Teresa Gądek-Hawlena
University of Economics in Katowice
gadek@ue.katowice.pl
ORCID id: https://orcid.org/0000-0003-4350-1246

Konrad Michalski
Szkoła Główna Gospodarstwa Wiejskiego w Warszawie
konrad_michalski@sggw.edu.pl
ORCID id: https://orcid.org/0000-0001-6997-352X

JOURNAL OF MODERN SCIENCE
TOM 1/48/2022 str. 141-159
www.jomswsge.com
DOI: https://doi.org/10.13166/jms/150599

Remote education and student online safety

Zdalna edukacja a bezpieczeństwo studentów w sieci internet

Abstract

The COVID-19 pandemic has had a significant impact on the higher education sector. The transfer of teaching activities to the web has seriously increased the likelihood of successful cyber-attacks on the student user group of the Internet. This paper explores the relationship between remote teaching and online student safety. 622 students from three Polish universities participated in the study. It was found that: (1) during remote teaching, students' main activities were browsing content posted by lecturers and participating in teaching activities. (2) Students primarily communicated via Facebook (93.09%), (3) The most common cyber threats encountered by students were spam, online auction scams and communication fraud. (4) Students' cybersecurity knowledge and security level in cyberspace is at an average level. (5) Students change their account passwords not at all (25.88%) or less often than once a year (39.87%),

and use antivirus software to a greater extent (69.61% of respondents). The correlation analysis between demographic variables and the frequency of changing passwords showed a statistically significant relationship in the case of the form of education and the level of study. On the other hand, taking into account the selected variables and the software used, a statistically significant relationship was only found in the case of the gender of the students and the form of study, while in the case of the other variables, there was no statistically significant relationship. Three of the parameters which was the question of interest in cyber security training at the university is statistically significant in the case of gender, age and level of study.

Streszczenie

Pandemia COVID-19 wpłynęła w istotny sposób na sektor szkolnictwa wyższego. Przeniesienie aktywności dydaktycznej do sieci poważnie zwiększyło prawdopodobieństwo udanych cyberataków na grupę użytkowników Internetu, jaką są studenci. W niniejszym artykule zbadano zależność pomiędzy zdalnym nauczaniem a bezpieczeństwem studentów w sieci. W badaniu wzięło udział 622 studentów trzech polskich uczelni wyższych. Stwierdzono, że: (1) w trakcie zdalnego nauczania główną aktywnością studentów było przeglądanie zamieszczanych przez wykładowców treści oraz udział w zajęciach dydaktycznych; (2) studenci komunikowali się przede wszystkim za pomocą Facebooka (93,09%); (3) najczęściej spotykanymi przez studentów cyberzagrożeniami był spam, oszustwa na aukcjach internetowych oraz oszustwa komunikacyjne; (4) wiedza na temat cyberbezpieczeństwa oraz poziom bezpieczeństwa studentów w cyberprzestrzeni jest na średnim poziomie; (5) studenci wcale (25,88%) lub rzadziej iż raz do roku (39,87%) zmieniają hasła zabezpieczające konta, w większym zakresie wykorzystują oprogramowania antywirusowe (69,61% badanych). Przeprowadzona analiza korelacji pomiędzy wybranymi zmiennymi a częstotliwością zmiany haseł wykazała zależność istotną statystycznie w przypadku formy kształcenia i poziomu studiów. Z kolei uwzględniając zmienne demograficzne i wykorzystywane oprogramowanie, należy stwierdzić, iż zależność statystycznie istota występuje tylko w przypadku płci studentów i formy kształcenia, w przypadku pozostałych zmiennych brak zależności statystycznie istotnej. Zainteresowanie szkoleniami na uczelni z zakresu cyberbezpieczeństwa, jest statystycznie istotne w przypadku płci, wieku i poziomu studiów.

Keywords: *Internet, cyber security, student, remote education, knowledge*

Słowa kluczowe: *Internet, cyberbezpieczeństwo, student, zdalna edukacja, wiedza*

Wprowadzenie

XXI w. to czas przemian, na który wpływ wywiera z jednej strony dynamiczny rozwój w obszarze technologii informacyjnych i komunikacyjnych, a z drugiej – pandemia COVID-19. Szybkie przenoszenie choroby koronawirusowej (COVID-19) pod koniec 2019 r. negatywnie wpłynęło na wszystkie aspekty społeczeństwa, w tym na edukację. Wiele uczelni na świecie przechodziło z nauczania w klasie *face-to-face* do nauczania online. Uniwersytety musiały znaleźć alternatywne sposoby edukacji, testując dostępne platformy i strategie nauczania online, aby kontynuować proces edukacji (Ulla, Perales, 2021, s. 7 i 11). Zdalne nauczanie daje studentom i wykładowcom możliwość pozostania w kontakcie i zaangażowania się w treści podczas pracy w domu (Ray, 2020). Edukacja zdalna nie byłaby jednak możliwa bez szerokiej gamy narzędzi cyfrowych przeznaczonych do prowadzenia zajęć online, platform e-learningowych, cyfrowych zasobów edukacyjnych (Plebańska, Szyller, Sieńczewska 2020). Ogólnie przyjmuje się, że edukacja cyfrowa obejmuje dwa główne nurty: rozwój kompetencji cyfrowych dla osób uczących się oraz pedagogiczne wykorzystanie technologii cyfrowych w celu transformacji i ulepszania nauczania (EC, 2019).

