FOLIA 368

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 12(2) (2022)
ISSN 2657-8549
DOI 10.24917/26578549.12.2.9

Paulina Motylińska
ORCID ID: 0000-0002-1652-4832
Uniwersytet Pedagogiczny w Krakowie

Anna Pieczka
ORCID ID: 0000-0002-5136-7975
Uniwersytet Pedagogiczny w Krakowie

Zagrożenia wpływające na poczucie bezpieczeństwa informacyjnego – perspektywa studentów

Threaths affecting the feeling of information safety – students' perspective

Abstrakt

Celem artykułu jest identyfikacja i kategoryzacja zagrożeń wpływających na poczucie bezpieczeństwa informacyjnego użytkowników informacji. Badanie zrealizowano w oparciu o metodę pamiętników. Jako narzędzie badawcze zastosowano strukturyzowane dzienniczki obserwacji zagrożeń, prowadzone w formie pisemnej i obejmujące cztery główne aspekty: opis sytuacji zagrożenia poczucia bezpieczeństwa informacyjnego, skutki zdarzenia, reakcja respondenta, uwagi/komentarze. Zgromadzono 134 wpisy, które w kolejnym etapie poddano analizie jakościowej z wykorzystaniem metody jakościowej analizy zawartości. Ustalono, że zagrożenia wpływające na poczucie bezpieczeństwa informacyjnego wskazywane przez respondentów można podzielić na dwie główne grupy: 1) zagrożenia w cyberprzestrzeni, oraz 2) zagrożenia w świecie rzeczywistym. Wśród zidentyfikowanych zagrożeń znalazły się m.in. niechciane wiadomości (w tym phishing), niechciane połączenia telefoniczne oraz zmanipulowane informacje w Internecie i mediach tradycyjnych.

Słowa kluczowe: poczucie bezpieczeństwa informacyjnego, bezpieczeństwo informacyjne, zagrożenia poczucia bezpieczeństwa informacyjnego, metoda pamiętników

Abstract

The aim of the article is to identify and categorize threats affecting the feeling of information safety of information users. The research was based on the method of solicited diaries. Structured observation diaries were used as a research tool, kept in written form and covering four main aspects: description of the threat to information safety, consequences of the event, respondent's reaction, remarks / comments. 134 diary entries were collected, which in the next stage were analysed using the method of qualitative analysis of content. It was established that threats influencing the feeling of information safety indicated by the respondents can be divided into two main groups: 1) threats in cyberspace, and 2) threats in the real world. Among the identified threats there are for example: unwanted messages

(including phishing), unwanted phone calls, and manipulated information on the Internet and traditional media.

Key words: feeling of information safety, information safety, threaths to feeling of information safety, diary method

Wprowadzenie

Poczucie bezpieczeństwa informacyjnego to nowa kategoria badawcza, powstała na pograniczu informatologii oraz nauk o bezpieczeństwie. Zasadza się ona na szerokim podejściu do problematyki bezpieczeństwa informacyjnego (m.in. Fehler, 2016; Korzeniowski, 2012; Liderman, 2012) i jako taka oznacza stan, w którym użytkownik informacji nie odczuwa zagrożeń wynikających: a) z kontaktu z informacją niskiej jakości oraz b) z utraty całości bądź części zgromadzonych zasobów informacyjnych. W zamian towarzyszy mu natomiast poczucie spokoju, bezpieczeństwa i satysfakcji z doświadczanego poziomu bezpieczeństwa informacyjnego, a także przekonanie o posiadaniu zasobów (np. wiedzy i umiejętności związanych z oceną jakości informacji), niezbędnych do podjęcia odpowiednich działań w obliczu sytuacji kryzysowej (Pieczka, Motylińska, 2021).

W badaniach poczucia bezpieczeństwa informacyjnego szczególnie istotny wydaje się być aspekt zagrożeń mogących wpływać na obniżenie subiektywnie doświadczanego poziomu bezpieczeństwa informacyjnego. Umiejętna identyfikacja i kategoryzacja tych trudności może znacząco pomóc gestorom (np. dostawcom informacji lub podmiotom oferującym usługi informacyjne) w podejmowaniu działań służących skutecznemu ich przezwyciężaniu, w efekcie przyczyniając się do podniesienia poziomu bezpieczeństwa informacyjnego jednostek i grup społecznych.

