KATEDRA INFORMATOLOGII i BIBLIOLOGII
Uniwersytet Łódzki

ACTA UNIVERSITATIS LODZIENSIS
FOLIA LIBRORUM 1 (34), 2022
ISSN 0860-7435

COPE
Member since 2021
JM15487

Anna Sikorska
Katedra Informatologii i Bibliologii
Uniwersytet Łódzki
e-mail: anna.sikorska481@gmail.com

Ocena wiedzy, umiejętności i postaw studentów Wydziału Filologicznego Uniwersytetu Łódzkiego w zakresie bezpiecznego korzystania z Internetu

DOI: http://doi.org/10.18778/0860-7435.34.05

Abstrakt: W artykule podjęto rozważania nad kompetencjami studentów Wydziału Filologicznego Uniwersytetu Łódzkiego w zakresie bezpiecznego korzystania z Internetu. Celem badań było poznanie i ocena wiedzy, umiejętności i postaw studentów w obrębie niezagrożonej konsumpcji treści zamieszczanych i spotykanych w sieci każdego dnia, a także innych aspektów związanych z wyzwaniami cyberprzestrzeni. Zwrócono również uwagę na potencjał kompetencji informacyjnych i cyfrowych, których nie powinno brakować szczególnie (choć nie tylko) osobom studiującym. Kluczowe znaczenie mają zatem: ustawiczny rozwój tych umiejętności, pozyskiwanie wiedzy i świadomość potencjalnych zagrożeń.

Realizacji wyznaczonych celów posłużyły następujące metody badań: metoda krytycznej analizy literatury przedmiotu, metoda bibliograficzna oraz metoda sondażu diagnostycznego. Niezbędne dla zrozumienia istoty problemu i zagłębienia się w tematykę bezpieczeństwa w sieci było przywołanie definicji „cyberprzestrzeni", „cyberbezpieczeństwa", „kompetencji cyfrowych" i „kompetencji informacyjnych" oraz scharakteryzowanie wybranych zagrożeń bezpieczeństwa w sieci, czego dokonano dzięki przeglądowi literatury.

W części o charakterze metodologicznym wskazano przedmiot badań, cele i problemy badawcze, określono zasady doboru próby oraz opisano metody, techniki i narzędzia badawcze. Część badawcza stanowi analizę wyników

Received: 16.05.2022; verified: 23.05.2022. Accepted: 29.05.2022.

badania ankietowego przeprowadzonego na studentach Wydziału Filologicznego Uniwersytetu Łódzkiego.
Badanie przeprowadzone na reprezentatywnej grupie studentów pozwoliło ustalić, jakich trudności związanych z korzystaniem z Internetu studenci Wydziału Filologicznego Uniwersytetu Łódzkiego najczęściej doświadczają, jakich zagrożeń w sieci obawiają się najbardziej, w jaki sposób studenci chronią swoje zasoby, prywatność i wizerunek w Internecie, z jakich źródeł czerpią wiedzę o cyberbezpieczeństwie i jak oceniają swoje kompetencje w tym zakresie. Z analizy można odczytać, że większość badanych ma podstawową wiedzę niezbędną do odpowiedzialnego korzystania z zasobów Internetu oraz umiejętności korzystania z narzędzi umożliwiających lepszą ochronę w cyfrowej przestrzeni. Zaleca się jednak prowadzenie dalszych badań w tym kierunku.

Słowa kluczowe: kompetencje informacyjne, kompetencje cyfrowe, cyberbezpieczeństwo, zagrożenia bezpieczeństwa w Internecie

Wstęp

Rozważania na temat istoty cyberprzestrzeni i wyzwań, jakie ze sobą niesie, podejmowane były jeszcze przed jej powstaniem jako takim. Choć swój rodowód zawdzięcza literaturze science fiction, dyskusje na jej temat przeniosły się na grunt środowiska naukowego także w naukach o informacji. Szczególną rolę przestrzeni wirtualnej podkreśla się zwłaszcza w kontekście Internetu z całym jego wachlarzem możliwości i zagrożeń. Zapobieganie tym drugim jest właśnie obiektem zainteresowania autorki tego artykułu.

Podstawowym celem badań było poznanie i ocena kompetencji studentów Wydziału Filologicznego Uniwersytetu Łódzkiego w kwestii bezpieczeństwa w sieci. Ocena wiedzy, umiejętności i postaw studentów oraz podkreślenie znaczenia kompetencji informacyjnych i cyfrowych we współczesnym świecie ma za zadanie zachęcić studiujących (i nie tylko) użytkowników Internetu do ustawicznego rozwoju w tym zakresie i do odpowiedzialnej konsumpcji treści online.

Przeprowadzone badanie miało przede wszystkim pomóc w ustaleniu kilku kwestii:

1. W jakim stopniu studenci są zainteresowani kwestiami bezpieczeństwa w Internecie?
2. Jak studenci chronią siebie, swój wizerunek i swoje zasoby w sieci?
3. Skąd osoby studiujące czerpią wiedzę na temat cyberbezpieczeństwa?
4. Jak wygląda samoocena studentów w zakresie bezpieczeństwa w środowisku cyfrowym?

Podstawowe terminy

Na początku artykułu konieczne jest usystematyzowanie metodą analizy krytycznej literatury najważniejszych pojęć związanych z przeprowadzonymi badaniami. We współczesnej literaturze pojawiły się pojęcia: „cyberprzestrzeń" i „cyberbezpieczeństwo", a także „kompetencje cyfrowe", „kompetencje informacyjne".

Mimo że określenie „cyberprzestrzeń" funkcjonuje w literaturze fachowej, istnieją realne wątpliwości co do prawidłowości tego terminu, który nie posiada naukowego ani technicznego rodowodu (Lakomy 2015, s. 73). Po raz pierwszy pojęcie „cyberprzestrzeń" pojawiło się w latach 80. XX wieku w dziełach amerykańskiego pisarza science fiction Wiliama Gibsona, a jego wizualnych interpretacji dokonali twórcy filmowi, np. w trylogii Matrix (Wasilewski 2013, s. 226; Lakomy 2015, s. 73). Wkrótce potem podjęto naukowe rozważania nad istotą cyberprzestrzeni. Wśród jej cech Maciejczuk, Wnorowski i Olchanowski (2019, s. 15–16) wymienili wirtualny charakter, uniezależniony od przestrzeni geograficznej, otwartość na nowych użytkowników oraz jej istnienie dzięki fizycznym gwarantom, komputerom czy infrastrukturze telekomunikacyjnej, i możliwości jej wizualizacji. Ci sami badacze proponują także zestaw cech, który eksponuje wielowymiarowość cyberprzestrzeni (Tamże, s. 16).

Jak wskazuje Janusz Wasilewski, najpowszechniej znaną i cytowaną jest definicja cyberprzestrzeni zaproponowana przez Departament Obrony USA:

> Globalna domena środowiska informacyjnego składająca się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery (cyt. za Wasilewski 2013, s. 277).

Wyjaśnienie to podkreśla, że cyberprzestrzeń nie odnosi się jedynie do sieci internetowej, co współcześnie funkcjonuje na gruncie języka potocznego, ale i nierzadko w dyskursie humanistycznym (Węgrzyn-Odzioba 2018, s. 79), ale jest pojęciem szerszym, co sygnalizuje także Miron Lakomy (2015, s. 71). O cyberprzestrzeni nie tylko jako Internecie przeczytamy również u Kasprzaka (2015, s. 33–34), który wyróżnia trzy jej płaszczyzny, nachodzące na siebie i wzajemnie się przenikające: Internet, telefonię i inne urządzenia cyfrowe.

Powyżej przedstawiona definicja Departamentu Obrony pomija jednak istotny, w pierwotnym rozumieniu, element społeczny (Wasilewski 2013, s. 228), który proponują inni autorzy (Marczyk 2018, s. 61–62). Analizując zaproponowane koncepcje i zastosowania cyberprzestrzeni, można zaobserwować narastające wokół niej zarówno ogromne możliwości, jak i wynikające z niej ograniczenia czy zagrożenia. W związku z tym, zwłaszcza w ostatnim czasie, szczególny nacisk kładzie się na kwestie zapewnienia bezpieczeństwa

w wirtualnej przestrzeni. Cyberbezpieczeństwo, bo o nim tu mowa, w ogólnym rozumieniu jest zbiorem wszystkich zagadnień powiązanych z zapewnianiem ochrony w cyberprzestrzeni. W węższym postrzeganiu jako bezpieczeństwa sieci i systemów informatycznych jest to:

> (…) odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne (cyt. za Kaczmarczyk, Szczepański & Dąbrowska 2019, s. 203).

Zainteresowanie badaczy technicznych skupia się szczególnie na zapobieganiu cyberatakom lub minimalizacji ich negatywnych skutków (Kasprzak i in. 2019, s. 41), pomija zaś poczucie bezpieczeństwa, anonimowości i ochronę prywatności w Internecie czy też swobodę czerpania informacji z bogactwa jej zasobów (Tamże, s. 204).