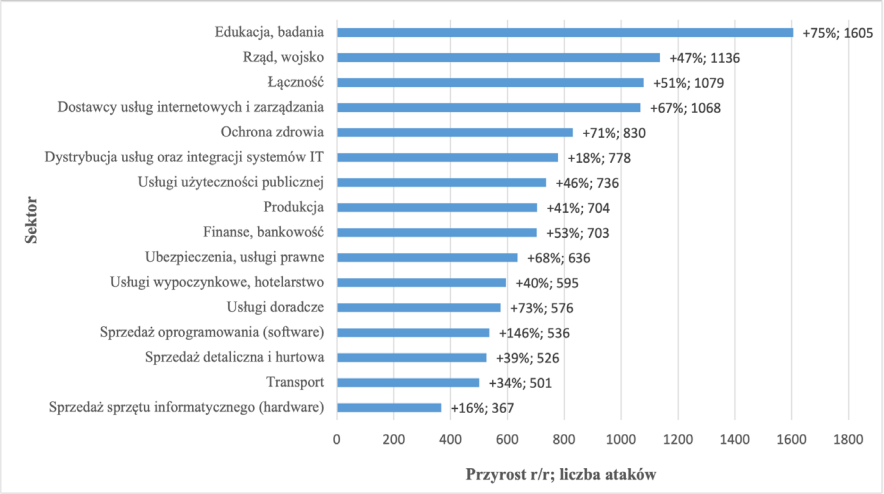
Jak wynika z badań, edukacja cyfrowa posiada wiele zalet, ale napotyka liczne trudności (Mukuka, Shumba, Mulenga, 2021; Leigh, Templet, Watson, 2021). Jedną z nich, stanowiącą przedmiot wielu opracowań naukowych, jest cyberprzestępczość (Škiljič, 2020; Suskruth, Reddy, Chandavarkar 2021; Fouad, 2021). Zjawisko to, wg definicji z X Kongresu ONZ w Sprawie Zapobiegania Przestępczości i Traktowania Przestępców, można sklasyfikować jako:

a. cyberprzestępstwo w sensie wąskim (przestępstwo komputerowe), obejmujące wszelkie nielegalne działania skierowane przeciwko bezpieczeństwu systemów komputerowych i elektronicznie przetwarzanych przez te systemy danych, wykonywane z wykorzystaniem operacji elektronicznych oraz
b. cyberprzestępstwo w sensie szerokim (przestępstwo dotyczące komputerów), obejmujące wszelkie nielegalne działania popełnione przy użyciu lub skierowane przeciwko systemom czy sieciom komputerowym, włączając w to m.in. nielegalne posiadanie oraz udostępnianie lub rozpowszechnianie

informacji za pomocą komputera bądź sieci (Wasilewski, 2016; Jaroszewska, 2017; Such-Pyrgiel, Gołębiowska, Prokopowicz, 2022, s. 2-4).

Katalog przestępstw popełnianych w cyberprzestrzeni jest znaczny (Gov.pl, 2022), wśród najpopularniejszych zagrożeń wymienia się: malware, spam, kradzież tożsamości, botnet, phishing, DDos, Internet IPR, pornografię dziecięcą, hazard internetowy, oszustwa na aukcjach, oszustwa telekomunikacyjne, pranie brudnych pieniędzy, carding. Liczba tego typu przestępstw systematycznie wzrasta. W Polsce w 2020 r. odnotowano 246 107 zgłoszeń dotyczących potencjalnego wystąpienia incydentu teleinformatycznego, w tym 23 309 okazało się faktycznymi. Liczba tych incydentów w 2020 r. była o ok. 88% wyższa w stosunku do 2019 r. (CSIRT GOV, 2021). Jak wynika z rys. 1, sektor, który dotknęła największa liczba cyberataków w 2021 r., to edukacja i badania.

Rysunek 1.
Średniotygodniowa liczba cyberataków na organizacje wg sektorów działalności



Źródło: [Stealthlabs, 2022].

Sektor edukacyjny i badawczy w porównaniu z rządowym i wojskowym doświadczył o ponad 30% więcej cyberataków i o ok. 33% więcej niż telekomunikacyjny. Ponadto, jak wynika z badań Yan i in (2018), przeprowadzonych wśród 462 studentów uczelni, poprawność oceny cyberbezpieczeństwa przez badanych wahała się w granicach 65%. Wynik ten, w warunkach przeniesienia

nawet całości nauczania do Internetu, nie jest korzystnym i oczekiwanym wśród studentów.

Powyższe stało się przyczynkiem do podjęcia przez autorów badań, które mogłyby przyczynić się do wzbogacenia wiedzy w tym zakresie. Celem poniższej pracy jest zbadane, czy istnieje zależność pomiędzy zdalnym nauczaniem a bezpieczeństwem studentów w sieci.

W świetle wyznaczonego celu wskazano następujące założenia badawcze:

- młodzież akademicka, wykorzystując Internet do różnych aktywności związanych z edukacją zdalną, jest narażona na cyberzagrożenia;
- ponieważ Internet jest powszechnym narzędziem młodych ludzi, nie do końca zwracają oni uwagę na cyberzagrożenia i nie starają się przed nimi zabezpieczać – być może z powodu przyzwyczajenia do łatwej dostępności Internetu.

Metoda badań

Na potrzeby badania opracowano kwestionariusz ankiety, który miał pomóc w realizacji przyjętych celów badawczych. Kwestionariusz został podzielony na trzy części. W pierwszej części, w celu zdefiniowania profilu respondenta, przedstawiono sześć zmiennych demograficznych: płeć, wiek, miejsce zamieszkania, formę kształcenia, poziom studiów, uczelnię. W drugiej części kwestionariusza umieszczono pytania dotyczące działań podejmowanych przez studentów w związku ze zdalną edukacją. W trzeciej części badania respondenci ocenili poziom własnego bezpieczeństwa w sieci w okresie zdalnej edukacji.

