Zeszyty Naukowe
Zbliżenia Cywilizacyjne XV (3)/2019

ISSN: 1896-4087
DOI: http://dx.doi.org/10.21784/ZC.2019.021

MACIEJ SZMIT
ANETA KACZMAREK
Uniwersytet Łódzki

Badania świadomości bezpieczeństwa informacji w wybranych grupach społecznych: studentów, instruktorów harcerskich oraz pracowników Wojewódzkiego Sądu Administracyjnego

Research on information security awareness in selected social groups: students, scout leaders and employees of the Regional Administrative Court

Streszczenie:
Artykuł przedstawia wyniki dwóch badań ankietowych, przeprowadzonych w grupach studentów, instruktorów harcerskich oraz pracowników Wojewódzkiego Sądu Administracyjnego. Celem badań było poznanie wiedzy i poglądów respondentów na wybrane tematy związane z cyberbezpieczeństwem, stwierdzenie czy istnieją statystycznie istotne związki pomiędzy cechami statystycznymi uczestników badania, a ich wiedzą (mierzoną liczbą prawidłowych odpowiedzi na pytania dotyczące cyberbezpieczeństwa) oraz poglądami na temat cyberbezpieczeństwa. Badano także nawyki uczestników związane z bezpieczeństwem (takie, jak wykonywanie kopii bezpieczeństwa czy używanie programu antywirusowego) oraz związek między wiedzą, zachowaniami a uczestnictwem w szkoleniach.
Słowa kluczowe: świadomość bezpieczeństwa informacji, cyberbezpieczeństwo

Abstract:

The article presents results of two surveys conducted in groups of students, scout leaders and employees of the Regional Administrative Court. The aim of the research was to recognize the knowledge and views of respondents on selected topics related to cybersecurity, to determine whether there are any significant statistical correlations between the statistical features of the survey participants, and their knowledge (measured by the number of correct answers to questions about cybersecurity) and views on cybersecurity. They surveys also examined the respondents' habits related to security (such as making back-up copies or using antivirus software) and the relationship between knowledge, behaviour and participation in training courses.
Keywords: information security awareness, cybersecurity

Wprowadzenie

Świadomość bezpieczeństwa informacji (ang. *Information security awareness*) jest pojęciem odnoszącym się zarówno do wiedzy, jak i do właściwych postaw i nawyków oraz do podejmowania odpowiednich działań prowadzących do zmniejszenia ekspozycji na ryzyko związane z bezpieczeństwem informacji bądź minimalizacji skutków jego materializacji. Rozpatrywana jest ona zazwyczaj w kontekście pracowników organizacji, mających dostęp do informacji stanowiących jej własność, bądź w kontekście właściwych zachowań użytkowników komputerów osobistych, którzy powinni przestrzegać zasad „higieny informacyjnej", aby zapobiec incydentom bezpieczeństwa, bądź zmniejszyć skutki zdarzeń, takich jak przypadkowa utrata danych, ekspozycja na złośliwe oprogramowanie czy naruszenie prywatności[1]. Budowanie świadomości bezpieczeństwa informacji, w szczególności informacji przetwarzanej w cyberprzestrzeni[2] (ang. *cybersecurity awareness*) wśród osób prywatnych i pracowników różnych instytucji

[1] Por. M. Szmit, *Świadomość bezpieczeństwa informacji wśród studentów i instruktorów harcerskich*, Łódź 2018.

[2] Norma ISO/IEC 27032:2012 Information technology – Security techniques – Information security incident management definiuje cyberprzestrzeń jako „złożone środowisko będące rezultatem oddziaływań ludzi, oprogramowania i usług w Internecie prowadzonych za pomocą urządzeń i sieci przyłączonych do niego, które nie istnieje w formie materialnej" (a więc swoiście rozumiany nadsystem, którego Internet jest „bazą").

jest jednym z podstawowych działań mającym mających na celu uniknięcie lub zminimalizowanie skutków utraty bezpieczeństwa informacji.

W artykule porównano wyniki dwóch badań sprawdzających poziom tej wiedzy oraz jej wpływ na postawy i zachowania badanych osób[3]. Pierwsze badanie przeprowadzone zostało w wybranych grupach osób zajmujących się nauczaniem i wychowywaniem[4], drugie, wśród osób pracujących w wojewódzkim sądzie administracyjnym.

Pojęcia podstawowe

Rozważania nad kwestiami cyberbezpieczeństwa i bezpieczeństwem informacji należy rozpocząć od ustalenia słownictwa, panuje bowiem w tych dziedzinach daleko idący chaos terminologiczny, różne definicje stosowane są zarówno w literaturze przedmiotu, jak i w różnych aktach prawnych[5]. Dla potrzeb niniejszego artykułu pojęcia używane będą w sensie z definicji zawartych w normach międzynarodowych.

Cyberbezpieczeństwo definiuje się w normie ISO/IEC 27032 jako bezpieczeństwo informacji w cyberprzestrzeni[6]. Bezpieczeństwo informacji jest z kolei zdefiniowane w normie PN-ISO/IEC 27000: jako

[3] R. J. Hill, M. Fishbein, I. Ajzen, *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research,* „Contemporary Sociology" 1977, nr 6 (2), s. 244.

[4] Badania przeprowadzone były w ramach pracy magisterskiej: M. Szmit, *Świadomość…,* op. cit.

