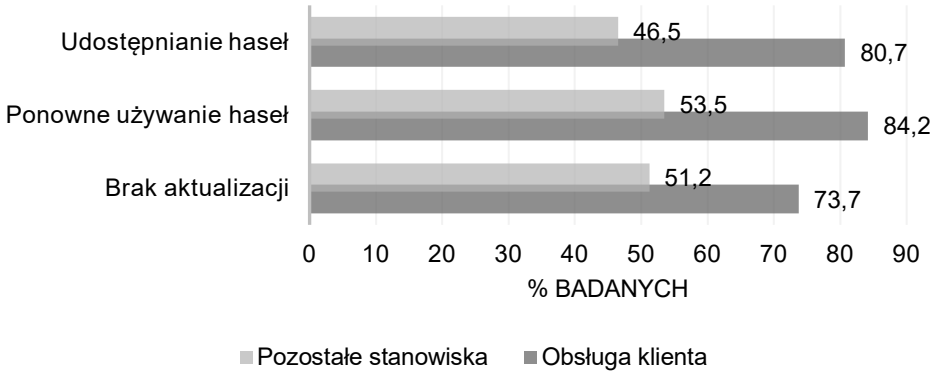
Oceniając zależności między rodzajem stanowiska a znajomością poszczególnych aspektów bezpieczeństwa cyfrowego, istotne ($p < 0,05$) zależności wykazano w 11 przypadkach, w tym dla ogólnego poziomu znajomości zasad (tab. 5). Wyniki istotne statystycznie zaprezentowano na wykresach 27–31.

Tabela 5. Wartości testu niezależności χ^2 między rodzajem stanowiska a znajomością zasad bezpieczeństwa cyfrowego

Pytanie	Chi^2	p
7. Czy wiesz, czym jest uwierzytelnianie wieloskładnikowe?	0,76	0,382
8. Które działanie najskuteczniej ogranicza ryzyko przejęcia konta?	0,65	0,884
9. Jakie zachowania zwiększają ryzyko incydentów cyfrowych?		
Brak aktualizacji	**5,40**	**0,020**
Ponowne używanie haseł	**11,24**	**<0,001**
Otwieranie nieznanych załączników	0,55	0,458
Udostępnianie haseł	**12,77**	**<0,001**
Niezabezpieczone sieci Wi-Fi	0,45	0,503
10. Czy wiesz, jakie mogą być skutki naruszenia bezpieczeństwa danych?	0,48	0,490
11. Jakie mogą być konsekwencje naruszenia bezpieczeństwa danych?		
Utrata dostępu do danych	**11,26**	**<0,001**
Ujawnienie danych osobowych	1,27	0,259
Przerwy w pracy systemów	0,95	0,330
Straty finansowe	0,30	0,582
Utrata zaufania klientów	**7,68**	**0,006**
Kradzież tożsamości	0,71	0,399
12. Czy potrafisz rozpoznać próbę wyłudzenia danych?	0,74	0,690
13. Jakie sygnały mogą świadczyć o próbie wyłudzenia danych?		
Nietypowy adres nadawcy	**30,28**	**<0,001**
Prośba o podanie hasła	0,48	0,490
Presja czasu	1,57	0,210
Błędy w treści wiadomości	0,02	0,884
Podejrzany adres odnośnika	**26,05**	**<0,001**
Nieoczekiwany załącznik	0,19	0,664
14. Czy znasz zasady zgłaszania incydentów w miejscu pracy?	4,93	0,085
15. Jakie działania pomagają ograniczyć ryzyko incydentów cyfrowych?		
Regularne aktualizacje	**18,00**	**<0,001**
Uwierzytelnianie wieloskładnikowe	**10,16**	**0,001**
Tworzenie kopii zapasowych	0,39	0,533
Szkolenia pracowników	**12,99**	**<0,001**
Ogólny poziom znajomości zasad bezpieczeństwa cyfrowego	**7,02**	**0,030**