Właściwe badanie poprzedził pilotaż. Kwestionariusz został przetestowany na próbie 25 respondentów. Pilotaż miał na celu zapewnienie adekwatności pytań oraz ocenę akceptowalności użytych sformułowań, jak też samo zrozumienie pytań. Ankieta online została stworzona przy użyciu oprogramowania Microsoft Forms, a następnie została udostępniona studentom Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie (SGGW), Uniwersytetu Ekonomicznego w Katowicach (UEKat) oraz dwóch uczelni (z Warszawy i Chorzowa) wchodzących w skład sieci szkół Wyższa Szkoła Bankowa (WSB).

Ankieta była dostępna w okresie listopad–grudzień 2021 r. Do analizy uzyskanych wyników wykorzystano narzędzia statystyki opisowej oraz test niezależności χ^2 (Chen, 2012).

Uczestnicy badania

W badaniu wzięło udział 642 respondentów, których odpowiedzi poddano kontroli i weryfikacji pod względem kompletności, a także poprawności i rzetelności informacji. Miało to na celu eliminację nieprawidłowości w wypełnionych kwestionariuszach. W rezultacie weryfikacji do dalszych badań dopuszczono 622 odpowiedzi.

Tabela 1.
Charakterystyka uczestników badania (N = 622)

Zmienne	Częstotliwość	Odsetek [%]
Płeć		
Kobieta	328	52,73
Mężczyzna	294	47,27
Wiek		
18–23 lata	520	83,60
Powyżej 23 lat	102	16,39
Miejsce zamieszkania		
Wieś	167	26,85
Miasto do 100 tys. mieszkańców	176	28,30
Miasto do 200 tys. mieszkańców	73	11,74
Miasto powyżej 200 tys. mieszkańców	206	33,12
Forma kształcenia		
Studia dzienne	423	68,00
Studia zaoczne	199	32,00
Poziom studiów		
Studia inżynierskie	285	45,82
Studia licencjackie	255	41,00
Studia magisterskie	82	13,18
Uczelnia		
SGGW	311	50,00
UEKat	207	33,28
WSB	104	16,72

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Jak wynika z tab. 1, w badaniu wzięło udział 52,73% kobiet i 47,27% mężczyzn. 83,06% studentów należało do grupy wiekowej 18–23 lata, a 16,39% liczyło ponad 23 lat. Najwięcej respondentów zamieszkiwało miasta powyżej 200 tys. mieszkańców (33,12%), a następnie miasta do 100 tys. mieszkańców (28,30%) oraz wieś (26,85%). Najmniej liczną grupę stanowili mieszkańcy miast do 200 tys. mieszkańców (11,74%). Wśród ankietowanych dominowali studenci studiów dziennych (68%), będący na studiach inżynierskich (45,82%) oraz studiujący w SGGW (50%).

ZASADY KORZYSTANIA PRZEZ STUDENTÓW Z INTERNETU W TRAKCIE NAUCZANIA ZDALNEGO

Zasadniczą kwestią w trakcie zdalnego nauczania jest dostęp do urządzeń umożliwiających czynny udział w zajęciach, możliwość oddawania prac zaliczeniowych czy zdawania egzaminów. Wśród badanych studentów do pracy zdalnej 72,67% wykorzystuje laptopy, 19,94% – komputery stacjonarne, 6,43% – smartfony, a zaledwie w 0,96% tablety (tab. 2).

Tabela 2.
Urządzenia wykorzystywane przez studentów w trakcie zdalnego nauczania

Zmienne	Częstotliwość	Odsetek [%]
Urządzenia wykorzystywane do pracy zdalnej		
Laptop	452	72,67
Komputer	124	19,94
Smartfon	40	6,43
Tablet	6	0,96
Aktywności podejmowane w Internecie w związku z pracą zdalną uczelni		
Przeglądanie treści zamieszczanych przez wykładowców i zamieszczanie zadań	479	–
Poszukiwanie informacji niezbędnych do przygotowania się do zajęć w przeglądarkach internetowych	465	–
Sprawdzanie poczty	416	–
Przeglądanie informacji dotyczących działalności uczelni	330	–
Czytanie serwisów internetowych	305	–
Czytanie książek i artykułów naukowych	237	–
Przeglądanie baz danych	199	–
Przeglądanie zasobów biblioteki zdalnej	103	–

Miejsce pozyskiwania wiedzy		
Wykłady i ćwiczenia online	559	–
Artykuły udostępnione za darmo	329	–
Fora i grupy dyskusyjne	87	–
Biblioteki online	74	–
Blogi	56	–
Sposób komunikowania się w trakcie zdalnego nauczania		
Facebook	579	93,09
Inny	28	4,50
Whatsapp	9	1,45
e-mail	6	0,96

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Uzyskane wyniki potwierdzają ogólnoświatowe dane dotyczące wykorzystywania z urządzeń przez użytkowników Internetu. W 2020 r. liczba użytkowników Internetu mobilnego wyniosła 4,28 mld, co oznacza, że ponad 90% światowej populacji korzysta z urządzenia mobilnego do łączenia się z Internetem (Statista, 2021). Laptop jest częściej wykorzystywany niż smartfon, co znajduje szczególne uzasadnienie w przypadku zdalnej edukacji. Praca na laptopie (pisanie prac, korzystanie z arkusza kalkulacyjnego, czytanie tekstu na ekranie) jest bowiem zdecydowanie wygodniejsza w porównaniu ze smartfonem. Jak wynika z badań, laptopa w trakcie zdalnej edukacji wykorzystuje 87,8% kobiet i 55,78% mężczyzn, natomiast z komputera częściej korzystają mężczyźni (35%) niż kobiety (5,79%). Najczęściej laptop w trakcie zdalnej edukacji wykorzystują studenci SGGW (77,17%) następnie WSB (73,08%) i UEKat (65,79%). Biorąc pod uwagę poziom studiów, należy stwierdzić, że studenci studiów magisterskich wykorzystują laptop w 80,49%, studenci studiów licencjackich w 78,04%, a studenci studiów inżynierskich w 65,61%.