[5] Por. J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 31; M. Szmit, *Cyberbezpieczeństwo jako zagadnienie interdyscyplinarne,* [w:] M. Chrabkowski et al. (red,), *Bezpieczeństwo w administracji i biznesie jako czynnik europejskiej integracji i rozwoju*, Gdynia 2015, s. 393–400.

Przegląd standardów i praktyk zarządzania bezpieczeństwem informacji można znaleźć w pracy: A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa 2006.

Natomiast zestawienie definicji zawartych w ustawach i rozporządzeniach – w pracy: M. Szmit, A. Szmit, *O normatywnych definicjach cyberbezpieczeństwa,* [w:] K. Załęski, P. Polko (red.), *Bezpieczeństwo Polski w drugiej dekadzie XXI wieku*, Dąbrowa Górnicza 2019.

[6] Por.: ISO/IEC 27032:2012 Information…, op. cit.

zachowanie poufności, integralności i dostępności informacji, a dodatkowo także innych własności, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność[7]. Z kolei te własności bezpieczeństwa informacji zdefiniowane zostały odpowiednio jako:

- **poufność** (ang. *confidentiality*, ISO/IEC 27000:2018-3.10), własność polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, przedmiotom lub procesom;
- **integralność** (ang. *integrity*, ISO/IEC 27000:2018-3.36), własność polegająca na zapewnieniu dokładności i kompletności aktywów;
- **dostępność** (ang. *availability*, ISO/IEC 27000:2018-3.7) własność bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.

Dodatkowe własności bezpieczeństwa informacji zdefiniowane są w normach jako:

- **autentyczność** (ang. *authenticity*, ISO/IEC 27000:2018-3.6), właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka jak deklarowana;
- **rozliczalność** (ang. *accountability*, ISO/IEC 2382:2015[8]-2126250) – właściwość, która zapewnia, że określone działania dowolnego podmiotu mogą być jednoznacznie przypisane temu podmiotowi;
- **niezaprzeczalność** (ang. *non-repudiation* – ISO/IEC 27000:2018-3.48) – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden podmiotów uczestniczących w tej wymianie;

[7] Por.: ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary, International Organization of Standardization, Geneva 2018.

[8] Por. ISO/IEC 2382:2015 Information technology — Vocabulary, International Organization of Standardization, Geneva 2015.

- **niezawodność** (ang. *reliability* – ISO/IEC 27000:2018-3.55) – zdolność jednostki funkcjonalnej do wykonywania wymaganej funkcji w danych warunkach w danym przedziale czasu.

Warto zwrócić uwagę, że informacja nie jest rzeczą, stąd też zarówno własności jej bezpieczeństwa, jak i sposoby jego naruszania są inne, niż w przypadku obiektów materialnych. Na przykład informacji nie można ukraść (jakkolwiek można w nieuprawniony sposób zapoznać się z informacją, która miała pozostać poufna), czy zniszczyć (co najwyżej można zniszczyć nośnik informacji, na którym była ona zapisana). Stąd też wszelkie analogie do zjawisk odnoszących się do bytów materialnych muszą być traktowane bardzo ostrożnie, zaś nawet podstawowe zasady zachowania bezpieczeństwa nie zawsze są proste i intuicyjne. Dodatkowo wysoka złożoność współczesnych systemów informatycznych powoduje, że istnieją zarówno liczne luki bezpieczeństwa o charakterze technicznym, jak i szereg możliwości odpowiedniego zmanipulowania użytkownika systemu (tzw. inżynieria społeczna), wykorzystanie których przez agresorów prowadzić może do daleko idących naruszeń bezpieczeństwa informacji. Z tego punktu widzenia budowanie świadomości bezpieczeństwa informacji jest ze wszech miar potrzebne i pożyteczne.

Mikko T. Siponen[9] definiuje świadomość bezpieczeństwa informacji jako wiedzę jednostki na temat poszczególnych zagrożeń bezpieczeństwa i potencjalnych środków zaradczych wobec tych zagrożeń. Joanna Chmura przedstawia istotę i znaczenie świadomości bezpieczeństwa informacji w organizacji oraz analizuje wybrane metody kształtowania świadomości pracowników w zakresie bezpieczeństwa informacji[10]. Wymienia również model KAB (*Knowledge, Attitude and Behaviour*), który wyjaśnia rolę wiedzy w zmianie zachowań. Zgodnie

[9] Por. M. Siponen, *A conceptual foundation for organizational information security awareness*, „Information Management & Computer Security" 2000, nr 8 (1), s. 31.

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

z tą koncepcją, skłonność osoby do robienia czegoś korzystnego lub niekorzystnego zależy od wiedzy i postawy.

Model KAB wykorzystany był przez Kathryn Parsons, Agatę Mc Cormac, Marcusa Butaviciusa, Malcolma Pattinsona, Cate Jerram do stworzenia narzędzia HAIS-Q (*Human Aspects of Information Security Questionnaire*), które służy do pomiaru świadomości bezpieczeństwa informacji wśród pracowników[11]. Badania te pokazują, że zwiększanie wiedzy pracowników na temat polityk i procedur bezpieczeństwa ma pozytywny wpływ zarówno na postawy wobec tych polityk i procedur, jak i na zachowanie pracowników.