Przewidywane niebezpieczeństwa, których potencjalnymi ofiarami są praktycznie wszyscy użytkownicy Internetu, mogą zostać zminimalizowane dzięki rozwijaniu katalogu umiejętności, których nie powinno brakować, przynajmniej w podstawowym zakresie, żadnej osobie poruszającej się w sieciowych zasobach. To tzw. kompetencje kluczowe, które scharakteryzowała Organizacja Współpracy i Rozwoju Gospodarczego (OECD) (Matusz 2007, s. 50–51; Stachowiak 2009, s. 113). W zbiorze tych kompetencji znalazła się umiejętność posługiwania się nowoczesną technologią informacyjną. Warto zatem pochylić się nad pojęciem „kompetencji cyfrowych". W rozumieniu Agnieszki Ogonowskiej kompetencje cyfrowe:

> (…) obejmują umiejętności niezbędne do aktywnego korzystania z technologii cyfrowych, swobodnego i krytycznego posługiwania się nimi we wszystkich kluczowych sferach życia, tzn. w pracy, czasie wolnym, edukacji i kształceniu, komunikacji oraz korzystaniu z szerokiej gamy e-usług oferowanych przez różne organizacje i instytucje (2016, s. 14).

Zdawać by się mogło, że wszystkie te zdolności posiadają tak zwani „cyfrowi tubylcy", który to przydomek MarcPrensky nadał pokoleniu młodych ludzi, narodzonych w czasach dynamicznego rozwoju technologii (Prensky 2001, s. 1; Jabłońska 2018, s. 13–14). Jak podkreślają badacze, swobodne korzystanie z dóbr technologicznych nie daje jednak gwarancji posiadania kompetencji cyfrowych (Jabłońska 2018, s. 14–16). Katalogi kompetencji cyfrowych, które szeroko przeanalizowała Paulina Motylińska (2020b, s. 204–213) mogą być dobrym drogowskazem uzmysławiającym ich niezwykłą rolę w XXI wieku.

Na uwagę zasługuje także pojęcie „kompetencji informacyjnych", które w dziedzinowej nomenklaturze funkcjonuje często także pod nazwą „alfabetyzacji informacyjnej" (ang. *Information literacy*). Najczęściej w literaturze przedmiotu

cytuje się definicję posiadacza kompetencji informacyjnych, sformułowaną przez Stowarzyszenie Bibliotek Amerykańskich (*American Library Association*):

> Osoba posiadająca kompetencje informacyjne musi być w stanie określić własne potrzeby informacyjne, zlokalizować potrzebną informację, ocenić ją i efektywnie wykorzystać. To osoby, które nauczyły się jak się uczyć (Lau 2011, str. 69).

We współczesnej literaturze wielu badaczy dokonuje też prób scharakteryzowania zagrożeń związanych z użytkowaniem sieci (Kaczmarczyk, Szczepański & Dąbrowska 2019, s. 204–205; Masrek et al. 2020, p. 1205; *Information Security Threats*… 2019; Motylińska 2020a, s. 16; Babik 2012, s. 52; Musiał 2020, s. 182; Kvardova 2021). Powszechną typologię zagrożeń, którą rozszerzają nowsze publikacje badaczy nauki o informacji i pokrewnych dyscyplin, sformułował Władysław Furmanek, który wyróżnił sześć ogólnych grup zagrożeń:

- zagrożenia o charakterze psychologicznym (przymus bycia w sieci, uzależnienie od Internetu, FOMO, nomofobia, cyberchondria, cyberlęk, alienacja, dostęp do patalogicznych grup kulturowych),
- zagrożenia o charakterze technicznym (kradzieże danych i informacji, złośliwe oprogramowania różnego typu),
- zagrożenia o charakterze medycznym (zaburzenia fizyczne),
- zagrożenia o charakterze prawnym (naruszenia praw autorskich),
- zagrożenia o charakterze społecznym (wykluczenie cyfrowe, polaryzacja społeczna wywołana zjawiskiem baniek filtrujących i algorytmicznej personalizacji, napływ niechcianych i nieodpowiednich treści,
- zagrożenia informacyjne wynikające z rozwoju współczesności (nadprodukcja informacji, brak kompetencji cyfrowych i informacyjnych (Furmanek 2014,s. 23-24).

Zagrożenia te i wynikające z nich konsekwencje były przyczynkiem do przeprowadzenia badań na studentach, od których często wymaga się świadomości tych zagrożeń i dobrego funkcjonowania w cyfrowym środowisku.

Założenia metodologiczne i organizacja badań

Przedmiotem badań, tak jak jednoznacznie wskazuje tytuł artykułu, są kompetencje – wiedza, umiejętności i postawy – studentów Wydziału Filologicznego Uniwersytetu Łódzkiego w zakresie bezpiecznego korzystania z Internetu – jednego z elementów cyberprzestrzeni. Współcześnie Internet jest podstawowym źródłem pozyskiwania różnego rodzaju informacji, a także wirtualnym miejscem spotkań i narzędziem rozrywki, dlatego właśnie użytkownicy sieci są potencjalnym celem ataku, a nieuważność internautów często prowadzi

do katastrofalnych skutków. Jednocześnie powstają nowe rozwiązania legislacyjne dotyczące bezpieczeństwa w sieci. W związku z tak dużym oddziaływaniem Internetu na różne aspekty życia człowieka przeprowadzenie tego typu badań wydaje się słuszne i uzasadnione.

Podstawowym celem badawczym niniejszego artykułu było przeanalizowanie wiedzy i umiejętności studentów w zakresie bezpiecznego poruszania się w Internecie oraz poznanie postaw studentów wobec wybranych zagrożeń, z którymi ma szansę zetknąć się każdy internauta. Dodatkowym celem praktycznym badania było pokazanie potencjału kompetencji informacyjnych i cyfrowych jako kompetencji kluczowych.

Próba poddania ocenie kompetencji studentów Wydziału Filologicznego Uniwersytetu Łódzkiego w zakresie bezpiecznego użytkowania sieci wymagała sformułowania szczegółowych kwestii. Autorkę interesowało znalezienie odpowiedzi na pytania: jakich trudności studenci doświadczają w Internecie najczęściej? Jakich zagrożeń związanych z korzystaniem z Internetu studenci obawiają się najbardziej? W jakim stopniu studenci interesują się kwestiami bezpieczeństwa w Internecie? Z jakich zabezpieczeń korzystają studenci w celu zwiększenia swojego bezpieczeństwa w sieci? Jak studenci chronią swoje zasoby, prywatność i wizerunek w Internecie? Z jakich źródeł studenci czerpią wiedzę na temat bezpieczeństwa Internecie? Jak studenci oceniają swoje kompetencje w zakresie bezpiecznego korzystania z Internetu?

Badanie objęło zarówno studentów, jak i doktorantów oraz uczestników szkoły doktorskiej Wydziału Filologicznego i było skierowane do osób powyżej 18 roku życia. Zdecydowano się na przeprowadzenie badań w tej grupie ze względu na brak podobnych dostępnych danych, których opracowanie mogłoby pomóc w zaobserwowaniu stanu cyberbezpieczeństwa i zwiększeniu jakości kształcenia na Wydziale Filologicznym Uniwersytetu Łódzkiego. Z tego też względu wyniki badań udostępniono Wydziałowemu Koordynatorowi ds. e-learningu.

Badanie zaplanowano na koniec kwietnia i początek maja 2021 roku, a przeprowadzono je za pomocą wcześniej przygotowanego elektronicznego kwestionariusza ankietowego. W związku z pandemią koronawirusa i warunkami nauki zdalnej na Uniwersytecie Łódzkim studenci wypełniali ankietę internetowo na platformie Google Forms.

Na potrzeby badań zdecydowano się na kwestionariusz ankietowy rozprowadzany drogą elektroniczną. Składał się on z siedmiu pytań właściwych poprzedzonych czterema pytaniami o charakterze metryczki [Załącznik]. Metryczka zawierała trzy pytania zamknięte, dotyczące płci, wieku i stopnia studiów, oraz jedno pytanie otwarte, związane ze studiowanym przez ankietowanych kierunkiem. Pytania właściwe zaś odnosiły się do wiedzy, umiejętności

i postaw respondentów z zakresu bezpieczeństwa w Internecie. Wśród nich znajdują się pytania zamknięte (pytania 1, 2, 3 i 7) oraz półotwarte (pytania 4, 5 i 6). W przypadku pytań o ocenę stopnia doświadczenia, obaw i kompetencji oraz skalę zainteresowania zagadnieniem (pytania zamknięte) zastosowano siedmiostopniową skalę Likerta, która sprawdza się lepiej przy ocenie postaw, opinii i zjawisk. Miała ona pomóc w zróżnicowaniu odpowiedzi ankietowanych i dać możliwość symetryczności wartościowania odpowiedzi oraz wyrażenia neutralności dzięki liczbie środkowej. Pytania w kwestionariuszu sformułowano na podstawie postawionych problemów badawczych.