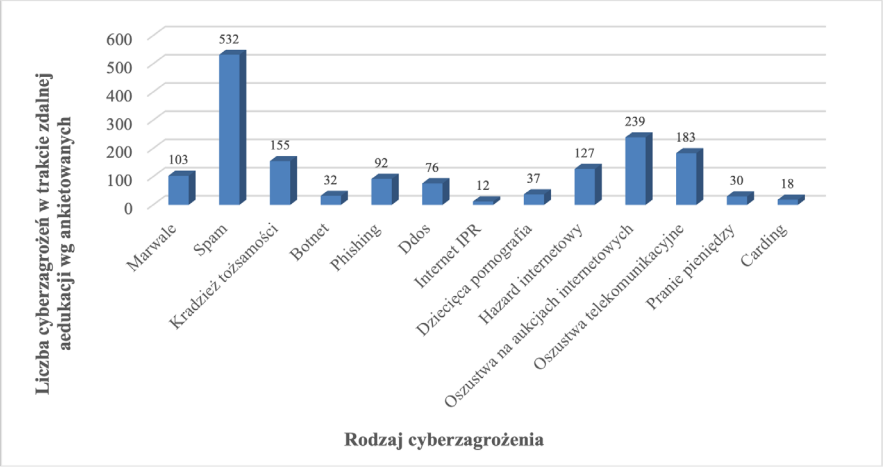
W trakcie zdalnej edukacji studenci podejmowali różne aktywności (tab. 2). Jak można zauważyć, najczęściej korzystali z Internetu do przeglądania zamieszczanych przez wykładowców treści, poszukiwania informacji niezbędnych do przygotowania się do zajęć w przeglądarkach internetowych czy sprawdzania poczty. Z kolei najrzadziej korzystali z zasobów biblioteki zdalnej. Tę formę aktywności przejawiało zaledwie 16,98% studentów studiów zaocznych i 16,55% studentów studiów dziennych. Najczęściej z biblioteki zdalnej korzystali studenci studiów licencjackich – 19,22% następnie studiów magisterskich – 15,85%, a najrzadziej studenci studiów inżynierskich – 14,03%. W przypadku uczelni dominowali studenci WSB – 20,19%, następnie plasowały się osoby studiujące na SGGW – 17,36% i UEKat – 13,04%.

W celu przygotowania się do zajęć korzystali przede wszystkim z treści przekazywanych podczas wykładów i ćwiczeń, zaś w nieco mniejszym zakresie – z udostępnianych bezpłatnie artykułów, forów i grup dyskusyjnych, zasobów biblioteki online, a najrzadziej – z blogów. Analizując formę kształcenia, nie zauważono istotnej różnicy w źródłach poszukiwania informacji i materiałów związanych z poziomem studiowania. 83,92% studentów zaocznych wskazało, że korzystają z wykładów i ćwiczeń online, podczas gdy w przypadku studentów dziennych było to 86,29%. Studenci na poziomie inżynierskim korzystali z wykładów i ćwiczeń online w 84,56%, przyszli licencjaci w 86,67%, a kandydaci na magistrów w 85,37%. Najczęściej z tej formy pozyskiwania wiedzy korzystali studenci SGGW (87,47%), następne UEKat (85,99%) i WSB (87,85%). Poza edukacją w trakcie pracy zdalnej uczelni ważnym aspektem było komunikowanie się studentów między sobą czy z uczelnią. Jak wskazują wyniki badań, najczęstszą formą komunikowania się był Facebook (93,03%), następnie, jak podano, „inna forma" (4,5%), Whatsapp (1,45%) i e-mail (0,96%). Jako inną formę komunikowania się studenci wskazywali fora dyskusyjne. Facebook był najczęściej wskazywany przez studentów licencjackich (94,90%) i inżynierskich (93,33%), nieco niższy odsetek wskazań zanotowano wśród studentów zdobywających wykształcenie na poziomie magisterskim (86,59%). Z Facebooka korzysta 94,78% studentów studiów dziennych i 89,45% – zaocznych. Jak wynika z raportu opublikowanego w 2021 r., Facebook zajmuje drugie miejsce wśród stron najchętniej odwiedzanych przez Polaków. Facebook przyciąga średnio 540,1 mln odwiedzających miesięcznie i jest liderem wśród portali społecznościowych używanych w Polsce (Zawada, Skurzyńska, 2021).

Bezpieczeństwo studentów w sieci internet a zdalne nauczanie

Głównym celem podjętych badań było zidentyfikowanie, z jakimi rodzajami zagrożeń studenci spotkali się w trakcie zdalnej edukacji (rys. 2).