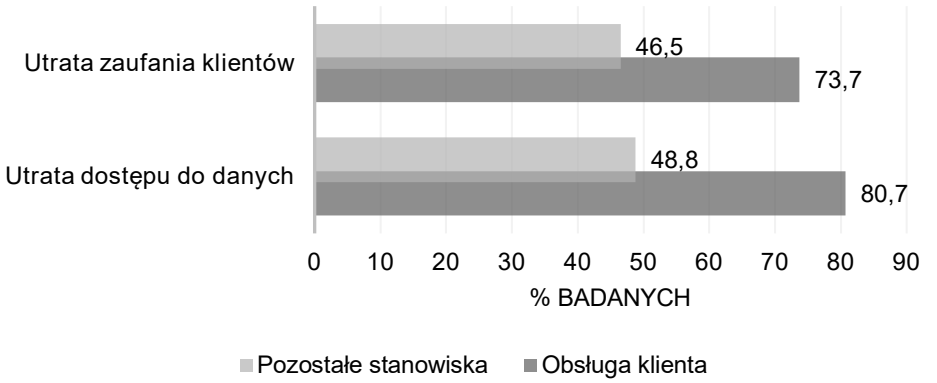
Objaśnienia: Chi^2 – wartość testu niezależności Chi^2, p – istotność

Wykazano, że pracownicy obsługi klienta istotnie częściej niż pracownicy na pozostałych stanowiskach wskazywali brak aktualizacji (73,7% wobec 51,2%), ponowne używanie haseł (84,2% wobec 53,5%) oraz udostępnianie haseł (80,7% wobec 46,5%) jako zachowania zwiększające ryzyko incydentów cyfrowych (wykres 27).



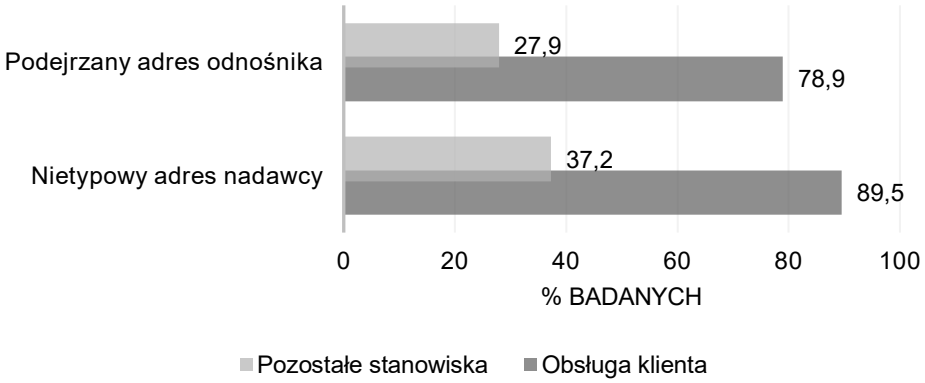
Wykres 27. Rozkład odpowiedzi na pytanie: *Jakie zachowania zwiększają ryzyko incydentów cyfrowych?* (wielokrotny wybór) w zależności od rodzaju stanowiska, dla odpowiedzi z istotnością statystyczną

Wykazano, że pracownicy obsługi klienta istotnie częściej niż pracownicy na pozostałych stanowiskach wskazywali utratę dostępu do danych (80,7% wobec 48,8%) oraz utratę zaufania klientów (73,7% wobec 46,5%) jako możliwe skutki naruszenia bezpieczeństwa danych (wykres 28).



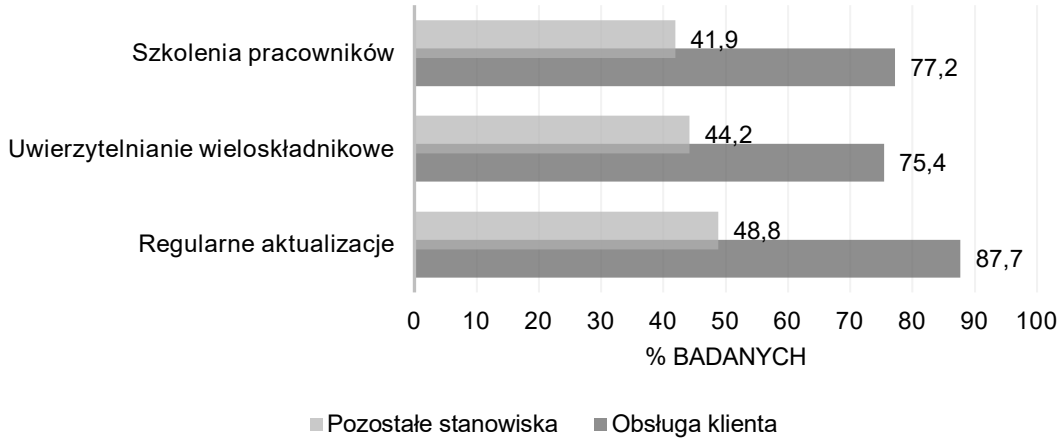
Wykres 28. Rozkład odpowiedzi na pytanie: *Jakie mogą być konsekwencje naruszenia bezpieczeństwa danych?* (wielokrotny wybór) w zależności od rodzaju stanowiska, dla odpowiedzi z istotnością statystyczną