Trafność i zrozumiałość pytań zweryfikowano dzięki przeprowadzonemu 27 kwietnia 2021 roku badaniu pilotażowemu. Piętnastoosobowa grupa respondentów, którzy zgłosili się do przetestowania formularza za pośrednictwem portalu Facebook, pozytywnie wypowiedziała się na temat struktury, kolejności pytań, długości ankiety i zastosowanej skali, co pozwoliło na szybkie przejście do kolejnego etapu organizacji badań.

Według danych uzyskanych 12 kwietnia 2021 roku w korespondencji mailowej od kierownika Biura ds. Obsługi Studenta liczba studentów Wydziału Filologicznego Uniwersytetu Łódzkiego (studenci 1 i 2 stopnia, doktoranci oraz uczestnicy szkoły doktorskiej) wynosiła 3681. Wyliczeniu próby reprezentatywnej posłużył internetowy kalkulator doboru próby, dostępny na portalu Naukowiec.org. Z reguły poziom ufności ustala się na poziomie 95%, wielkość frakcji – 0.5, a błąd maksymalny – 5%, co wymagałoby odpowiedzi w ankiecie uzyskanych od 348 osób. Ze względu jednak na niewystarczającą liczbę odpowiedzi ankietowych zdecydowano się na zwiększenie błędu maksymalnego do 8%. Przy takich założeniach w badaniu powinny wziąć udział co najmniej 144 osoby.

Aby pozyskać respondentów, kwestionariusz ankiety rozsyłano studentom w prywatnych wiadomościach oraz udostępniano na portalu Facebook w grupach tematycznych związanych z Uniwersytetem Łódzkim: *Dzieje się – Uniwersytet Łódzki*, *Perspektywiczny Filologiczny* oraz *Wydział Filologiczny UŁ (Pierwszaki 2018) Uniwersytetu Łódzkiego*. W badaniu przeprowadzonym na przełomie kwietnia i maja 2021 roku uzyskano 165 odpowiedzi, a 4 z nich odrzucono ze względu na zaobserwowane błędy w części z metryczką. Analiza wyników badań przeprowadzona została zatem na podstawie 161 ankiet.

Analiza i interpretacja wyników badań

Poniżej przeanalizowano i zaprezentowano wyniki badań, dotyczących kompetencji w zakresie bezpieczeństwa w Internecie, przeprowadzonych na reprezentacyjnej grupie studentów Wydziału Filologicznego Uniwersytetu

Łódzkiego. Wyniki przedstawiono na wykresach opatrzonych opisem i legendą – przy pytaniach półotwartych i zamkniętych – oraz za pomocą tabeli – przy pytaniu o charakterze otwartym.

Na początku warto przeanalizować cechy społeczno-demograficzne respondentów. Pierwsze pytanie w metryczce dotyczyło płci ankietowanych studentów. W grupie 161 respondentów 80%, czyli 128 osób, stanowiły kobiety, zaś tylko 20% ankietowanych, czyli 33 osoby, to przedstawiciele płci męskiej. Podziału dokonano również według wieku. Największą grupę respondentów stanowili studenci w wieku 22–23 lat (43%), najmniej zaś odpowiedziało 18- i 19-latków oraz osób powyżej 26 roku życia (po 3%). Dość liczną grupę stanowili też studenci w wieku 20–21 lat (35%), odpowiedź 24–25 lat zaznaczyło zaś 16% ankietowanych.

Badanych poproszono również o określenie stopnia studiów. Ponad połowa ankietowanych (68%) to studenci studiów licencjackich. Studenci drugiego stopnia również stanowili stosunkowo dużą grupę (30%). Nieliczni ankietowani (2%) to doktoranci i uczestnicy szkoły doktorskiej.

Z przeprowadzonej analizy wynika, że kwestionariusz ankiety wypełnili przedstawiciele 28 kierunków studiów (w tym 17 studiów licencjackich, 8 studiów magisterskich i 2 studiów doktoranckich), na których kształcenie się na Wydziale Filologicznym Uniwersytetu Łódzkiego było możliwe w roku akademickim 2020/2021. Najwięcej odpowiedzi uzyskano od studentów Informacji w środowisku cyfrowym (22%), Informatologii z językiem angielskim (14%) oraz 1 stopnia Filologii angielskiej (11%). Najmniejszą grupę respondentów stanowili zaś studenci 2 stopnia Dziennikarstwa i komunikacji społecznej (1%), 1 stopnia Dziennikarstwa międzynarodowego (1%), 1 stopnia Filologii rosyjskiej (1%), 2 stopnia Lingwistyki w komunikacji specjalistycznej (1%), 1 stopnia Filmoznawstwa i wiedzy o mediach audiowizualnych (1%), 1 stopnia Filologii germańskiej (1%), 2 i 3 stopnia Filologii polskiej (1% i 1%), 2 stopnia Filologii romańskiej (1%), 3 stopnia Językoznawstwa (1%), 2 stopnia Logopedii (1%), 1 stopnia Produkcji teatralnej (1%) oraz Studiów doktoranckich języka, literatury i kultury (1%).

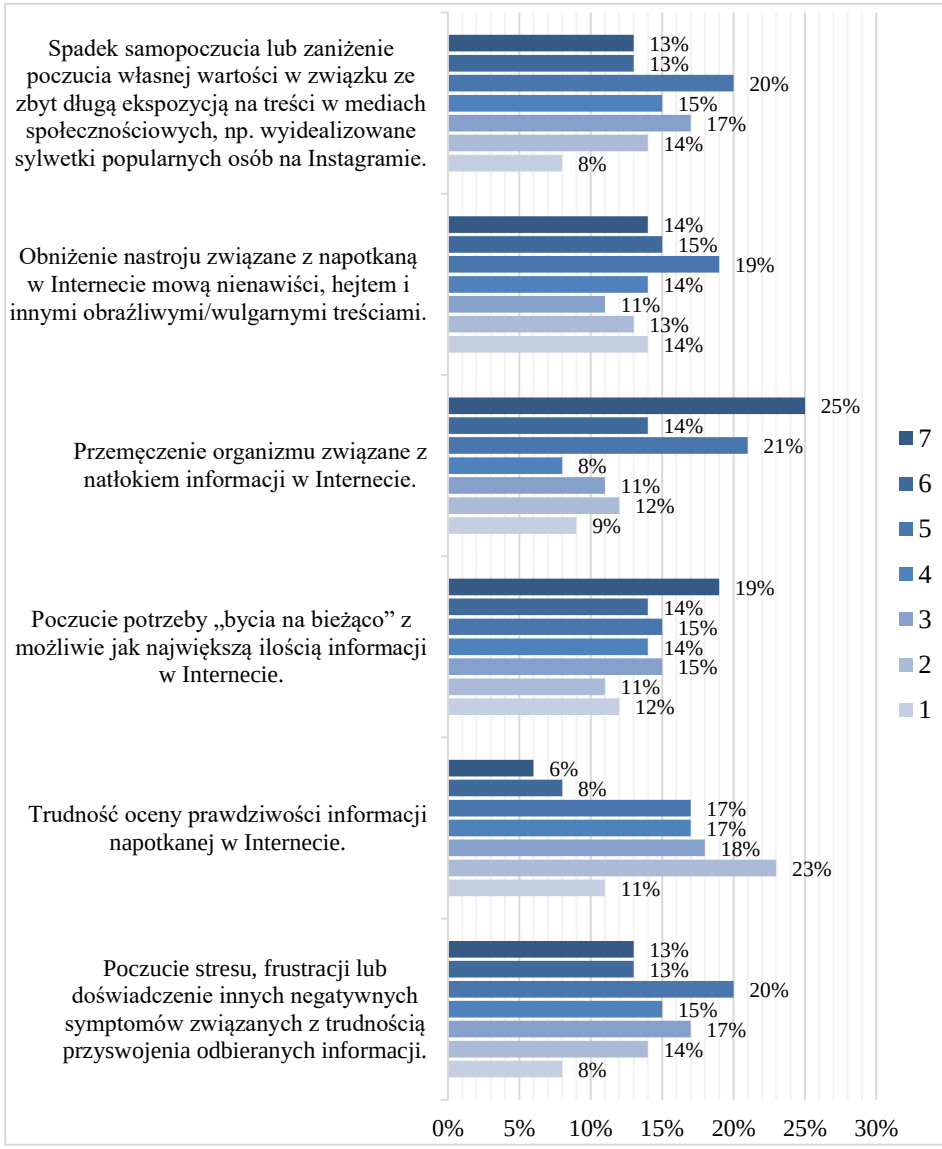
Dalsza część analizy to pytania właściwe, dotyczące zagadnień bezpieczeństwa w sieci: trudności, których studenci doświadczają w Internecie, obaw studentów przed zagrożeniami występującymi w cyfrowym środowisku, ich zainteresowania cyberbezpieczeństwem, zabezpieczenia przed potencjalnymi zagrożeniami, z jakich respondenci korzystają, sposobów ochrony zasobów, prywatności i wizerunku w Internecie, źródeł, z jakich ankietowani czerpią wiedzę na temat cyberbezpieczeństwa. Studentów poproszono również o samoocenę kluczowych kompetencji związanych z ochroną w sieci.