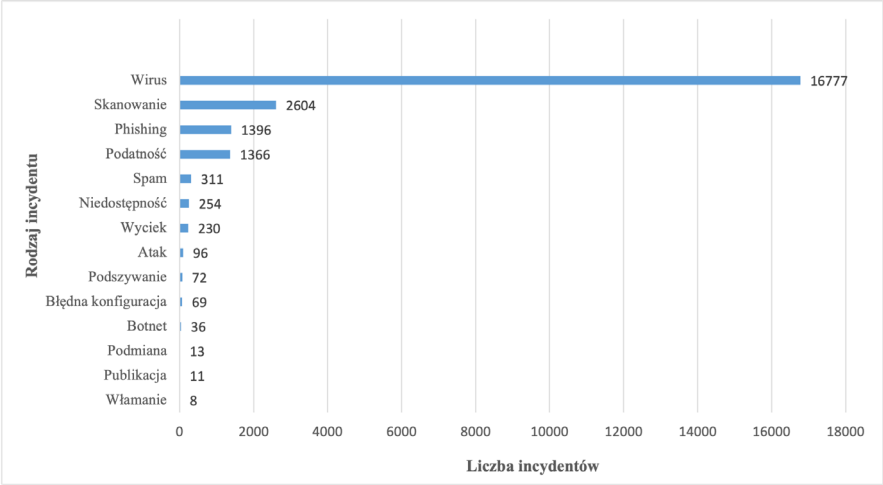
Rysunek 2.
Cyberzagrożenia, z jakimi spotkali się studenci w trakcie zdalnej edukacji



Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Wśród zagrożeń, na które narażeni są najczęściej badani studenci, są spamy, oszustwa na aukcjach internetowych i oszustwa telekomunikacyjne. Spamy jako cyberzagrożenie zostało wskazane przez ponad 85% respondentów, co oznacza, że studenci najczęściej spotykają się z tym rodzajem zagrożenia. Około 38% ankietowanych wskazywało oszustwa na aukcjach internetowych, a ok. 29% na oszustwa telekomunikacyjne. Analizując częstotliwość zetknięcia się ze spamem jako cyberzagrożeniem w ujęciu poziomu studiów, można zauważyć, że 49,75% stanowili studenci studiów zaocznych i aż 83,21% studentów studiów dziennych. Na spam jako cyberzagrożenie wskazało 67,72% studentów studiów inżynierskich, 80,78% studentów studiów licencjackich i 63,41% studentów studiów magisterskich. Porównując ten wskaźnik w różnych uczelniach, można stwierdzić, iż był on najwyższy w SGGW (78,14%), następnie plasowały się UEKat (69,08%) i WSB (62,5%). Studenci najrzadziej spotykają się z Internetem IPR i cardingiem. Wyniki te znajdują częściowe potwierdzenie we wspominanym już opracowaniu (CSIRT GOV, 2021), z którego wyniki zaprezentowano na rys. 3.

Rysunek 3.
Liczba incydentów wśród polskich użytkowników sieci Internet w 2020 r. wg kategorii



Źródło: [CSIRT GOV, 2021].

Jak wynika z rys. 3, spam jest na piątym miejscu wśród najczęściej występujących incydentów. Jednocześnie duża liczba wskazań na spam wśród ankietowanych w przypadku uczelni może być efektem komunikowania się studentów z administracją uczelni (dziekanat) czy wykładowcami (przesyłanie prac dyplomowych), które odbywa się za pomocą skrzynki e-mail.

W związku z przedstawionymi zagrożeniami poproszono studentów o udzielenie odpowiedzi dotyczących oceny ich cyberbezpieczeństwa (tab. 3).

Tabela 3.
Cyberbezpieczeństwo w czasie edukacji zdalnej (N = 622)

Zmienne	Średnia	Odchylenie standardowe
Urządzenia wykorzystywane do pracy zdalnej		
Ocena bezpieczeństwa połączeń w trakcie zajęć online	5,60	1,19
Ocena bezpieczeństwa przeglądanych stron zawierających informacje (wirtualny dziekanat, platforma moodle, classroom)	5,60	1,21
Ocena wiedzy na temat bezpieczeństwa w sieci	4,78	1,42
Ocena własnego bezpieczeństwa w sieci	4,80	1,26

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Uzyskane dane wskazują, że studenci wysoko oceniają bezpieczeństwo połączeń w trakcie zajęć oraz podczas korzystania z innych aktywności na uczelni (średnia 5,6). Nieco niżej oceniają swoją wiedzę na temat cyberbezpieczeństwa (średnia 4,78) oraz własne bezpieczeństwo w sieci (średnia 4,8). Uzyskane wyniki są na poziomie przeciętnym i znajdują potwierdzenie w odpowiedziach respondentów dotyczących częstotliwości zmian haseł. Ponad połowa ankietowanych nie zmienia hasła wcale (25,88%) lub robi to rzadziej niż raz na rok (39,87%) (tab. 4). Zaledwie 4,01% studentów zmienia hasło co miesiąc, a 4,82% raz na trzy miesiące.

Tabela 4.

Działania podejmowane w celu ochrony przed cyberzagrożeniami (N = 622)

Zmienne	Częstotliwość	Odsetek [%]
Częstotliwość zmiany haseł		
Rzadziej niż raz na rok	248	39,87
Raz na rok	102	16,40
Nie zmieniam hasła	161	25,88
Raz na pół roku	56	9,00
Raz na trzy miesiące	30	4,82
Co miesiąc	25	4,01
Oprogramowanie antywirusowe		
Tak	433	69,61
Nie	117	18,81
Nie wiem	72	11,57
Korzystanie z sieci wi-fi uczelni		
Tak	174	27,97
Nie	448	78,46
Organizowanie przez uczelnię szkoleń dotyczących cyberbezpieczeństwa		
Tak	171	27,49
Nie	451	72,50
Zainteresowanie szkoleniami z zakresu cyberbezpieczeństwa organizowanymi przez uczelnię		
Tak	278	44,69
Nie	344	55,31

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Lepiej przedstawia się sytuacja w przypadku oprogramowania antywirusowego. 69,61% respondentów posiada oprogramowanie antywirusowe. Istotnym spostrzeżeniem jest mały odsetek studentów (27,97%) korzystających z udostępnianych przez uczelnię połączeń wi-fi. Niski jest też poziom wiedzy na temat organizowania przez uczelnie szkoleń na temat cyberbezpieczeństwa. 72,50% studentów odpowiedziało, że uczelnie nie organizują szkoleń z zakresu cyberbezpieczeństwa a jednocześnie mniej niż połowa respondentów była zainteresowana tego typu szkoleniami (44,69%).