Wykazano, że pracownicy obsługi klienta istotnie częściej niż pracownicy na pozostałych stanowiskach wskazywali nietypowy adres nadawcy (89,5% wobec 37,2%) oraz podejrzany adres odnośnika (78,9% wobec 27,9%) jako sygnały mogące świadczyć o próbie wyłudzenia danych (wykres 29).



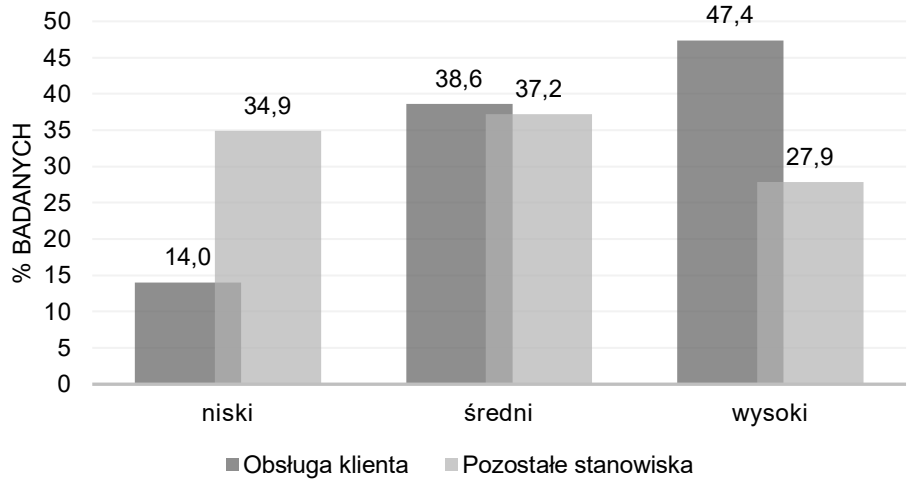
Wykres 29. Rozkład odpowiedzi na pytanie: *Jakie sygnały mogą świadczyć o próbie wyłudzenia danych?* (wielokrotny wybór) w zależności od rodzaju stanowiska, dla odpowiedzi z istotnością statystyczną

Wykazano, że pracownicy obsługi klienta istotnie częściej niż pracownicy na pozostałych stanowiskach wskazywali regularne aktualizacje (87,7% wobec 48,8%), uwierzytelnianie wieloskładnikowe (75,4% wobec 44,2%) oraz szkolenia pracowników (77,2% wobec 41,9%) jako działania ograniczające ryzyko incydentów cyfrowych (wykres 30).



Wykres 30. Rozkład odpowiedzi na pytanie: *Jakie działania pomagają ograniczyć ryzyko incydentów cyfrowych?* (wielokrotny wybór) w zależności od rodzaju stanowiska, dla odpowiedzi z istotnością statystyczną

Wykazano istotne ($p < 0,05$) różnice pod względem ogólnego poziomu znajomości zasad bezpieczeństwa cyfrowego w zależności od rodzaju stanowiska. Pracownicy obsługi klienta częściej prezentowali wysoki poziom (47,4% wobec 27,9%), natomiast osoby na pozostałych stanowiskach – niski (34,9% wobec 14,0%). Odsetek osób o średnim poziomie był w obu grupach zbliżony (38,6% i 37,2%) (wykres 31).



Wykres 31. Ogólny poziom znajomości zasad bezpieczeństwa cyfrowego w zależności od rodzaju stanowiska

Na podstawie powyższych analiz uzyskano podstawy do potwierdzenia hipotezy czwartej, zakładającej wyższy ogólny poziom znajomości zasad bezpieczeństwa cyfrowego wśród pracowników obsługi klienta niż wśród osób na pozostałych stanowiskach. Różnice dotyczyły także wybranych zagrożeń, możliwych konsekwencji incydentów oraz działań zapobiegawczych.