Przegląd krajowego piśmiennictwa naukowego ujawnił, że problematyka zagrożeń poczucia bezpieczeństwa informacyjnego nie stanowiła dotąd przedmiotu autonomicznych badań. W obszarze nauk o bezpieczeństwie pojawiają się co prawda publikacje poświęcone zagrożeniom bezpieczeństwa informacyjnego, są to jednak prace odnoszące się do obiektywnych niebezpieczeństw zagrażających bezpieczeństwu informacyjnemu np. państwa (Bączek, 2016), policji (Polończyk, 2017), organizacji (Więcaszek-Kuczyńska, 2014), w środowisku nadmiarowości informacji (Musiał, 2020), zatem nie do zagrożeń subiektywnie postrzeganego poczucia bezpieczeństwa informacyjnego jednostki.

Sam termin „poczucie bezpieczeństwa informacyjnego" bywa w literaturze przywoływany, jednak jego stosowanie ma przeważnie charakter potoczny, intuicyjny i dotyczy m.in.: pozyskiwania aktualnych i sprawdzonych (pochodzących bezpośrednio od dysponenta) informacji podczas użytkowania serwisu Facebook (Popiołek, 2018, s. 222), „zapewniania poczucia bezpieczeństwa informacyjnego" w kontekście stosowania dwóch obiegów informacji w organizacji – obiegu papierowego oraz elektronicznego (w intranecie) (Kozłowski, 2013, s. 176), standaryzacji procedur i jednolitego sposobu zaspokajania potrzeb użytkowników bibliotek w przypadku placówek zakorzenionych w różnych kulturach i językach (Kisilowska, 2010, s. 130) oraz przetwarzania danych osobowych osób fizycznych (Poniatowski,

2021, s. 71). Pewien wyjątek stanowi tu praca K. Łąbędzia, w której poczucie bezpieczeństwa informacyjnego zostało powiązane z takimi aspektami, jak: cyberwojny, cyberterroryzm, niebezpieczeństwa związane z przesyłaniem, wymianą i wykorzystaniem informacji w Internecie oraz zagrożenia wynikające z naruszania prywatności przez policję i inne służby, i jako takie uznane za jeden z elementów poczucia bezpieczeństwa społeczeństwa (Łabędź, 2018, s. 54–55).

Prezentowany artykuł stanowi kontynuację i rozszerzenie badań zainicjowanych we wcześniejszej pracy autorek na temat poczucia bezpieczeństwa informacyjnego. Materiał badawczy – swobodne wypowiedzi studentów – poddano wówczas analizie jakościowej z wykorzystaniem metody jakościowej analizy treści. Badanie prowadzone było w czterech obszarach:

1) zakres znaczeniowy pojęcia „bezpieczeństwo informacyjne";
2) zakres znaczeniowy pojęcia „poczucie bezpieczeństwa informacyjnego";
3) sytuacje poczucia bezpieczeństwa informacyjnego;
4) sytuacje poczucia zagrożenia bezpieczeństwa informacyjnego.

W odniesieniu do zagrożeń ustalono, że zachodzą one zarówno w cyberprzestrzeni, jak i w świecie rzeczywistym. W kontekście cyberprzestrzeni do zagrożeń najczęściej wzmiankowanych przez respondentów należały: naruszenie bezpieczeństwa danych osobowych i informacji, naruszenie prywatności w Internecie oraz sytuacje związane z nieprawidłowym funkcjonowaniem stron internetowych. Zagrożenia obserwowane w świecie rzeczywistym dotyczyły w znacznej mierze obaw i naruszeń związanych z transakcjami finansowymi i ochroną danych osobowych, jak również naruszeń tajemnicy korespondencji, naruszeń funkcjonowania systemów teleinformatycznych i sprzętu oraz naruszeń związanych z odbieranymi komunikatami medialnymi (Pieczka, Motylińska, 2021).