Stopień niedogodności związanych z korzystaniem z Internetu, których doświadczyli ankietowani w ciągu 12 miesięcy poprzedzających badanie, oceniany był w siedmiostopniowej skali Likerta, gdzie 1 oznaczało brak takich doświadczeń, a 7 – nieustanne doświadczanie danej trudności. Studenci mieli szeroki katalog doświadczeń do wyboru. Wśród najczęściej doznawanych trudności znalazło się przemęczenie organizmu związane z natłokiem informacji, z którym zmagali się badani w związku z korzystaniem z Internetu – aż 25% respondentów uznało, że trudność ta dotykała ich bez przerwy, a 35% opowiedziało się za bardzo częstym lub częstym odczuwaniem informacyjnego przeładowania. Wysoko w tym zestawieniu znalazło się również poczucie „bycia na bieżąco" z możliwie jak największą ilością informacji – 19% ankietowanych doświadczało tego nieustannie.

Dla studentów nie było natomiast aż tak kłopotliwe ocenianie wiarygodności informacji – zaledwie 6% respondentów nagminnie doznawało trudności z oceną prawdziwości treści przeglądanych w sieci. Spory odsetek ankietowanych był natomiast zaznajomiony z negatywnymi symptomami związanymi z trudnością przyswojenia odbieranych informacji oraz doświadczył spadku samopoczucia w związku ze zbyt długą ekspozycją na treści w social mediach – 46% doświadczało tych dolegliwości przynajmniej od czasu do czasu. Duża część respondentów dostrzegła również u siebie obniżony nastrój wywołany przez napotkane w Internecie przemocowe czy wulgarne treści – prawie połowa (48%) ankietowanych zaznaczyła odpowiedzi powyżej 4 w siedmiostopniowej skali.

Szczegółowe wyniki przedstawiono na wykresie 1 poniżej. Jak wykazano w zestawieniu, odpowiedzi ankietowanych były dość zróżnicowane i nie wskazują na jednoznaczne tendencje dominujące wśród badanych studentów.

Wykres 1. Trudności doświadczane przez studentów WFUŁ (1 – w ogóle tego nie doświadczałem/łam, 7 – doświadczałem/łam tego nieustannie)



Źródło: opracowanie własne

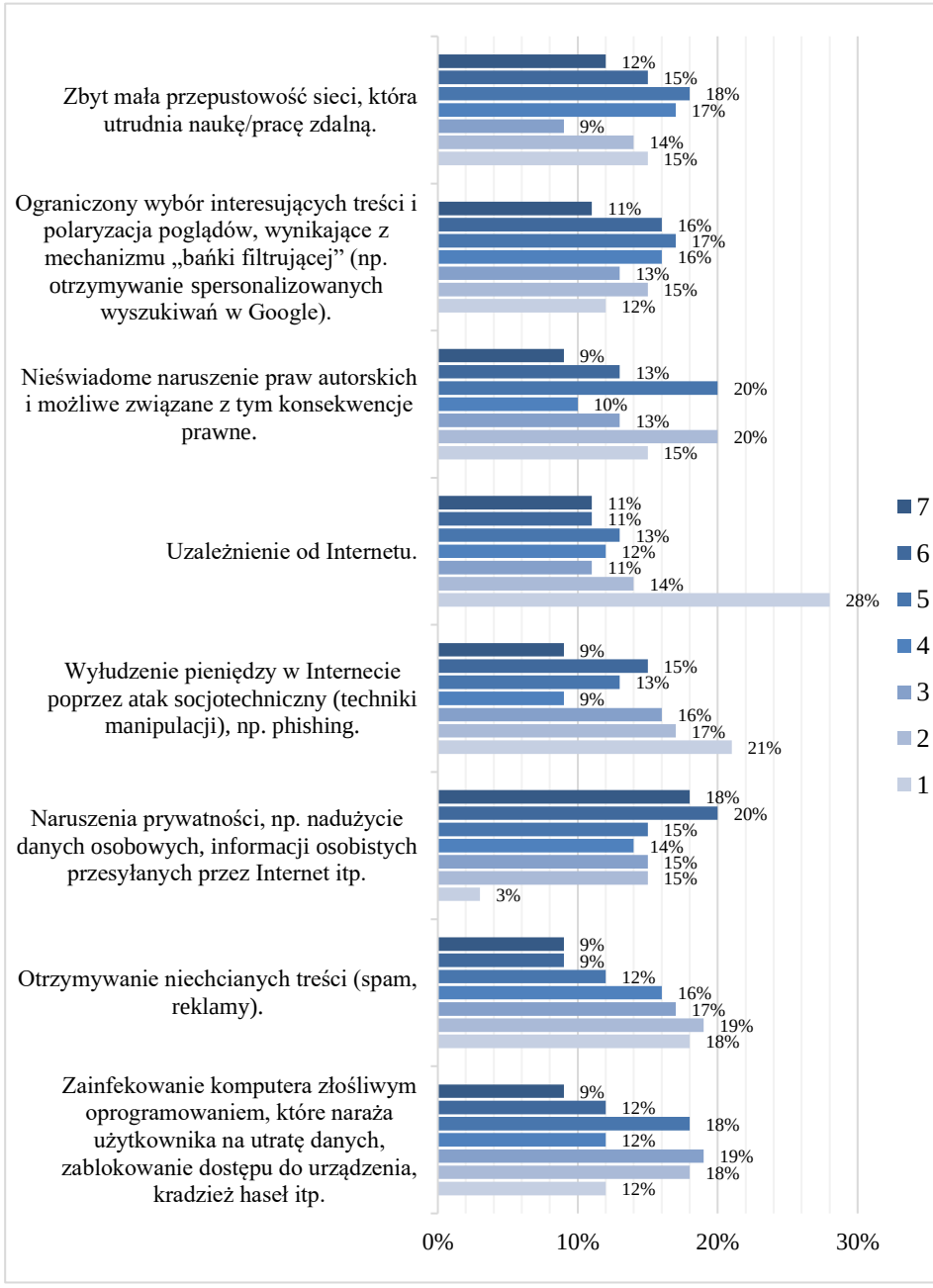
Kolejnym aspektem, który wzięto na warsztat na potrzeby tego badania, było zainteresowanie studentów i doktorantów kwestiami bezpieczeństwa w Internecie. Aspekt ten zbadano, tak jak w przypadku doświadczanych trudności, posługując się siedmiostopniową skalą Likerta, gdzie 1 oznaczało

„w ogóle się tego nie obawiałem/łam", a 7 – „obawiałem/łam się tego nieustannie". Zainteresowanie to może objawiać się między innymi poprzez ich obawy dotyczące wybranych zagrożeń, które użytkownicy mogą napotkać każdego dnia w sieci.

Najmniejsze niepokoje studenci wykazywali w stosunku do otrzymywania niechcianych treści, takich jak spam w skrzynce mailowej czy reklamy – 54% ankietowanych zaznaczyło odpowiedzi między 1-3. Dość jednoznacznie wskazali oni również, że nie odczuwają oni zagrożenia związanego z uzależnieniem od Internetu – 25% pytanych wykazuje niewielkie obawy, a 28% w ogóle się tego nie obawia. 54% badanych nie ma również większych obaw w związku z wyłudzeniami w wyniku ataków socjotechnicznych, do których można zaliczyć phishing, pozwalający przestępcy na uzyskanie wrażliwych danych. Z drugiej strony spory odsetek studentów, bo aż 53%, w dużym lub bardzo dużym stopniu niepokoi się naruszeniami prywatności, osobistych informacji, którymi dzieli się w Internecie. Obawy te mogą wynikać jednak nie tyle z braku umiejętności zabezpieczania danych, ale z braku zaufania studentów do narzędzi, którymi się posługują, i korporacji, które niewystarczająco dbają o bezpieczeństwo danych, a ich polityka prywatności często jest nieprzejrzysta.

Wiele sprzeczności wykazał podpunkt dotyczący obaw przed nieświadomym naruszeniem praw autorskich. Choć nieco więcej studentów ma niewielkie obawy (33%) lub w ogóle nie ma takich obaw (15%), duża grupa respondentów (42%) wykazywała większe niepokoje w związku z tym zagadnieniem. Głębsza analiza odpowiedzi pozwoliła na wysnucie wniosków, że zagadnienie to wzbudza niepokój wśród studentów, którzy są w trakcie pisania prac dyplomowych (studenci ostatniego roku studiów licencjackich i studiów magisterskich). Zróżnicowane odpowiedzi pojawiły się również w przypadku obaw związanych z zainfekowaniem komputera złośliwym oprogramowaniem – 49% badanych wykazuje niewielki stopień zaniepokojenia, a wysoki – 39% (choć tylko 9% obawiało się tego nieustannie). Częściowo (45%) studenci bali się również o niedostateczną jakość sieci w trakcie pracy czy zajęć zdalnych. Niemal taki sam odsetek studentów miewa obawy zarówno niemałe (44%), jak i nieznaczne (40%) związane z mechanizmem bańki filtrującej. Pełne zestawienie zobrazowano na wykresie 2.