Stefan Bauer, Edward W. N. Bernroider i Katharina Chudzikowski w swoich badaniach zajęli się problemem projektowania skutecznych programów uświadamiających (*Information Security Awareness* – ISA) pracowników, tak aby właściwie zarządzać bezpieczeństwem informacji w organizacji[12]. Badali również w jaki sposób użytkownicy postrzegają te programy uświadamiające i jak one wpływają na zachowanie zgodnego z obowiązującymi zasadami. Badanie przeprowadzone zostało w trzech bankach z Europy Środkowej i Wschodniej. Wyniki badań pokazały między innymi, że projektując programy ISA powinno się rozważyć różne sposoby działania, aby dostosować swoje programy do różnych potrzeb grup użytkowników oraz, że istotne jest interaktywne podejście w procesie uświadamiania użytkowników w zakresie bezpieczeństwa informacji.

Wymagania dotyczące świadomości bezpieczeństwa informacji są zawarte w normie ISO/IEC 27001:2013 w punkcie 7.3[13]. Osoby wykonujące pracę pod nadzorem organizacji muszą być świadome obowiązującej polityki bezpieczeństwa informacji i muszą znać swoją rolę

[11] Por.: K. Parsons, A. Mc Cormac, M. Butavicius, M. Pattinson, C. Jerram, *Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)*, „Computers and Security" 2014, nr 42, s. 174–175.

[12] Por. S. Bauer, E. W. N. Bernroider, K. Chudzikowski, *Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks*, „Computers and Security" 2017, nr 68, passim.

[13] Por. ISO/IEC 27001:2013 ..., op. cit.

w kształtowaniu bezpieczeństwa, dostrzegać korzyści płynące z doskonalenia wyników dotyczących bezpieczeństwa informacji oraz znać konsekwencje niezgodności z wymaganiami systemu zarządzania bezpieczeństwem informacji.

Przedmiot i metody badań

W ramach prac nad świadomością bezpieczeństwa informacji przeprowadzono dwa badania:

- studentów i instruktorów harcerskich oraz
- pracowników Wojewódzkiego Sądu Administracyjnego.

W obu badaniach zastosowaną metodą badawczą był sondaż diagnostyczny, techniką badawczą – ankieta z wykorzystaniem narzędzia CAWI (ang. *Computer-Assisted Web Interview* – wspomagany komputerowo wywiad przy pomocy strony WWW). Taki sposób prowadzenia badania zapewnia wysoką standaryzację testu (brak ryzyka błędów popełnianych przez ankietera), jakkolwiek ograniczona jest kontrola nad tym, kto rzeczywiście wypełnia ankietę. W przypadku prowadzonych przez nas badań to ryzyko było zmniejszone przez celowy dobór respondentów do badania. Ankiety zostały przygotowane w systemie webankieta.pl. W pytaniach, w których więcej niż jedna odpowiedź była odpowiedzią prawidłową, punkt był liczony, gdy wybrano wszystkie właściwe odpowiedzi.

Trafność diagnostyczną testu wiedzy spróbowano osiągnąć poprzez uwzględnienie sumarycznego wyniku odpowiedzi na pytania testowe. W przypadku badania 2 (pracowników sądu) rozkład wyników otrzymanych z testu wiedzy był zgodny z rozkładem normalnym (wartość testu zgodności Shapiro-Wilka wynosiła 0,968 co dla N=60 odpowiada poziomowi istotności 0,111.; wartość testu godności Kołmogorowa-Smirnowa z poprawką istotności Lillieforsa wynosiła 0,132 co dla N=60 odpowiada poziomowi istotności 0,012).

W przypadku badania 1, dla całej badanej grupy, rozkład odpowiedzi nie był zgodny z rozkładem normalnym. Mogłoby to świadczyć

o nieprawidłowym wystandaryzowaniu testu, jednak uwzględniając fakt, że grupa obejmująca wszystkich badanych miała charakter niejednorodny policzono dodatkowo zgodność rozkładów wyników z testu wiedzy otrzymanych w poszczególnych podgrupach z rozkładem normalnym, otrzymując następujące wyniki:

Wśród studentów UNS rozkład wyników otrzymanych z testu wiedzy był zgodny z rozkładem normalnym (wartość testu zgodności Shapiro-Wilka wynosiła 0,882 co dla N=14 odpowiada poziomowi istotności 0,061; wartość testu zgodności Kołmogorowa-Smirnowa z poprawką istotności Lillieforsa wynosiła 0,257 co dla N=14 odpowiada poziomowi istotności p: 0,013).

Wśród studentów UŁ rozkład wyników otrzymanych z testu wiedzy nie był zgodny z rozkładem normalnym (wartość testu zgodności Shapiro-Wilka wynosiła 0,829 co dla N=35 odpowiada poziomowi istotności mniejszemu niż 0,001, wartość testu zgodności Kołmogorowa-Smirnowa z poprawką istotności Lillieforsa wynosiła 0,285 co dla N=35 odpowiada poziomowi istotności mniejszemu niż 0,001).

Wśród studentów innych uczelni rozkład wyników otrzymanych z testu wiedzy był zgodny z rozkładem normalnym (wartość testu zgodności Shapiro-Wilka wynosiła 0,827 co dla N=8 odpowiada poziomowi istotności 0,056; wartość testu zgodności Kołmogorowa wynosiła 0,263 co dla N=8 odpowiada poziomowi istotności 0,109).

Wśród instruktorów harcerskich rozkład wyników otrzymanych z testu wiedzy nie był zgodny z rozkładem normalnym (wartość testu zgodności Shapiro-Wilka wynosiła 0,824 co dla N=26 odpowiada poziomowi istotności mniejszemu niż 0,001, wartość testu zgodności Kołmogorowa-Smirnowa z poprawką istotności Lillieforsa wynosiła 0,284 co dla N=26 odpowiada poziomowi istotności mniejszemu niż 0,001).