Celem niniejszej pracy jest szczegółowa identyfikacja i kategoryzacja zagrożeń wpływających na poczucie bezpieczeństwa informacyjnego użytkowników informacji. Przedmiot badań stanowią zagrożenia subiektywnie odczuwane przez respondentów i zarejestrowane przez nich w ramach zleconego zadania. Sposób realizacji analiz własnych przedstawiono w kolejnej części artykułu.

Metodologia badania

Ze względu na przyjęte założenia badawcze, dotyczące bieżącego rejestrowania zagrożeń wpływających na poczucie bezpieczeństwa informacyjnego przy jednoczesnej minimalizacji błędów wynikających z konieczności przypominania sobie przeszłych wydarzeń, w prowadzonych analizach zdecydowano się wykorzystać metodę pamiętników. Przyjęto, że materiałem badawczym będą dokumenty w formie pisemnej, tworzone na zamówienie (ang. *solicited diaries*). W celu zredukowania wątpliwości respondentów co do tego, czy daną sytuację odnotować czy też nie, pamiętnikom nadana została określona struktura, nakierowująca na aspekty szczególnie istotne z punktu widzenia badaczy. Wprowadzanie poszczególnych wpisów warunkowane było wystąpieniem sytuacji zagrożenia poczucia bezpieczeństwa informacyjnego (tzw. podejście *event-contingent,* zasadne przy analizowaniu zjawisk rzadkich), przy czym ustalono, że wpisy będą zamieszczane nie rzadziej niż raz na

dwa tygodnie. Jako że w zastosowanym wariancie kluczowe jest, aby kryteria definicyjne badanego zjawiska były dla respondentów zrozumiałe (Wildemuth, 2009, s. 212–213), badanie poprzedził szczegółowy instruktaż, zawierający informację o przedmiocie prowadzonych analiz.

W badaniu wzięło udział 22 studentów kierunku „bezpieczeństwo państwa" (specjalność „bezpieczeństwo informacyjne") realizowanego na Uniwersytecie Pedagogicznym w Krakowie. Wśród badanych znalazło się 12 studentów (7 mężczyzn i 5 kobiet) II roku studiów stacjonarnych II stopnia oraz 10 studentów (7 mężczyzn i 3 kobiety) II roku studiów niestacjonarnych II stopnia. W terminie od 23.11.2021 r. do 05.02.2022 r. studenci zostali poproszeni o prowadzenie dzienników obserwacji zagrożeń dla ich bezpieczeństwa informacyjnego w codziennym życiu. Uzupełnianie dzienników miało się odbywać na bieżąco, w krótkim czasie od zaobserwowania zagrożenia. Studenci otrzymali formularz obserwacji zagrożenia do uzupełniania, obejmujący następujące elementy:

1) Opis sytuacji – Co się wydarzyło? Kiedy? Gdzie? Kto i co zrobił?

2) Skutki zdarzenia – Jaki był rezultat / konsekwencje tej sytuacji?

3) Reakcja – Jaka była Twoja reakcja na tę sytuację? Co zrobiłaś/eś? Jakie masz odczucia wobec tego zdarzenia?

4) Uwagi/komentarze – Co sądzisz o tej sytuacji? Jakie wnioski możesz wyciągnąć?

Przystępując do wykonania zadania studenci znali różnicę pomiędzy pojęciem „bezpieczeństwa informacyjnego" i „bezpieczeństwem informacji". *Bezpieczeństwo informacyjne* obejmuje zarówno perspektywę ochrony obiektu (informacji) przed zagrożeniami, jak i perspektywę niepowodowania zagrożeń przez sam obiekt (informację) – w tym np. informację niskiej jakości – zaś *bezpieczeństwo informacji* odnosi się wyłącznie do zabezpieczenia obiektu (informacji) przed zagrożeniami (Ilvonen, 2011). W dziennikach studentów zarejestrowano w sumie 134 wpisy z analizą zagrożeń.