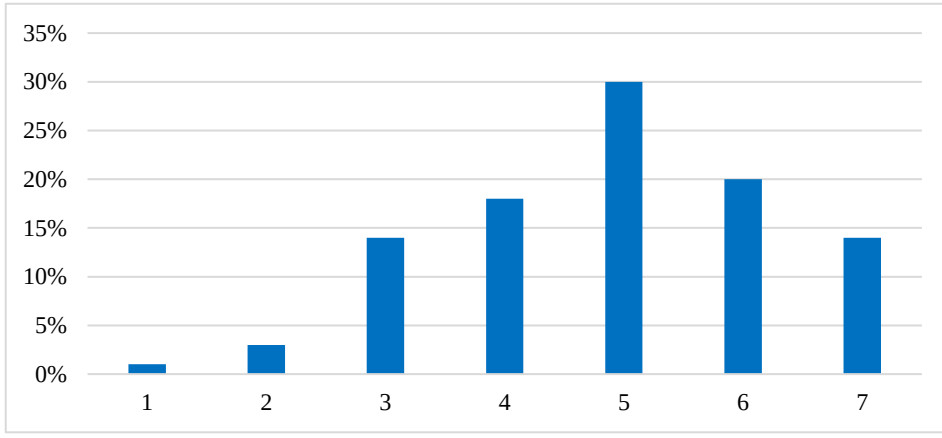
Wykres 2. Obawy studentów WFUŁ przed zagrożeniami związanymi z korzystaniem z Internetu (1 – w ogóle się tego nie obawiałem/łam, 7 – obawiałem/łam się tego nieustannie)



Źródło: opracowanie własne

Chęć poszerzania wiedzy studentów i doktorantów Wydziału Filologicznego Uniwersytetu Łódzkiego w zakresie zmniejszania ryzyka zagrożeń w Internecie zbadano również w formie pytania o określenie w skali od 1 do 7, w jakim stopniu interesują się oni kwestiami bezpieczeństwa w sieci. Jak widać na wykresie 3, ponadprzeciętne zainteresowanie (5) wykazało aż 30% ankietowanych, a duże lub bardzo duże – kolejno 20% i 14%. Tylko 1% nie czuje potrzeby poszerzania zasobów wiedzy w tych kwestiach, 17% zaś odczuwa taką potrzebę w małym stopniu. Oznacza to, że kwestie bezpieczeństwa w Internecie w większości (64%) są dla studentów istotne i nie brak im ambicji do rozwijania kompetencji w tym zakresie. Zazwyczaj mają oni świadomość tego, jak ważną rolę odgrywa Internet i niezakłócone poruszanie się po jego zasobach.

Wykres 3. Zainteresowanie studentów WFUŁ kwestiami bezpieczeństwa w Internecie



Źródło: opracowanie własne

Dobrą praktyką w celu poprawy bezpieczeństwa w Internecie jest korzystanie z różnego rodzaju programów i narzędzi zabezpieczających. Studenci zostali zapytani o to, z jakich zabezpieczeń korzystają w celu ochrony swojego bezpieczeństwa w Internecie. Pytanie miało charakter półotwarty – poza wyborem odpowiedzi respondenci mogli podzielić się innymi narzędziami, z których korzystają, wypisując je w odpowiedzi „Inne".

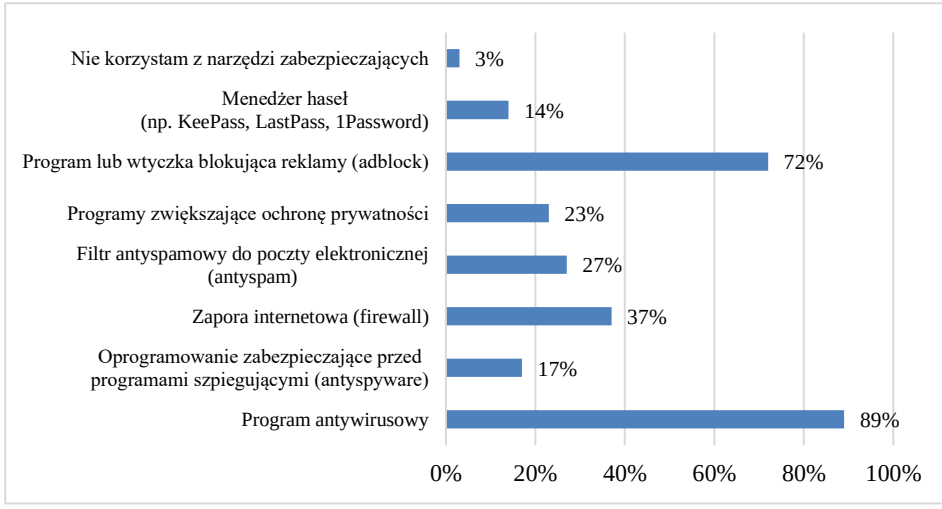
Na wykresie 4 można odczytać, że z narzędzi zabezpieczających nie korzysta zaledwie 3% ankietowanych. Znaczna większość ankietowanych (89%) dla ochrony swojego komputera korzysta z programu antywirusowego. Duży odsetek badanych (72%) to posiadacze wtyczki lub programu blokującego reklamy. Nieco mniej, bo 37% respondentów, wykorzystuje zaporę sieciową w celu ochrony sieci przed intruzami, natomiast z filtra do poczty elektronicznej korzysta 27 % ankietowanych. Choć duży odsetek studentów (zob. wykres 2)

obawia się naruszeń poufnych informacji, tylko 23% z nich korzysta z programów zwiększających ochronę prywatności. 17% ankietowanych ma zaś zainstalowane oprogramowanie antyspyware, zabezpieczające przez programami szpiegującymi, a 14% badanych zadeklarowało, że korzysta z menedżera haseł.

Część studentów korzysta także z innych rozwiązań. Niektórzy wszelkie aspekty związane z cyberbezpieczeństwem zawierzają urządzeniu od Apple (MacBook), które, w opinii wielu internautów, daje pełną ochronę środowiska cyfrowego. Inni zaś żartobliwie wymieniają zdrowy rozsądek jako „najlepszego antywirusa". Dwie osoby wymieniły również konkretne programy, z których korzystają – bezpłatna wersja oprogramowania Malwarebytes, które usuwa złośliwe oprogramowanie i spyware, oraz otwarte oprogramowanie NetGuard, blokujące dostęp do Internetu wybranym aplikacjom mobilnym.

Można więc uznać, że podstawą, z której korzysta znaczna większość studentów, jest antywirus – głębsza analiza odpowiedzi pokazała, że 19 osób zadeklarowało, że jest on jedynym narzędziem zabezpieczającym, z którego korzystają. Prawdopodobnie niektóre wymienione rozwiązania nie są studentom jeszcze znane lub nie rozumieją oni podstaw ich działania ze względu na mniejszą popularność tego typu narzędzi.

Wykres 4. Korzystanie studentów WFUŁ z programów i narzędzi zabezpieczających



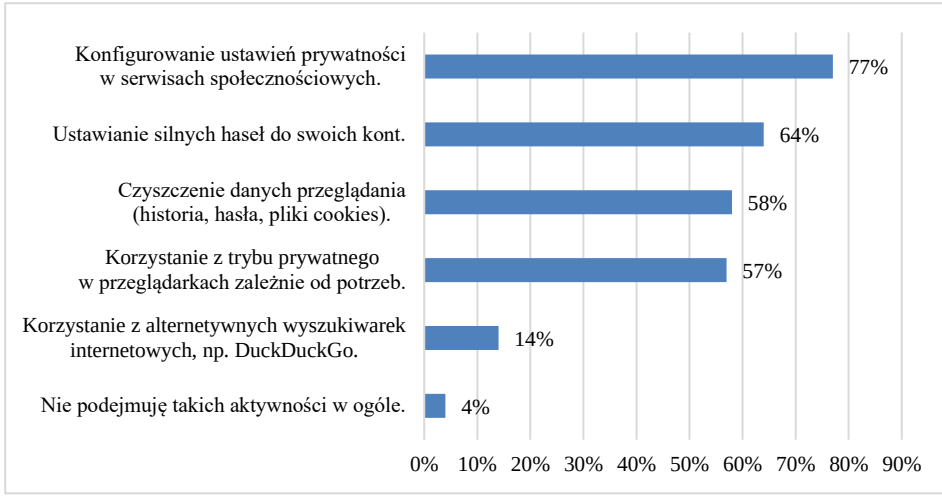
Źródło: opracowanie własne

Ochrona zasobów, prywatności i wizerunku to ważne aspekty, które mogą zwiększyć poczucie bezpieczeństwa w przestrzeni wirtualnej. Aktywności tych dotyczyło pytanie 5 w części pytań właściwych. Studenci mieli do wyboru 6 odpowiedzi, mogli też podać własne sugestie podejmowanych na co dzień działań.