W dwóch z czterech wyodrębnionych grup badana cecha statystyczna ma więc rozkład normalny, zaś w dwóch – nie. Rozpatrując łącznie wszystkich uczestników badania 1: rozkład miał charakter jednomodowy, natomiast jego skośność wynosiła 0,88, czyli rozkład charakteryzował się prawostronną asymetrią – mediana osiągniętego

wyniku była mniejsza od średniej: w grupie było nadspodziewanie dużo osób o małej wiedzy (średni wynik z testu 1,41 z 5), szczególnie że z merytorycznego punktu widzenia zadane pytania i tak w większości odnosiły się do wiedzy elementarnej, brak której może stanowić istotny czynnik ryzyka przy korzystaniu z urządzeń techniki komputerowej).

Badanie 1

Pierwsze badanie zostało przeprowadzone w okresie od 12 lipca do 11 listopada 2018 r w ramach pracy magisterskiej „Świadomość bezpieczeństwa informacji wśród studentów i instruktorów harcerskich”[14]. Celami badania były:

- poznanie wiedzy i poglądów respondentów na wybrane tematy związane z cyberbezpieczeństwem;
- porównanie, czy badane grupy różnią się od siebie pod względem posiadanej wiedzy bądź poglądów;
- stwierdzenie czy istnieje związek statystyczny pomiędzy wykształceniem uczestników badania, grupą, do jakiej należeli, ich wiedzą (mierzoną liczbą prawidłowych odpowiedzi na pytania dotyczące cyberbezpieczeństwa) bądź poglądami na temat cyberbezpieczeństwa.

Badanie ankietowe objęło trzy grupy osób: instruktorów Związku Harcerstwa Polskiego, Studentów Uczelni Nauk Społecznych (kierunek pedagogika) oraz – jako grupę porównawczą – studentów innych uczelni. Problematyka pracy dotyczyła świadomości bezpieczeństwa informacji, w szczególności wśród osób zajmujących się wychowaniem, a więc takich, które powinny prezentować odpowiednio wysoki poziom kultury bezpieczeństwa informacji. Osoby takie powinny – przynajmniej w zakresie elementarnym – umieć zadbać o bezpieczeń-

[14] Por. M. Szmit, *Świadomość…,* op. cit.

stwo własne i swoich podopiecznych. W pracy rozważano następujące problemy badawcze:

1. Jaki jest stan wiedzy na temat bezpieczeństwa informacji wśród uczestników badania?
2. W jakim stopniu uczestniczenie w szkoleniach z zakresu bezpieczeństwa informacji przekłada się na wzrost wiedzy z zakresu tegoż bezpieczeństwa?
3. Czy istnieje związek między płcią a częstością wykonywania kopii bezpieczeństwa[15]?
4. W jakim stopniu uczestniczenie w szkoleniach z zakresu bezpieczeństwa informacji przekłada się na praktykę w zakresie wykonywania kopii bezpieczeństwa?
5. Czy istnieje związek pomiędzy wiedzą z zakresu cyberbezpieczeństwa a postrzeganiem rodzajów zagrożeń[16] (związanych z treścią oraz natury technicznych)?

Dobór próby miał charakter celowy (dostępność badanych). W badaniu uczestniczyło 31 instruktorów harcerskich Związku Harcerstwa Polskiego (niektórzy z nich to także studenci), 14 studentów pedagogiki z Uczelni Nauk Społecznych oraz 50 studentów kierunków niepedagogicznych innych uczelni, w tym jedna osoba nie będąca ani studentem ani instruktorem harcerskim.

Badanie prowadzone było anonimowo. Pięć pytań w kwestionariuszu dotyczyło wiedzy na temat bezpieczeństwa informacji. Jedno py-

[15] Kopia bezpieczeństwa (ang. *Backup*) – pliki, sprzęt, dane i procedury dostępne do wykorzystania w przypadku awarii lub innych strat, jeżeli oryginały są zniszczone lub niedostępne.

Por. *Glossary*, ISACA, https://www.isaca.org/Pages/Glossary.aspx [dostęp: 10-06-2019].

[16] Zagrożenia bezpieczeństwa podzielono umownie na dwa rodzaje: zagrożenia związane z technicznymi aspektami przetwarzania informacji (tj. związane z ryzykiem naruszenia poufności, integralności, dostępności i pozostałych własności bezpieczeństwa informacji) oraz zagrożenia związane z treścią (ang. *content*) informacji (do tzw. „przestępstw kontentowych", będących specyficznym rodzajem przestępstw z wykorzystaniem komputerów zalicza się na przykład piractwo programów komputerowych czy rozpowszechnianie pornografii dziecięcej).

tanie dotyczyło zachowań (częstotliwości wykonywania przez respondenta kopii bezpieczeństwa swoich danych), pozostałe pytania miały na celu zbadania poglądów osób ankietowanych. Łączna liczba osób biorących udział w ankiecie wynosiła 83. Wśród badanych było 50 kobiet i 33 mężczyzn, przeważały osoby w wieku 23 lat, średnia wieku wynosiła 27,5 roku, zaś mediana – 23 lata. Prawie połowę badanych stanowiły osoby z wykształceniem średnim, a nieco ponad jedną trzecią – osoby po studiach. W szkoleniu dotyczącym bezpieczeństwa informacji lub cyberbezpieczeństwa brało udział 30 osób (36,14% respondentów). Przeprowadzone badanie ankietowe miało na celu poznanie wiedzy i poglądów respondentów na wybrane tematy związane z cyberbezpieczeństwem oraz stwierdzenie czy istnieje związek statystyczny pomiędzy wykształceniem uczestników badania, grupą, do jakiej należeli, ich wiedzą (mierzoną liczbą prawidłowych odpowiedzi na pytania dotyczące cyberbezpieczeństwa) bądź poglądami na temat cyberbezpieczeństwa.