Zgromadzony materiał badawczy poddano analizie jakościowej. W tym celu wykorzystano metodę jakościowej analizy zawartości (ang. *qualitative analysis of content*), dzięki której możliwe jest rozpoznanie zakresów znaczeniowych danego pojęcia bądź zjawiska (Wildemuth, 2009). Opracowując wypowiedzi studentów starano się wyodrębnić grupy tematyczne/kategorie nadrzędne, do których można by przyporządkować zidentyfikowane zagrożenia. Rezultaty analiz przedstawiono w formie tabelarycznej w kolejnej części artykułu.

Wyniki

W tabeli 1 przedstawiono pogrupowane tematycznie wpisy studentów, w nawiasach podano liczbę wpisów w pamiętnikach, w których dane zagrożenie wystąpiło (n=134). Wpisy w pamiętnikach studentów znacznie różniły się poziomem szczegółowości oraz sposobem charakteryzowania zagrożeń – studenci nie zawsze opisywali swoje reakcje lub konsekwencje zdarzenia. W kilku przypadkach w jednym wpisie scharakteryzowano więcej niż jedno zagrożenie (na podstawie 134 wpisów

wyodrębniono 141 opisy zagrożeń). Przykłady wypowiedzi studentów przytoczono w oryginalnym brzmieniu.

Rejestr zagrożeń wpływających na poczucie bezpieczeństwa informacyjnego

Zagrożenia wpływające na poczucie bezpieczeństwa informacyjnego, zaobserwowane przez studentów i opisane przez nich w pamiętnikach, można umownie podzielić na dwie grupy: 1) zagrożenia w cyberprzestrzeni, oraz 2) zagrożenia występujące w świecie rzeczywistym.

Wśród zagrożeń występujących w cyberprzestrzeni, wpływających na poczucie bezpieczeństwa informacyjnego respondentów, najczęściej wskazywano otrzymywanie niechcianych wiadomości, głównie wiadomości phishingowych (w tym wiadomości mailowych, smsowych oraz wiadomości w mediach społecznościowych):

> Otrzymanie wiadomości mailowej, której autor podszywał się pod firmę, której ofertą ja i inni ludzie w moim miejscu pracy mogą być zainteresowani. […] Nie odpowiadałem na tę wiadomość mailową i poinformowałem w ramach ostrzeżenia współpracujące ze mną osoby.

> 19.12.2021 dostałem SMS'a z informacją o problemie z dostawą przesyłki ze zwykłego numeru. W wiadomości był link przekierowujący na stronę zupełnie nie związaną z firmą dostarczającą przesyłki. […] W związku z tym, że rzeczywiście czekałem na przesyłkę, kliknąłem w link.

> Data: 03.12.2021. Mail z agencji towarzyskiej/biura matrymonialnego z propozycją kliknięcia w zapewne podejrzany link. Co ciekawe, na dole maila widniała informacja, że zleceniodawcą wiadomości była Interia. Zablokowałam nadawcę, jednak sytuacja z tego typu wiadomościami pojawia się cyklicznie.

W przypadku wystąpienia zagrożenia o charakterze phishingowym studenci deklarowali, że ich reakcje były rozważne i ostrożne – wiadomości phishingowe najczęściej ignorowano lub usuwano, a nadawcę wiadomości blokowano. Część studentów deklarowała także informowanie osób bliskich o potencjalnym zagrożeniu.

Zagrożenia dla bezpieczeństwa informacyjnego we wpisach studentów obejmowały także zagrożenia wynikające z kontaktu z treściami internetowymi niskiej jakości – zmanipulowanymi informacjami dostępnymi w Internecie, przekazami reklamowymi (w tym reklamami spersonalizowanymi) oraz treściami spersonalizowanymi, które wyświetlane są użytkownikowi na podstawie jego wcześniejszej aktywności:

> Manipulacja informacjami. Zobaczyłam post na Facebooku Mateusza Morawieckiego dotyczący Polskiego Ładu udostępniony przez innego Pana. Była to grafika dotycząca, ile procent Polaków zarabia do 12 800 zł brutto. Robiąc projekt postanowiłam to sprawdzić i znalazłam rzekomy post Mateusza Morawieckiego, ale już o innej treści. Nie wiem, który post jest prawdziwy, ale mimo to albo jeden albo drugi był manipulacją.