Zaledwie 4% ankietowanych przyznało, że nie podejmuje takich aktywności w ogóle. Niewielki odsetek studentów (14%) w celu ochrony prywatności korzysta zaś z alternatywnych (czyli poza Google) wyszukiwarek internetowych. Większość respondentów (ponad połowa) podejmuje pozostałe wymienione działania. 77% badanych potrafi konfigurować ustawienia prywatności w serwisach społecznościowych według swoich potrzeb, 64% dba o ustawianie silnych haseł do swoich kont. Nieco niżej, ale wciąż wysoko, plasuje się czyszczenie danych przeglądania (58%), czyli historii, zapisanych haseł czy plików cookies, co również służy zwiększeniu bezpieczeństwa prywatności użytkownika. Z trybu prywatnego w przeglądarkach internetowych korzysta natomiast 57% badanych studentów (zob. wykres 5).

Z przeprowadzonej analizy wynika zatem, że tego typu działania zapobiegawcze nie są studentom obojętne i mają oni dość dobrą wiedzę, jak chronić swoje zasoby, prywatność i wizerunek w podstawowym zakresie.

Wykres 5. Aktywności podejmowane przez studentów WFUŁ w celu ochrony swoich zasobów, prywatności i wizerunku w Internecie



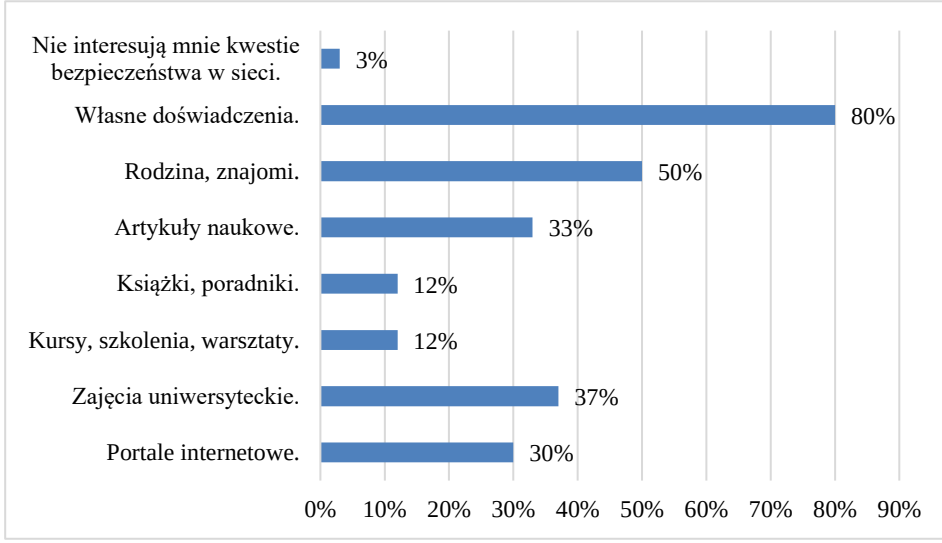
Źródło: opracowanie własne

Zwiększeniu bezpieczeństwa w cyfrowym środowisku sprzyja także korzystanie z wiarygodnych źródeł wiedzy na temat ochrony w sieci. Kolejne pytanie miało na celu sprawdzenie, gdzie studenci poszukują informacji na temat ochrony w Internecie. Było to pytanie o charakterze półotwartym, które poza odpowiedziami do wyboru dawało respondentom możliwość podzielenia się źródłami, które nie zostały uwzględnione w zestawieniu. 3% badanych studentów nie jest zainteresowanych bezpieczeństwem w sieci i nie poszerza swojej wiedzy w tych kwestiach.

Najsłabiej w zestawieniu (zob. wykres 6) wypadły kursy, szkolenia i warsztaty oraz książki i poradniki – tylko 12% studentów wykorzystuje te źródła do podnoszenia poziomu swoich umiejętności. 30% ankietowanych poszukuje zasobów wiedzy na portalach internetowych takich jak Niebezpiecznik czy Sekurak, zaś 33% respondentów przyznało, że w celu poszerzenia wiedzy z zakresu bezpieczeństwa w sieci czyta teksty naukowe. Niemały odsetek badanych (37%) nową wiedzę pozyskuje w trakcie zajęć uniwersyteckich. Wysoko ceniona przez ankietowanych jest wiedza pozyskiwana od rodziny i znajomych (50%), wyniki jednoznacznie wykazały jednak, że to własne, codzienne doświadczenia, czujność i praktyka są dla badanych zasadnicze jeśli chodzi o zdobywanie informacji o ochronie w Internecie – 80% studentów w ten właśnie sposób dowiaduje się o potencjalnych zagrożeniach i ochronie w cyberprzestrzeni.

Studenci wymieniali również dodatkowe miejsca, w których szukają wiedzy na temat cyberbezpieczeństwa. Często wymieniano materiały wideo zamieszczane w serwisie YouTube (np. kanały The PC Security Channel, SomeOrdinaryGamers, Tom Scott). Inni badani czerpią wiedzę także z blogów, zaufanych stron na Facebooku, podcastów, a nawet z telewizji. Jak można odczytać na wykresie 6, badani w mniejszym stopniu czerpią zatem z profesjonalnie przygotowywanych materiałów, a zdają się raczej na doświadczenia swoje i swoich bliskich.

Wykres 6. Źródła wiedzy studentów WFUŁ na temat bezpieczeństwa w Internecie

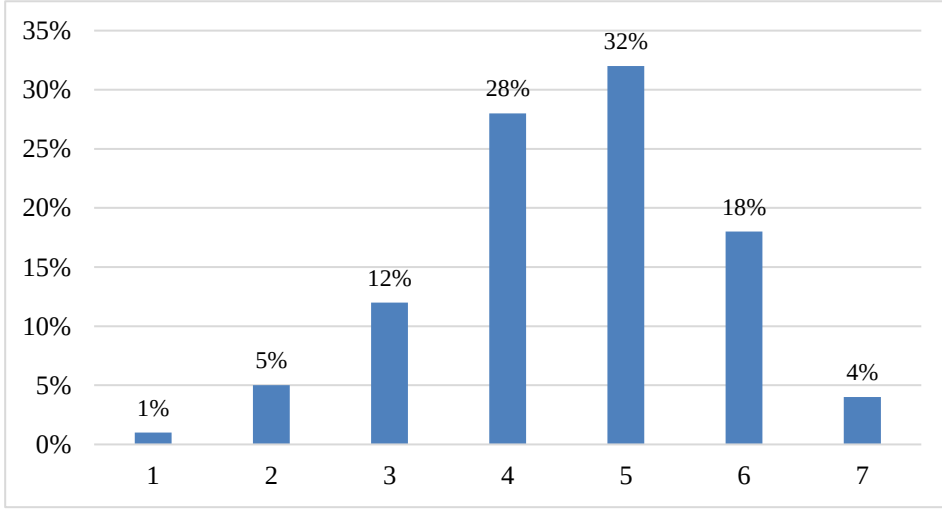


Źródło: opracowanie własne

Studentów zapytano także o samoocenę ich kompetencji związanych z cyberbezpieczeństwem. Badani stosunkowo wysoko ocenili swoją wiedzę, umiejętności i doświadczenie. Aż 32% ankietowanych w siedmiostopniowej skali przyznała sobie ocenę 5, 28% – ocenę 4. Niewielki odsetek pytanych osób uznał, że ma bardzo niskie lub niskie kompetencje w zakresie bezpiecznego korzystania z Internetu (1% ankietowanych przyznało sobie ocenę 1, 5% – ocenę 2, a 12% – ocenę 3). Bardzo wysoką ocenę (6) przyznało sobie 18% studentów biorących udział w badaniu, natomiast najwyższą notę (7) – 4%.

Analiza danych zaprezentowanych na wykresie 7 wskazuje, że studenci są dość pewni swoich umiejętności, doświadczenia i wiedzy. Wysoka ocena wynika najprawdopodobniej z wieloletniej znajomości środowiska cyfrowego i płynnego poruszania się w sieci – szczególnie, że, jak wynika z zamieszczonej wcześniej analizy źródeł wiedzy na temat bezpieczeństwa w sieci, to swoje doświadczenia studenci traktują jako dobry wyznacznik wiedzy i umiejętności. Deklarowany przez nich poziom kompetencji wymaga sprawdzenia ich rzeczywistych zdolności, co stanowi pole do dalszych badań w dziedzinie informatologii. Taka weryfikacja mogłaby mieć charakter symulacji wybranych cyberzagrożeń (np. ataków socjotechnicznych) w praktyce i być przestrogą dla nieostrożnych użytkowników sieci i zachęcić ich do ustawicznego zwiększania stopnia swoich umiejętności i wiedzy.