Badanie 2

Drugie badanie zostało przeprowadzone w okresie od 3 lutego do 24 marca 2019 roku wśród pracowników wojewódzkiego sądu administracyjnego. W badaniu uczestniczyły zarówno osoby z wykształceniem prawniczym: sędziowie, asesorzy, referendarze sądowi, asystenci sędziów, jak i pracownicy administracyjni. Organizacja wdrożyła System Zarządzania Bezpieczeństwem Informacji (SZBI) i objęła pracowników obowiązkiem uczestnictwa w szkoleniach z zakresu bezpieczeństwa informacji. Sędziowie są informowani o przepisach wewnętrznych obowiązujących w organizacji, ale nie są zobligowani do udziału w szkoleniach z zakresu bezpieczeństwa informacji.

Przepisy prawa Unii Europejskiej[17] i prawa polskiego[18] regulują wiele kwestii związanych z bezpieczeństwem informacji. Wynika to

[17] Por. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

z faktu, że bezpieczeństwo informacji ma wpływ na bezpieczeństwo organizacji działających w państwie, a przede wszystkim na bezpieczeństwo obywateli. W wojewódzkich sądach administracyjnych, których głównym zadaniem jest badanie właściwego stosowania prawa przez administrację państwową i samorządową, świadomość bezpieczeństwa informacji wśród pracowników powinna być wysoka. Sąd przetwarza informacje, których bezpieczeństwo powinno być szczególnie chronione.

Celem badania było poznanie wiedzy i poglądów respondentów na wybrane tematy związane z cyberbezpieczeństwem. Kwestionariusz ankiety i problemy badawcze w badaniu przeprowadzonym wśród pracowników sądu administracyjnego różniły się nieco od użytych w badaniu osób związanych z wychowaniem. Rozważono następujące problemy badawcze:

1. Jaki jest poziom wiedzy na temat bezpieczeństwa informacji wśród uczestników badania?
2. W jakim stopniu udział w szkoleniach z zakresu bezpieczeństwa informacji przekłada się na wzrost wiedzy na temat bezpieczeństwa informacji?
3. Czy istnieje związek między płcią a częstotliwością kopii zapasowych?
4. W jakim stopniu uczestnictwo w szkoleniach z zakresu bezpieczeństwa informacji przekłada się na praktykę używania i aktualizacji oprogramowania antywirusowego[19]?

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1); Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

[18] Por. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. poz. 1560); Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz.U. z 2017 r., poz. 2247).

[19] Oprogramowanie antywirusowe (ang. *Antivirus software*) – aplikacja wdrożona w wielu punktach architektury IT. Zaprojektowana tak, aby wykrywać i eliminować

5. Czy istnieje związek między wiedzą na temat cyberbezpieczeństwa a postrzeganiem nowoczesnych technologii informacyjno-komunikacyjnych?

Badanie zostało przeprowadzone anonimowo. Dziesięć pytań w kwestionariuszu dotyczyło wiedzy na temat bezpieczeństwa informacji. Pięć pytań dotyczyło zachowań, pozostałe pytania dotyczyły poglądów na temat ochrony informacji w miejscu pracy, percepcji technologii informacyjnych i komunikacyjnych oraz pytań dotyczących wieku, płci, udziału w szkoleniach. Łączna liczba osób biorących udział w badaniu wyniosła 60. Respondentami było 47 kobiet i 13 mężczyzn, dominującą grupę wiekową stanowiły osoby w wieku 41–60 lat – 38 osób. 53 osoby przynajmniej raz wzięło udział w szkoleniu (88,33% respondentów).

Wyniki

W badaniu przeprowadzonym wśród studentów i instruktorów harcerskich najwięcej osób uzyskało 1 punkt na 5 możliwych do uzyskania (Rysunek 2). Średnia liczba punktów jaką uzyskali respondenci wyniosła 1,41 punktów na 5 możliwych do uzyskania. Mediana wyników testu wiedzy wyniosła 1 punktów.

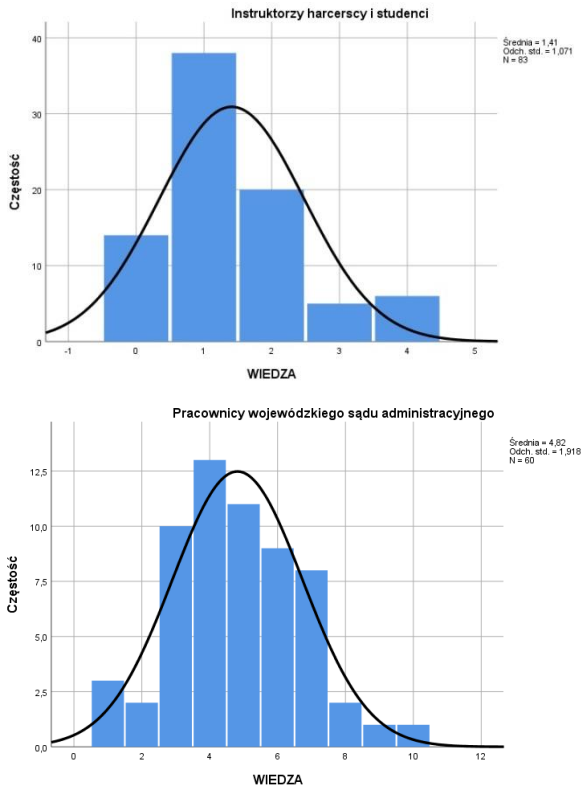
W badaniu pracowników sądu średnia liczba punktów jaką uzyskali respondenci wyniosła 4,82 punktów na 10 możliwych do uzyskania mediana wyników testu wiedzy wyniosła 5 punktów.