> Moją codzienną rutyną jest przeglądanie memów. Doszedłem do wniosku, że same w sobie są one pewnego rodzaju zagrożeniem informacyjnym. Przedstawiają one bowiem w kilku słowach perspektywę na dany (zazwyczaj aktualny) aspekt. Nietrudno więc zauważyć że w kilku słowach nie sposób omówić bardziej skomplikowanych spraw.

> 29.12.2021 r. Sugestie w reklamach. Kiedy szukałem w internecie interesujących mnie produktów. W tym przypadku były to spodnie, po odwiedzeniu kilkunastu stron ze spodniami, zaczęły się one pojawiać dosłownie co kilka „stron" na facebooku w sugestiach jako reklamy.

> 21.12; platforma Youtube; pokazywanie filmów wyłącznie na podstawie moich poprzednich wyników (w tym wypadku filmiki o gotowaniu). Na stronie głównej portalu pojawiały się przepisy tego samego dania od innych autorów (niekiedy dalekowschodnich lub rosyjskich użytkowników).

W przypadku tego zagrożenia studenci bardzo często opisywali swoje emocje i odczucia, mające wyraźnie negatywny charakter: „czułem się monitorowany", „zostałam zmanipulowana", „doszedłem do wniosku, że inwigilacja jest na porządku dziennym", „czułam się dość dziwnie", „byliśmy zszokowani tą sytuacją", „zniechęcenie do dalszego zgłębiania tematu (chwilowe)".

Zagrożeniem poczucia bezpieczeństwa informacyjnego w opinii badanych są także próby włamania na konto (np. mailowe lub w mediach społecznościowych), otrzymywanie komunikatów o próbach nieautoryzowanego logowania do konta lub nawet rzeczywiste przejęcia konta użytkownika:

> Na popularnym portalu społecznościowym (Facebook) dostałem komunikat o próbie włamania się na moje konto. W komunikacie była informacja na temat tego, z jakiej miejscowości próbowano zalogować się na moje konto – około 250 km od miejsca mojego zamieszkania.

> Do wielu kont używam takich samych, w dodatku dość prostych haseł. Pewnego razu na moje konto na portalu Facebook ktoś się włamał, nie mogłam się na nie zalogować. Co za tym idzie, straciłam również dostęp do kont na Instagramie czy poczcie, ponieważ hasła do w/w kont również miałam tam takie same.

Studenci rejestrowali także zagrożenia związane z próbami oszustw w mediach społecznościowych (obejmujących m.in. otrzymanie zaproszenia do znajomych od osoby z fałszywym kontem, otrzymanie wiadomości z prośbą o przesłanie pieniędzy przez BLIK) oraz z próbami oszustw podczas zakupów elektronicznych (najczęściej – otrzymanie fałszywej wiadomości od kupującego):

> Niedawno dodała mnie osoba na facebooku o takim samym imieniu i nazwisku jak mój kolega z liceum pisząc wiadomość w celu pożyczenia 15 zł blikiem na bilet autobusowy.

> Podczas wystawienia rzeczy na sprzedaż na portalu „Vinted" zainteresowana osoba kupnem przedmiotu napisała wiadomość abym podał adres mailowy. Po chwili przyszedł mi mail od Vinted, ale gdy się wczytałem zobaczyłem dużo błędów ortograficznych i literówek, stwierdziłem że to może być phishing."

W przypadku opisu różnego rodzaju oszustw studenci w znacznej większości deklarowali, że udało im się rozpoznać zagrożenie, a fałszywe wiadomości były przez nich usuwane lub ignorowane.