Wykres 7. Samoocena kompetencji studentów WFUŁ w zakresie bezpieczeństwa w Internecie



Źródło: opracowanie własne

Zakończenie

Realizacja założeń badania i postawionych celów została zakończona sukcesem, a wyniki przeprowadzonego badania pozwoliły na udzielenie odpowiedzi na postawione pytania badawcze. Badanie empiryczne, przeprowadzone na reprezentacyjnej grupie studentów, pozwoliło ustalić, jakich trudności związanych z korzystaniem z Internetu studenci Wydziału Filologicznego Uniwersytetu Łódzkiego najczęściej doświadczają, jakich zagrożeń w sieci najbardziej się obawiają, w jaki sposób studenci chronią swoje zasoby, prywatność i wizerunek w Internecie, z jakich źródeł czerpią wiedzę o cyberbezpieczeństwie i jak oceniają swoje kompetencje w tym zakresie.

Badania przeprowadzone na grupie studentów pozwoliły dojść do wielu ciekawych wniosków. Wśród najczęściej doświadczanych przez ankietowanych trudności można wymienić przeciążenie informacyjne związane z wszechobecną nadprodukcją informacji oraz poczucie potrzeby „bycia na bieżąco" z wszystkim, co dzieje się w sieci, w lęku przed pominięciem jakiejś istotnej informacji. Najmniej kłopotliwe dla respondentów jest zaś weryfikowanie prawdziwości treści napotykanych w Internecie.

Naruszenia prywatności w cyberprzestrzeni, takie jak nadużycia danych osobowych czy informacji osobistych, to najczęściej wymieniane zagrożenia, których studenci obawiają się najbardziej. Najmniej obaw studenci mają natomiast w związkuz zainfekowaniem komputera złośliwym oprogramowaniem, otrzymywaniem niechcianych treści (takich jak spam czy reklamy) oraz wyłudzeniami w wyniku ataków socjotechnicznych, np. phishingowych.

Analiza wykazała, że zainteresowanie kwestiami bezpieczeństwa w Internecie wśród studentów Wydziału Filologicznego Uniwersytetu Łódzkiego jest na wysokim poziomie, a ankietowanych nie trzeba przekonywać o fundamentalnym znaczeniu tego zagadnienia.

Zwiększeniu ochrony w sieci ankietowanym służą przede wszystkim programy antywirusowe oraz wtyczki i programy blokujące reklamy.

Aby ochronić swoje zasoby, prywatność i wizerunek w Internecie, respondenci zazwyczaj konfigurują ustawienia prywatności w serwisach społecznościowych, ustawiają silne hasła do kont i czyszczą dane przeglądania (historię, hasła, pliki cookies), najrzadziej zaś korzystają z alternatywnych wyszukiwarek. Niewielki odsetek pytanych nie podejmuje takich aktywności.

Najczęstszym źródłem wiedzy na temat cyberbezpieczeństwa są własne doświadczenia studentów oraz informacje zaczerpnięte od przyjaciół czy rodziny. Ankietowani rzadziej korzystają z bardziej formalnych źródeł wiedzy – szczególnie słabo wypadły tutaj książki i poradniki oraz kursy, szkolenia i warsztaty poruszające tematykę świadomego korzystania z Internetu i zasad bezpieczeństwa w sieci.

Reasumując należy powiedzieć, że studenci oceniają swoje kompetencje dość wysoko. W ocenie autorki artykułu większość z nich ma podstawową wiedzę, niezbędną do bezpiecznego poruszania się w sieci, oraz umiejętności korzystania z narzędzi umożliwiających lepszą ochronę w cyfrowej przestrzeni. Istnieje jednak niemała grupa studentów, która posiada pewne braki, przez co może być narażona na zagrożenia bezpieczeństwa w sieci. Szczególnie warte zarekomendowania wśród studentów zdaje się poszukiwanie przez nich wiedzy w wiarygodnych źródłach – większość z nich polega zarówno na doświadczeniach własnych, jak i swojej rodziny czy znajomych, ale znacznie rzadziej korzystają oni z zasobów wiedzy naukowej.

Zdecydowanie wskazane byłyby dalsze badania w tym kierunku, przeprowadzone na studentach wszystkich wydziałów Uniwersytetu Łódzkiego i badania porównawcze innych uczelni wyższych, co pozwoliłoby uzyskać miarodajne wyniki dla tej społeczności. Praktycznym polem do dalszej analizy byłoby poszukiwanie korelacji między cechami demograficznymi ankietowanych a poszczególnymi kwestiami związanymi z zachowaniem bezpieczeństwa w sieci.

Bibliografia

Babik, Wiesław (2012). Ekologia informacji katalizatorem równoważenia rozwoju społeczeństwa informacji i wiedzy. *Zagadnienia Informacji Naukowej*, **2**, 48–65, [online]. Pobrano 28 marca 2021 r., z: http://bbc.uw.edu.pl/dlibra/docmetadata?id=1865&from=publication&.

Furmanek, Waldemar (2014). Zagrożenia wynikające z rozwoju technologii informacyjnych. *Dydaktyka informatyki*, **9**, 20–48, [online]. Pobrano 17 marca 2021 r., z: http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-8cea2630-e302-4479-bdc9-1f829e0539ff/c/Furmanek_1.pdf

Information Security Threats and Tools for Addressing Them (2019). In: exabeam.com [online], Pobrano 17 marca 2021 r., z: https://www.exabeam.com/information-security/information-security-threats/

Internet Usage Statistics. The Internet Big Picture (2021). In: Internet World Stats [online]. Pobrano 6 stycznia 2021 r., z: https://www.internetworldstats.com/stats.htm

Jabłońska, Marta R. (2018). *Człowiek w cyberprzestrzeni. Wprowadzenie do psychologii Internetu*. Łódź: Wydawnictwo Uniwersytetu Łódzkiego.

Kaczmarczyk, Barbara, Szczepański, Piotr & Dąbrowska, Marlena (2019). Wybrane zagadnienia cyberbezpieczeństwa. *Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy*, **32**(3), 201–210, [online]. Pobrano 9 stycznia 2021 r., z: http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-d9156188-4716-4a21-9ad6-6204c6e5931a

Kasprzak, Wojciech (2015). *Ślady cyfrowe. Studium prawno-kryminalistyczne*. Warszawa: Wydawnictwo Difin.

Kasprzak, Włodzimierz, Szynkiewicz, Wojciech, Stefańczyk, Maciej, Dudek, Wojciech, Figat, Maksym, Węgierek, Maciej, Seredyński Dawid & Zieliński Cezary (2019). Agentowa struktura wielomodalnego interfejsu do Narodowej Platformy Cyberbezpieczeństwa, część 1. *Pomiary*

Automatyka Robotyka, **23**(3), 41–54, [online]. Pobrano 9 stycznia 2021 r., z: https://bibliotekanauki.pl/articles/275795

Kvardova, Nikol, Smahel, David, Machackova, Hana & Subrahmanyam, Kaveri (2021). Who Is Exposed to Harmful Online Content The Role of Risk and Protective Factors Among Czech, Finnish, and Spanish Adolescents. *Journal of Youth and Adolescence*, 50, 2294–2310, [online]. Pobrano 9 marca 2021 r., z: https://doi.org/10.1007/s10964-021-01422-2

Lakomy, Miron (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice: Wydawnictwo Uniwersytetu Śląskiego, [online]. Pobrano 6 stycznia 2021 r., z: https://rebus.us.edu.pl/bitstream/20.500.12128/3499/1/Lakomy_Cyberprzestrzen_jako_nowy_wymiar_rywalizacji.pdf

Lau, Jesús (2011). *Kompetencje informacyjne w procesie uczenia się przez całe życie. Wytyczne*. Warszawa: Stowarzyszenie Bibliotekarzy Polskich, [online]. Pobrano 12 stycznia 2021 r., z: https://www.ifla.org/files/assets/information-literacy/publications/ifla-guidelines-pl.pdf

Maciejczuk, Mateusz, Wnorowski, Konrad & Olchanowski, Mateusz (2019). Cyberprzestrzeń a bezpieczeństwo dzieci w świetle rozwiązań Organizacji Narodów Zjednoczonych oraz Rady Europy. *Zeszyty Naukowe Zbliżenia Cywilizacyjne*, **14**(3), 10–34, [online]. Pobrano 6 stycznia 2021 r., z: https://journals.indexcopernicus.com/api/file/viewByFileId/513085.pdf.

Marczyk, Maciej (2018). Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa. *Przegląd Teleinformatyczny*, T. 6, **1-2**(46), 59–72, [online]. Pobrano 8 stycznia 2021 r., z: http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-44818be5-0fed-41b3-8d4e-b339ad40a286

Masrek, Mohamad N., Soesantari, Tri, Khan, Asad & Dermawan, Aang K. (2020). Examining the relationship between information security effectiveness and information security threats. *International Journal of Business and Society*, **21**(3), 1203–1214.