W badaniach przeprowadzonych na grupie studentów i instruktorów harcerskich nie zauważono pozytywnego wpływu szkoleń z zakresu cyberbezpieczeństwa na wiedzę osób, biorących udział w takich szkoleniach. Otrzymane wyniki statystyki r Pearsona wskazują na istnienie ujemnej, statystycznie nieistotnej korelacji pomiędzy wiedzą osób biorących udział w badaniu a faktem bycia przeszkolonym,

kod wirusowy przed dokonaniem uszkodzenia oraz naprawiać lub poddawać kwarantannie pliki, które zostały już zainfekowane. Por.: *Glossary…,* op. cit.

to znaczy osoby przeszkolone nie mają większej wiedzy z zakresu bezpieczeństwa niż osoby nieprzeszkolone.

Rysunek 2. Histogramy punktów uzyskanych z testu wiedzy o bezpieczeństwie informacji



Źródło: Opracowanie własne.

Otrzymane, w badaniu przeprowadzonym wśród pracowników sądu, wyniki statystyki r Pearsona wskazują na umiarkowaną korelację liniową pomiędzy faktem uczestniczenia w szkoleniach a wiedzą. Wartość współczynnika V Cramera V= 0,426 (χ^2=21.794 przy wartości krytycznej testu χ^2= 28,87 i poziomie istotności p=0,05) wskazują na statystycznie nieistotną kontyngencję. Podobna zależność w grupie

pracowników WSA istnieje pomiędzy wiekiem a wiedzą na temat bezpieczeństwa przetwarzania informacji. Im starsze osoby, tym słabsze wyniki uzyskały w teście wiedzy.

W badaniu wśród instruktorów harcerskich i studentów otrzymane wyniki statystyki V Cramera wskazują na istotną kontyngencję pomiędzy płcią a częstością wykonywania kopii bezpieczeństwa: Kobiety wykonują takie kopie rzadziej niż mężczyźni. Kierunek znalezionej zależności wydaje się być nieintuicyjny (tradycyjnie raczej kobiety postrzega się jako dbające bardziej o bezpieczeństwo, zaś mężczyzn – jako skłonnych do, często nawet nadmiernego, ryzyka). Również badania wśród pracowników sądu potwierdziły zależność, iż kobiety rzadziej wykonują kopię bezpieczeństwa danych, w tym przypadku zależność nie jest jednak statystycznie istotna.

Tylko 15% pracowników sądu twierdzi, że wykonuje kopie zapasowe codziennie lub raz w tygodniu, 46,7% twierdzi, że nie tworzy kopii zapasowych. Również wyniki w grupie instruktorów harcerskich i studentów są niepokojące, tylko 8,43% twierdzi, że wykonuje kopie codziennie lub raz w tygodniu, 33,73% – nie tworzy kopii w ogóle. W tej grupie otrzymane wyniki statystyki V Cramera V=0,578 przy wartości testu χ^2=27,7 i wartości krytycznej testu χ^2=5,99 wskazują na istotną statystycznie kontyngencję pomiędzy uczestnictwem w formalnych szkoleniach z zakresu cyberbezpieczeństwa a wpływem na zachowania osób, biorących udział w takich szkoleniach, w zakresie wykonywania kopii bezpieczeństwa. U osób pracujących w sądzie stwierdzono taką zależność, jednakże nie jest ona statystycznie istotna. W tej grupie osób stwierdzono również pozytywny związek pomiędzy udziałem w szkoleniu z zakresu bezpieczeństwa informacji a częstością instalacji i aktualizacji oprogramowania antywirusowego (V= 0,473 z χ^2=26.820, wartość krytyczna testu wynosi χ^2= 12,592 dla poziomu istotności α=0,05, liczba stopni swobody df=6, co oznacza, że kontyngencja jest statystycznie istotna – zob. tabela 1).

Tabela 1. Porównanie wyników badań w zakresie wykonywania kopii bezpieczeństwa oraz instalacji i aktualizacji programów antywirusowych

	Instruktorzy harcerscy i studenci	**Pracownicy WSA**
Respondenci, którzy wykonują kopię bezpieczeństwa codziennie lub raz w tygodniu	8,43% (7 respondentów)	15% (9 respondentów)
Respondenci, którzy nie wykonują kopii bezpieczeństwa w ogóle	33,73% (28 respondentów)	46,7% (28 respondentów)
Płeć a wykonywanie kopii bezpieczeństwa	Istotna statystycznie kontyngencja V=0,333 χ^2=9,21 , wartości krytyczna χ^2=5,99	Nieistotna statystycznie kontyngencja V=0,291 χ^2=5,091 , wartości krytyczna χ^2=9,488
Uczestniczenie w szkoleniach z zakresu cyberbezpieczeństwa a wykonywanie kopii bezpieczeństwa	Istotna statystycznie kontyngencja V=0,578 χ^2=27,7, wartości krytyczna χ^2=5,99	Nieistotna statystycznie kontyngencja V=0,189 χ^2=4,292 , wartości krytyczna χ^2=15,51
Uczestniczenie w szkoleniach z zakresu cyberbezpieczeństwa a instalacja i aktualizacja programu antywirusowego	–	Istotna statystycznie kontyngencja V=0,473χ^2=26.820, wartość krytyczna χ^2= 12,592

Źródło: Opracowanie własne.