Wpływ zmiennych demograficznych na zachowania studentów dotyczących cyberbezpieczeństwa

W celu sprawdzenie, czy istnieje zależność pomiędzy zmiennymi demograficznymi a częstotliwością zmiany haseł, przeprowadzono test χ^2 (tab. 5).

Tabela 5.
Zmienne demograficzne a cyberbezpieczeństwo studentów – wyniki testu χ^2

Zmienne	Wartość	df	p
Częstotliwość zmiany haseł			
Płeć	8,93	df = 10	p = 0,53856
Wiek	15,80	df = 10	p = 0,10549
Miejsce zamieszkania	7,18	df = 20	p = 0,99604
Forma kształcenia	15,79	df = 5	p = 0,00746
Poziom studiów	28,39	df = 10	p = 0,00156
Uczelnia	21,39	df = 10	p = 0,01854
Oprogramowanie antywirusowe			
Płeć	26,15	df = 4	p = 0,00003
Wiek	4,06	df = 4	p = 0,39784
Miejsce zamieszkania	5,96	df = 8	p = 0,65209
Forma kształcenia	7,48	df = 2	p = 0,02371
Poziom studiów	3,95	df = 4	p = 0,41222
Uczelnia	3,52	df = 4	p = 0,47448
Zainteresowanie szkoleniami z zakresu cyberbezpieczeństwa organizowanymi przez uczelnię			
Płeć	7,02	df = 2	p = 0,02990
Wiek	7,62	df = 2	p = 0,02215
Miejsce zamieszkania	1,11	df = 4	p = 0,89309
Forma kształcenia	0,76	df = 1	p = 0,38185
Poziom studiów	13,39	df = 2	p = 0,00124
Uczelnia	1,40	df = 2	p = 0,49611

Źródło: opracowanie własne na podstawie przeprowadzonych badań.

Przeprowadzony test pokazuje, że istnieje zależność statystycznie istotna pomiędzy częstotliwością zmiany haseł a formą kształcenia (p = 0,00746) i poziomem studiów (p = 00156) oraz rodzajem uczeni (p = 0,0185). Z analizy danych dotyczących poziomu kształcenia i częstotliwości zmiany haseł wynika, że raz w miesiącu zmienia hasła 7,54% studentów studiów zaocznych i jeszcze

mniej studentów studiów dziennych (2,36%). Natomiast 2,43% studentów studiów magisterskich zmienia hasła raz w miesiącu, podobnie jest przypadku studentów studiów licencjackich (2,75%) i 5,67% studentów studiów inżynierskich. Większy odsetek wskazań w tej ostatniej grupie może wynikać z profilu studiów. Pomiędzy pozostałymi zmiennymi demograficznych brak zależności statystycznie istotnych. Badanie zależności pomiędzy zmiennymi demograficznych i oprogramowaniem antywirusowym pokazuje, że zależność statystycznie istotna występuje tylko w przypadku płci (p = 0,0003) i formy kształcenia (p = 02371) a oprogramowaniem antywirusowym. Aż 73,47% mężczyzn posiada oprogramowanie antywirusowe, podczas gdy odsetek ten dla kobiet wynosi 66,16%. Analizując trzeci z parametrów, jakim jest zainteresowanie szkoleniami z zakresu cybezbezpieczeństwa, można zauważyć, że zależność statystycznie istotna występuje tylko w przypadku płci (p = 02990), wieku (p = 0,2215) i poziomu studiów (p = 0,00124).

Dyskusja i wnioski

Kwestie podjęte w artykule stanowią przedmiot zainteresować wielu badaczy. Jedną z nich jest korzystanie z Facebooka. Z badań I. Miloševiča i in. (2015) wynika, że Facebook może przyczynić się do poprawy komunikacji studentów z rówieśnikami i profesorami, usprawnić i rozszerzyć dyskusję z innymi studentami, umożliwić zamieszczaanie ogłoszeń związanych z wykładami, egzaminami i innymi wydarzeniami na uczelni, a tym samym zapewnić pomoc w nauce. Tym samym może stanowić istotne wsparcie w realizacji zadań, umożliwić poprawę jakości procesu kształcenia i poszerzenie całkowitego zasobu wiedzy. Podobne podejście przedstawili już wcześniej w swoich badaniach Ch. Pimmer i in. (2014) oraz niedawno M.B. Ulla i W. F. Peralles (2021). Wyniki przytaczanych badań wskazują, że Facebook pełni ważną rolę w edukacji zdalnej i jest najczęstszą formą komunikowania się studentów. Zasadniczym aspektem badań były cyberzagrożenia, z którymi zetknęli się studenci. Problematyka cyberzagrożeń na uczelniach podejmowana jest już od dawna, np. przez M. B. McDonald i B. Roberts-Prottman (2010). W badaniach tych 439 studentów college'u zapytano o to, jak często

doświadczyli każdego z licznych zachowań związanych z zastraszaniem, odkąd są na studiach. Wyniki pokazały, że 38% studentów zna kogoś, kto był ofiarą cyberprzemocy, 21,9% ankietowanych było ofiarami cyberprzemocy, a 8,6% użyło cyberprzemocy wobec kogoś innego. Z kolei w artykule P. van Shaika i in. (2017) na podstawie badań ilościowych przeprowadzonych wśród studentów z Wielkiej Brytanii i Stanów Zjednoczonych, dotyczących postrzegania cyberryzyka stwierdzono, że najwyższe ryzyko dostrzegano w przypadku kradzieży tożsamości, keyloggerów, cyberprzemocy i socjotechniki.