Matusz, Magdalena (2007). Kompetencje informacyjne uczniów. W: J. Pavelka (red.), *Kľúčovékompetencie a technickévzdelávanie*. Prešov: FHPV, s. 48–55.

Motylińska, Paulina (2020a). Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji. Wprowadzenie. W: H. Batorowska & P. Motylińska (red.), *Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji*. Warszawa: Wydawnictwo Naukowe i Edukacyjne Stowarzyszenia Bibliotekarzy Polskich, s. 11–18.

Motylińska, Paulina (2020b). Profilaktyka i kształtowanie świadomości w zakresie bezpieczeństwa informacyjnego w środowisku nadmiarowości informacji. W: H. Batorowska & P. Motylińska (red.), *Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji*. Warszawa: Wydawnictwo Naukowe i Edukacyjne Stowarzyszenia Bibliotekarzy Polskich, s. 201–222.

Musiał, Emilia (2020). Zagrożenia bezpieczeństwa informacyjnego w kontekście nadmiarowości informacji. W: H. Batorowska & P. Motylińska (red.), *Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji*. Warszawa: Wydawnictwo Naukowe i Edukacyjne Stowarzyszenia Bibliotekarzy Polskich, s. 177–200.

Ogonowska, Agnieszka (2016). Kompetencje cyfrowe we współczesnej cywilizacji medialnej. *Annales Universitatis Paedagogicae Cracoviensis*, **8**(2), 14–26, [online]. Pobrano 11 stycznia 2021 r., z: http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-b06b7d89-e5ca-4144-b0e7-3e53ccad5be1/c/de_Cultura_VIII__2__.14-26.pdf

Prensky, Mark (2001). Digital Natives, Digital Immigrants. *On the Horizon*, **9**(6), 1–6, [online]. Pobrano 11 stycznia 2021 r., z: https://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

Stachowiak, Beata (2009). Kompetencje kluczowe studentów w kontekście oczekiwań społeczeństwa informacyjnego. W: A. Szeląg (red.), *Kompetencje absolwentów szkół wyższych na miarę czasów. Wybrane ujęcia*. Wrocław: Oficyna Wydawnicza ATUT, s. 111–119.

Wasilewski, Janusz (2013). Zarys definicyjny cyberprzestrzeni. *Przegląd bezpieczeństwa wewnętrznego*, **9**(5), 225–234, [online]. Pobrano 6 stycznia 2021 r., z: https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa/987,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-9-5-2013.html

Węgrzyn-Odzioba, Liliana (2018). Zagrożenia bezpieczeństwa społecznego związane z funkcjonowaniem w cyberprzestrzeni. *Teka Komisji Politologii i Stosunków Międzynarodowych*, **13**(2), 77–96, [online]. Pobrano 9 stycznia 2021 r., z: https://journals.umcs.pl/teka/article/download/9435/6555

Załącznik – Kwestionariusz ankiety

Ankieta dotycząca wiedzy, umiejętności i postaw studentów Wydziału Filologicznego Uniwersytetu Łódzkiego w zakresie bezpiecznego korzystania z Internetu

Metryczka

Płeć
Kobieta
Mężczyzna

Wiek
18–19 lat
20–21 lat
22–23 lata
24–25 lat
26 lat i więcej

Stopień studiów
1 stopień (studia licencjackie)
2 stopień (studia magisterskie)
studia jednolite magisterskie
3 stopień (studia doktoranckie)

Kierunek studiów
.....

Pytania właściwe

1. W jakim stopniu doświadczył(a) Pan/Pani następujących trudności w ciągu ostatnich 12 miesięcy?

1. Poczucie stresu, frustracji lub doświadczenie innych negatywnych symptomów związanych z trudnością przyswojenia odbieranych informacji.
2. Trudność oceny prawdziwości informacji napotkanej w Internecie.
3. Poczucie potrzeby „bycia na bieżąco" z możliwie jak największą liczbą wiadomości w Internecie.
4. Przemęczenie organizmu związane z natłokiem informacji w Internecie.
5. Obniżenie nastroju związane z napotkaną w Internecie mową nienawiści, hejtem i innymi obraźliwymi/wulgarnymi treściami.
6. Spadek samopoczucia lub zaniżenie poczucia własnej wartości w związku ze zbyt długą ekspozycją na treści w mediach społecznościowych, np. wyidealizowane sylwetki popularnych osób na Instagramie.

2. Na ile obawia się Pan/Pani możliwych zagrożeń związanych z korzystaniem z Internetu?

1. Zainfekowanie komputera złośliwym oprogramowaniem, które naraża użytkownika na utratę danych, zablokowanie dostępu do urządzenia, kradzież haseł itp.
2. Otrzymywanie niechcianych treści (spam, reklamy).
3. Naruszenia prywatności, np. nadużycie danych osobowych, informacji osobistych przesyłanych przez Internet itp.

4. Wyłudzenie pieniędzy w Internecie poprzez atak socjotechniczny, np. phishing.
5. Uzależnienie od Internetu.
6. Nieświadome naruszenie praw autorskich i możliwe związane z tym konsekwencje prawne.
7. Ograniczony wybór interesujących treści i polaryzacja poglądów, wynikającez mechanizmu „bańki filtrującej".
8. Zbyt mała przepustowość sieci, która utrudnia naukę zdalną/pracę.

3. W jakim stopniu interesują Pana/Panią kwestie bezpieczeństwa w Internecie

Skala 1–7

4. Z jakich programów lub narzędzi zabezpieczających korzysta Pan/Pani dla zwiększenia ochrony w sieci?

a) Program antywirusowy.
b) Oprogramowanie zabezpieczające przed programami szpiegującymi (antyspyware).
c) Zapora internetowa (firewall).
d) Filtr antyspamowy do poczty elektronicznej (antyspam).
e) Programy zwiększające ochronę prywatności.
f) Program lub wtyczka blokująca reklamy (adblock).
g) Menedżerhaseł (np. KeePass, LastPass, 1Password).
h) Nie korzystam z narzędzi zabezpieczających.
i) Inne (jakie?).

5. Jakich innych aktywności podejmuje się Pan/Pani w celu ochrony swoich zasobów, prywatności i wizerunku w Internecie?

a) Konfigurowanie ustawień prywatności w serwisach społecznościowych.
b) Korzystanie z trybu prywatnego w przeglądarkach zależnie od potrzeb.
c) Korzystanie z alternatywnych wyszukiwarek internetowych, np. DuckDuckGo.
d) Czyszczenie danych przeglądania (historia, hasła, pliki cookies).
e) Ustawianie silnych haseł do swoich kont.
f) Nie podejmuję takich aktywności w ogóle.
g) Inne (jakie?).

6. Z jakich źródeł czerpie Pan/Pani wiedzę na temat bezpieczeństwa w Internecie?

a) Portale internetowe, np. Niebezpiecznik, Sekurak.
b) Zajęcia uniwersyteckie.
c) Kursy, szkolenia, warsztaty.
d) Książki, poradniki.
e) Artykuły naukowe.
f) Rodzina, znajomi.
g) Własne doświadczenia.
h) Nie interesują mnie kwestie bezpieczeństwa w Internecie.
i) Inne (jakie?).

7. Jak ocenia Pan/Pani swoje kompetencje w zakresie bezpiecznego korzystania z Internetu?

Skala 1–7.

Measurement of the knowledge, skills and attitudes of students of the Faculty of Philology at the University of Lodz in the field of safe use of the Internet

ABSTRACT: The article discusses the competences of students of the Faculty of Philology at the University of Lodz on the topic of safe usage of the Internet. The goal of the research was to recognise, analyse and measure the knowledge, skills and attitudes of students, within the safe consumption of content posted and faced on the Internet every day, as well as other facets related to challenges of cyberspace. Attention was also paid to the potential of competences related to information and digital skills which should not be lacking, especially (but not only) by students of the university. Therefore, the key values would be: continuous development of those skills, gaining knowledge and awareness of potential dangers.

The following research methods were used to achieve set goals: critical analysis of the literature, the bibliographic method and the method of diagnostic survey. To understand the essence of the issue and to delve into the subject of online security, it was necessary to address definitions of "cyberspace", "cybersecurity", "digital competences" and "information literacy" as well as characterize selected threats to online security, which was done by review of literature.

In the methodological part, the subject of the research, goals and research issues was pointed out, the principles of the sampling were defined and research methods, techniques and tools were described. The research part is an analysis of the results of the survey conducted on students of the Faculty of Philology at the University of Lodz.

The survey was conducted on a group of students and is now able to determine the difficult that would arise from using the Internet, in addition students of the Faculty of Philology were experiencing most frequently what threats they were most afraid to encounter and how students protect their privacy, resources and image on the Internet, from what sources they learn about cybersecurity and how they asses their own competences in this area. The analysis shows that most of the respondents have basic knowledge necessary for responsible usage of Internet resources, as well as abilities to use tools that enable better protection in digital space. However, further research in this direction is recommended.

KEYWORDS: information literacy, digital competences, cybersecurity, Internet security threats