Tylko 15,66% instruktorów harcerskich i studentów (13 respondentów) zdaje sobie sprawę z rzeczywistej częstotliwości występowania incydentów związanych z bezpieczeństwem informacji w ciągu roku. Niewiele więcej, bo 18,33% pracowników sądu (11 respondentów) udzieliło poprawnej odpowiedzi na to pytanie. Również tylko 6,67% respondentów (4 osoby) dostrzega problemy, z pewnością wy-

stępujące, związane z bezpieczeństwem informacji przetwarzanych w sądzie.

Wśród instruktorów harcerskich i studentów 13,28% respondentów (11 osób) uważa nowoczesne technologie informacyjno-komunikacyjne[20] za zjawisko groźne, jakkolwiek posiadające kilka pozytywów, które można wykorzystać przy zachowaniu szczególnej ostrożności, wśród pracowników sądu ten odsetek jest mniejszy, wynosi 8,33% (5 respondentów). W obu grupach nie było osób, które zgodziłyby się ze stwierdzeniem, że jest to zjawisko zdecydowanie groźne, nie posiadające żadnych lub prawie żadnych aspektów pozytywnych.

Podsumowanie

Stosunkowo duża liczba punktów, którą otrzymali z testu z wiedzy pracownicy WSA wynika zapewne z faktu, że więcej osób z tej grupy uczestniczyło w szkoleniach dotyczących bezpieczeństwa informacji. Uzyskana wiedza wpłynęła na zachowanie respondentów w aspekcie zminimalizowania ryzyka utraty bezpieczeństwa informacji, jednakże wpływ ten nie jest satysfakcjonujący. Wyniki badań wskazują zatem na konieczność zmiany sposobu kształcenia w tym zakresie, tak aby za większą wiedzą szły bardziej właściwe zachowania.

W literaturze przedmiotu można znaleźć szereg uwag krytycznych dotyczących szkoleń z bezpieczeństwa informacji, jak również szereg zaleceń, które powinny spełniać szkolenia z zakresu cyberbezpieczeń-

[20] Pod pojęciem technologii informacyjnych i komunikacyjnych (ang. *Information and communication technologies,* w skrócie ICT, zwane zamiennie technologiami informacyjno-telekomunikacyjnymi, teleinformatycznymi lub technikami informacyjnymi) kryje się rodzina technologii przetwarzających, gromadzących i przesyłających informacje w formie elektronicznej. Węższym pojęciem są technologie informatyczne (IT), które odnoszą się do technologii związanych z komputerami i oprogramowaniem, nie związanych jednak z technologiami komunikacyjnymi i dotyczącymi sieci. Por. *Społeczeństwo informacyjne w Polsce. Wynik badań statystycznych z lat 2006-2010*, Główny Urząd Statystyczny, Warszawa 2010,
https://stat.gov.pl/cps/rde/xbcr/gus/nts_spolecz_inform_w_polsce_2006-2010.pdf [dostęp: 15-05-2019].

stwa, aby mogły skutecznie podnosić świadomość bezpieczeństwa[21]. Zaleca się między innymi, aby szkolenia takie obejmowały praktyczne laboratoria, rzeczywiste scenariusze i przykłady z życia codziennego, symulacje, konkursy, odtwarzanie nagrań wideo. Zaleca się przewagę praktyki nad teorią, elastyczną strukturę zajęć, ciągłe uaktualnianie materiałów, szkolenie prowadzących[22].

Wyniki porównywanych badań wskazują pewien (słaby lub umiarkowany) wpływ świadomości bezpieczeństwa na odpowiednie zachowania w zakresie bezpieczeństwa. Oznacza to, że pewne metody eliminowania negatywnych skutków bądź zapobiegania przyczynom zdarzeń związanych z bezpieczeństwem informacji poznanych w trakcie szkoleń są stosowane, pewne zaś nie. Wyniki badań wśród pracowników sądu wskazują, że więcej osób systematycznie aktualizuje oprogramowanie antywirusowe niż stosuje mechanizmy kopii bezpieczeństwa. W ich miejscu pracy za wykonanie kopii odpowiedzialne są służby informatyczne, więc użytkownicy przetwarzający informacje w miejscu pracy nie muszą samodzielnie dbać o to zabezpieczenie danych, stąd nie mają takiego nawyku również w odniesieniu do danych prywatnych. Można uznać, że użytkownicy niewłaściwie oceniają ryzyko i skutki utraty danych na komputerach prywatnych. Planowane w przyszłości przeprowadzenie badań przy użyciu modelu PMT[23] (ang. *Protection Motivation Theory*), może pozwolić na ocenę, czy świadomość zagrożeń (ang. *Threat Awareness*), czy świadomość przeciwdziałania (ang. *Countermeasure Awareness*), ma większy wpływ w badanych grupach użytkowników na bezpieczne zachowanie[24].

---

[21] Por. R. Leszczyna, *Nauczanie zagadnień cyberbezpieczeństwa w Unii Europejskiej – trendy, wyzwania,* „Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej" 2007, nr 52, s. 64.