Z badań przeprowadzonych przez autorów niniejszego artykułu wynika, że bardzo wielu polskich studentów narażonych było na spam. Zbadania tego zjawiska podjęli się m.in. R. Kaur, S. Singh i H. Kumar (2018), którzy wskazali, że spamerzy sieci społecznościowych stają się coraz sprytniejsi, aby oszukać użytkowników. W praktyce konta zagrożone można wykrywać na dwóch etapach korzystania z nich: przy logowaniu lub przy ich użyciu. Zauważono, że wykrywanie przy logowaniu nie doczekało się jeszcze wielu badań naukowych (przede wszystkim ze względu na problem dostępu do danych). Głównym celem badaczy było wykrywanie użycia. Większość prac koncentrowała się na profilowaniu różnych cech i wykrywaniu nietypowych odchyleń w tych cechach, aby uruchomić funkcje alarmowania o naruszeniu kont. Jak widać, problem spamu jest także szeroko podejmowany. Ważnym problemem jest kwestia ochrony przed cyberzagrożeniami. Do podobnych wniosków co autorzy artykułu doszli E. Rotas i M. Cahapay (2021). Wyniki przeprowadzonych przez nich badań ujawniły, że studenci mają pewną wiedzę na temat możliwych zagrożeń i czasami przejawiają zachowania ochronne w nauczaniu zdalnym. Jednocześnie uzyskane wyniki badań wskazują na praktyczną potrzebę zwiększenia bezpieczeństwa cybernetycznego studentów. Badanie nie wykazało również istotnego związku pomiędzy wiedzą o zagrożeniach a zachowaniami ochronnymi studentów.

Z przeprowadzonych badań wynikają następujące wnioski:

- w trakcie zdalnej edukacji podejmowana przez studentów aktywność w sieci dotyczy przede wszystkim treści prowadzonych wykładów i ćwiczeń oraz poszukiwania materiałów i informacji niezbędnych do przygotowywania się do zajęć. Pomimo że uczelnie posiadają zdalne

biblioteki, to studenci nie korzystają z nich, często wybierając inne formy pozyskiwania informacji;
- dominującym sposobem komunikowania się wśród studentów jest Facebook, inne formy komunikacji mają znaczenie marginalne;
- głównymi cyberzagrożeniami dotykającymi studentów są spam, oszustwa na aukcjach internetowych i oszustwa telekomunikacyjne. Różne mogą być powody dużej liczebności wymienionych zagrożeń, jednym z nich może być dokonywanie zakupów przez studentów na aukcjach internetowych, w trakcie lockdownu związanego z pandemią COVID-19, z kolei na znaczną liczbę wskazań dotyczących oszustw telekomunikacyjnych mogą mieć wpływ metody i kanały komunikacji pomiędzy administracją uczelni a studentami;
- studenci posiadają przeciętny poziom wiedzy o cyberzagrożeniach, w większym zakresie dbając o bezpieczeństwo w sieci poprzez wykorzystywanie oprogramowania antywirusowego niż zmianę haseł. Jednocześnie przedstawiona w badaniu tendencja panująca wśród studentów może zostać uogólniona do znacznej części społeczeństwa
- studenci wskazują na brak szkoleń z zakresu cyberbezpieczeństwa organizowanych przez uczelnie, jednocześnie nie wykazują bardzo dużego zainteresowania tą formą pogłębiania wiedzy o bezpieczeństwie w sieci;
- przeprowadzona analiza korelacji pomiędzy przyjętymi zmiennymi a częstotliwością zmiany haseł wykazała zależność istotną statystycznie w przypadku formy kształcenia i poziomu studiów. Z kolei uwzględniając zmienne demograficzne i wykorzystywane oprogramowanie, można zauważyć, iż zależność statystycznie istota występuje tylko w przypadku płci studentów i formy kształcenia, zaś w przypadku pozostałych zmiennych jej brak. Zainteresowanie szkoleniami na uczelni z zakresu cyberbezpieczeństwa, jest statystycznie istotne w przypadku płci, wieku i poziomu studiów.

Reasumując, celowe wydaje się podjęcie kolejnych badań wskazujących, jakiego typu działania należałoby przedsięwziąć, aby studenci dążyli do poprawy swojego bezpieczeństwa cyberprzestrzeni.

References

Chen, Y.-P. (2011). *Do the Chi-Square Test and Fisher's Exact Test Agree in Determining Extreme for 2×2 Tables?* „The American Statistician", No. 64, s. 239–245. DOI: https://doi.org/10.1198/tas.2011.10115.

CSIRT GOV (2021). *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku*, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/974,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2020-roku.html (dostęp: 13.02.2022).

Gov.pl (2022). *Rodzaje cyberzagrożeń – zagrożenia techniczne*, https://www.gov.pl/web/baza-wiedzy/zagr-techniczne (dostęp: 12.02.2022).