[22] Por. A. Szmit, M. Szmit, *Kilka uwag o dydaktyce bezpieczeństwa informatycznego*, [w:] A. Kwiatkowski, A. Urbanek (red.), *Edukacja dla bezpieczeństwa – wybrane zagadnienia*, Słupsk 2013, s. 72.

[23] Por. R. W. Rogers, *A protection motivation theory of fear appeals and attitude change,* „The Journal of Psychology" 1975, nr 91 (1), passim.

[24] Por. B. Hanus, Y. „Andy" Wu, *Information Systems Management Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective*, „Information Systems Management" 2017, nr 33(1), passim.

Świadomość liczby zagrożeń pojawiających się w Internecie jest niska. Niskie jest również zaangażowanie w kwestie bezpieczeństwa i słaby poziom wrażliwości na incydenty wewnątrz organizacji, co może mieć negatywny wpływ na bezpieczeństwo informacji. Nowoczesne techniki informacyjno-komunikacyjne są natomiast uznawane przez większość respondentów za zjawisko pozytywne, oferujące szereg szans i możliwości.

Kształcenie w zakresie bezpieczeństwa informacji powinno obejmować wszystkie grupy zawodowe, również te, które nie są zobligowane prawem do obowiązkowego uczestnictwa. Można przypuszczać, że obligatoryjność szkoleń, kontrola i rozliczalność w miejscu pracy wpłynęła by pozytywnie na poziomu wiedzy i odpowiednie zachowanie pracowników sądu. Studenci i instruktorzy harcerscy nie są, aż tak bardzo rozliczani ze swoich działań. Pożądany obowiązek stosowania zasad bezpieczeństwa informacji jest trudny do uzyskania bez odpowiedniego kształcenia w tym zakresie. Szkolenia powinny odbywać się systematycznie, gdyż często zmienia się sposób przetwarzania informacji, wykorzystywane są nowe narzędzi oraz pojawiają się nowe zagrożenia. Szkolenia nie tylko powinny przekazywać teoretyczną wiedzę na temat zagrożeń i środków zaradczych, ale skupić się na praktycznym jej wykorzystaniu[25]. Wiedza i umiejętność stosowania środków zaradczych przyczynia się do wykształcenia odpowiednich postaw i zachowań.

Bibliografia:

Bauer S., Bernroider E. W. N., Chudzikowski K., *Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks*, „Computers and Security" 2017, nr 68.

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wyd. PWN, Warszawa 2006.

[25] Por. K. Parsons et al., op. cit., s. 174.

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

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

Glossary, ISACA, https://www.isaca.org/Pages/Glossary.aspx.

Hanus B., Wu Y. „Andy", *Information Systems Management Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective*, „Information Systems Management", 2017, nr 33 (1).

Hill R. J., Fishbein M., Ajzen I., *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research,* „Contemporary Sociology" 1977, nr 6 (2).

ISO/IEC 2382:2015 Information technology – Vocabulary, International Organization of Standardization, Geneva 2015.

ISO/IEC 27000:2018 Information technology Security techniques – Information security management systems – Overview and vocabulary, International Organization of Standardization, Geneva 2018.

ISO/IEC 27001:2013 Information technology – S*ec*urity techniques – Information security management systems – Requirements, International Organization of Standardization, Geneva 2013.

ISO/IEC 27032:2012 Information technology – Security techniques – Information security incident management, International Organization of Standardization, Geneva 2012.

Kosiński J., *Paradygmaty cyberprzestępczości*, Wyd. Difin, Warszawa 2015.

Leszcz*yna R., Nauczanie zagadnień cyberbezpieczeństwa w Unii Europejskiej – trendy, wyzwania,* „Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej" 2007, nr 52.

Parsons K., Mc Cormac A., Butavicius M., Pattinson M., Jerram C., *Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q),* „Computers and Security" 2014, nr 42.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

Rogers R.W., *A protection motivation theory of fear appeals and attitude change,* „The Journal of Psychology" 1975, nr 91 (1).

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. 2017, poz. 2247).

Siponen M., *A conceptual foundation for organizational information security awareness*, „Information Management & Computer Security" 2000, nr 8 (1).

Społeczeństwo informacyjne w Polsce. Wynik badań statystycznych z lat 2006–2010, Główny Urząd Statystyczny, Warszawa 2010, https://stat.gov.pl/cps/rde/xbcr/gus/nts_spolecz_inform_w_polsce_2006-2010.pdf.

Szmit A., Szmit M., *Kilka uwag o dydaktyce bezpieczeństwa informatycznego*. [w:] A. Kwiatkowski, A. Urbanek (red.), *Edukacja dla bezpieczeństwa – wybrane zagadnienia*, Wyd. Akademii Pomorskiej w Słupsku, Słupsk 2013.

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

Szmit M., *Cyberbezpieczeństwo jako zagadnienie interdyscyplinarne,* [w:] M. Chrabkowski et al. (red,), *Bezpieczeństwo w administracji i biznesie jako czynnik europejskiej integracji i rozwoju*, Wyd. Wyższej Szkoły Administracji i Biznesu, Gdynia 2015.

Szmit M., *Świadomość bezpieczeństwa informacji wśród studentów i instruktorów harcerskich*, Wyd. Uczelni Nauk Społecznych w Łodzi, Łódź 2018.

Torten R., Reaiche C., Boyle S., *The impact of security awareness on information technology professionals' behavior,* „Computers and Security" 2018, nr 79.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018, poz. 1560).