EC (2019). *Digital Education at School in Europe*. Eurydice Report, https://eacea.ec.europa.eu/national-policies/eurydice/content/digital-education-school-europe_en (dostęp: 11.02.2022).

Fouad, N.S. (2021). *Securing higher education against cyberthreats: from an institutional risk to a national policy challenge*. „Journal of Cyber Policy", No. 6(2), s. 137–154. DOI: https://doi.org/10.1080/23738871.2021.1973526.

Jaroszewska, A.I. (2017). *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*. „Kortowski Przegląd Prawniczy. Monografie", http://www.uwm.edu.pl/kpp/files/numery_kpp/kpp_monografie_studium.pdf (dostęp: 12.02.2022).

Kaur, R., Singh, S., Kumar, H. (2018). *Rise of spam and compromised accounts in online social networks: A state-of-the-art review of different combating approaches*. „Journal of Network and Computer Applications", No. 112, s. 53–88. DOI: https://doi.org/10.1016/j.jnca.2018.03.015.

Leigh, G., Templet, T., Watson, C. (2021). *Feelings on remote education in the era of coronavirus pandemic, a pilot study*. „Teaching and Learning in Nursing", No. 16 (4), s. 332–337. DOI: https://doi.org/10.1016/j.teln.2021.07.001.

MacDonald, Ch.D., Roberts-Pittman, B. (2010). *Cyberbullying among college students: prevalence and demographic differences*. „Procedia – Social and Behavioral Sciences", No. 9, s. 2003–2009. DOI: https://doi.org/10.1016/j.sbspro.2010.12.436.

Milošević, I. i in. (2015). *Facebook as virtual classroom – Social networking in learning and teaching among Serbian students*. „Telematics and Informatics", No. 32(4), s. 576–585. DOI: https://doi.org/10.1016/j.tele.2015.02.003.

Mukuka, A. i in. (2021). *Students' experiences with remote learning during the COVID-19 school closure: implications for mathematics education* „Heliyon", No. 7(7). DOI: https://doi.org/10.1016/j.heliyon.2021.e07523.

Pimmer, Ch. i in. (2014). *Informal mobile learning in nurse education and practice in remote areas – A case study from rural South Africa*. „Nurse Education Today", No. 34(11), s. 1398–1404. DOI: https://doi.org/10.1016/j.nedt.2014.03.013.

Plebańska, M., Szyller, A., Sieńczewska, M. (2020). *Edukacja zdalna w czasach COVID-19. Raport z badania*, Wydział Pedagogiczny UW, https://files.librus.pl/articles/00pic/20/07/09/librus/a_nauczanie_zdalne_oczami_nauczycieli_i_uczniow_RAPORT.pdf (dostęp: 11.02.2022).

Ray, K. (2020). *What is remote learning?*, https://www.techlearning.com/how-to/what-is-remote-learning (dostęp: 11.02.2022).

Rotas, E., Cahapay, M. (2021). *Does threat knowledge influence protective behaviors of students in the context of cyber security in remote learning amid COVID-19 crisis?* „Journal of Pedagogical Sociology and Psychology", No. 3 (1), s. 45–53. DOI: https://doi.org/10.33902/JPSP.2021167595.

Statista (2021). *Mobile internet connectivity worldwide in 2020 (in millions of people)*, https://www.statista.com/statistics/1258847/mobile-internet-connectivity-worldwide/ (dostęp: 15.02.2022).

Stealtlabs (2021). *Cyberattacks Increase 50% in 2021, Peaking All-time High of 925 Weekly Attacks per Organization!*, https://www.stealthlabs.com/news/cyberattacks-increase-50-in-2021-peaking-all-time-high-of-925-weekly-attacks-per-organization/ (dostęp: 15.02.2022).

Such-Pyrgiel, M., Gołębiowska, A., Prokopowicz, D. (2022). The Impact of the COVID-19 Pandemic on the Growing Importance of Cybersecurity of Data Transfer on the Internet. Polish Political Science Yearbook, 51(issue number), pages 1-15. https://doi.org/10.15804/ppsy202224.

Sushruth, V., Rahul Reddy, K., Chandavarkar, R.B. (2021). *Social Engineering Attacks During the COVID-19 Pandemic*. „SN Computer Science", No. 2, s. 78. DOI: https://doi.org/10.1007/s42979-020-00443-1.

Škiljič, A. (2020). *Cybersecurity and remote working: Croatia's (non-)response to increased cyber threats*. „International Cybersecurity Law Review", No. 1, s. 51–61. DOI: https://doi.org/10.1365/s43439-020-00014-3.

Ulla, M.B., Perales, W.F. (2021). *Facebook as an integrated online learning support application during the COVID-19 pandemic: Thai university students' experiences and perspectives*. „Heliyon", No. 7(11). DOI: https://doi.org/10.1016/j.heliyon.2021.e08317.

van Schaik P. i in. (2017). *Risk perceptions of cyber-security and precautionary behaviour*. „Computers in Human Behavior", No. 75, s. 547–559. DOI: https://doi.org/10.1016/j.chb.2017.05.038.

Wasilewski, J. (2016). *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*. „Przegląd Bezpieczeństwa Wewnętrznego" , No. 8, s. 149–173.

Yan, Z. i in. (2018). *Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?* „Computers in Human Behavior", No. 84, s. 375–382. DOI: https://doi.org/10.1016/j.chb.2018.02.019.

Zawada, K., Skurzyńska, W. (2021). *Uzależnienie od Facebooka a satysfakcja ze statusu związku*, No. 1 (46), s. 111–122, „Journal of Modern Science". DOI: 10.13166/JMS/133595.