Zagrożeniem wymienionym jedynie we wpisach dwóch respondentów, jednak zdecydowanie wartym uwagi, jest nadawanie nadmiernych uprawnień

instalowanym aplikacjom. Studenci zwrócili uwagę na fakt, że aplikacje mogą żądać dostępu m.in. do danych lokalizacyjnych użytkownika lub materiałów multimedialnych, przez co użytkownicy mogą czuć się inwigilowani:

> 25.01.2022 r. Prośba o zezwolenie dostępu do zdjęć i lokalizacji przy instalowaniu gry na androida. W konsekwencji tej sytuacji zrezygnowałem z zainstalowania gry, ponieważ bez akceptacji powyższych warunków nie można było z niej korzystać. Moim zdaniem jest to podejrzana sytuacja.

Wśród innych zagrożeń dla poczucia bezpieczeństwa informacyjnego, które wskazywane były w nielicznych wpisach studentów, można wyróżnić przypadkowe upublicznienie swoich danych osobowych lub prywatnych informacji (np. podanie swojego numeru telefonu w publicznym ogłoszeniu na Facebooku), wykrycie na swoim urządzeniu złośliwego oprogramowania, kradzież zdjęć z mediów społecznościowych i wykorzystanie ich do stworzenia fałszywego konta oraz podłączenie swojego telefonu do publicznej sieci Wi-Fi.

Opisów zagrożeń poczucia bezpieczeństwa informacyjnego występujących w świecie rzeczywistym było zdecydowanie mniej, niż wpisów dotyczących zagrożeń w cyberprzestrzeni (zagrożenia występujące w świecie rzeczywistym opisywano 47 razy, natomiast zagrożenia w cyberprzestrzeni – 94). Najczęściej wskazywanym zagrożeniem w świecie rzeczywistym było otrzymywanie niechcianych połączeń telefonicznych. Podczas rozmów telefonicznych dochodziło najczęściej do prób wyłudzenia danych osobowych i reklamowania produktów/usług:

> 17.01.2022. Usilne próby dodzwonienia się z ofertą fotowoltaiczną skierowaną do województwa małopolskiego. Brak odpowiedzi na pytanie skąd firma posiada mój numer.

> 13.01.2022 r. Telefon zza granicy. Pewnego dnia, kiedy zadzwonił do mnie telefon o dziwnym kierunkowym przez przypadek odebrałem. W rezultacie tego zdarzenia zmartwiłem się czy nie zostaną pobrane jakieś opłaty, ponieważ był to jakiś automat, który się rozłączył po moim odebraniu.

> Data: 26–30.11.2021. Ogromna ilość połączeń z nieznanych numerów, z wielu różnych miast, około 30 połączeń w 4 dni. Po sprawdzeniu w Internecie kilku numerów, okazało się że to telefony w sprawie szczepień, programów zdrowotnych realizowanych na terenie mojego województwa, szczepień, thermomixów, pokazów garnków i tym podobnych.

Większość badanych deklaruje, że blokuje nieznane numery telefonów, a w przypadku odebrania połączenia – że odmawia podania danych osobowych. Jednak jeden ze studentów zdecydował się na udział w loterii po odebraniu takiego połączenia telefonicznego:

> W czwartek 13.01.2022 r., zadzwonił do mnie warszawski numer. Po odebraniu okazało się, że była to głosowa reklama nagrana przez jednego z redaktorów i zachęta do udziału w loterii radia RMF FM. Jedynym rezultatem całej tej sytuacji było to, że dałem się namówić na wzięcie udziału w loterii i wysłałem SMS.

Podobnie jak w przypadku zagrożeń w cyberprzestrzeni, studenci raportowali zagrożenia związane z wykryciem zmanipulowanych treści oraz ogólnie pojętym nadmiarem informacji, głównie w telewizji:

> 02.02.2022 – fałszywe informacje podane w głównym wydaniu wiadomości TVP. W celu wyolbrzymienia problemu podano błędną informację na temat osób zatrudnionych w Kopalni Turów. W kopalni i firmach współpracujących pracuje ok 15 tys. osób. Podano informacje o kilkudziesięciu tysiącach miejsc pracy. Po usłyszeniu tej informacji sprawdziłem ile tak naprawdę miejsc pracy jest w kopalni Turów na jej oficjalnej stronie. Podawanie nieprawdziwych informacji i nierzetelnych jest złe.

Interesujące spostrzeżenia badanych, dotyczące sytuacji stanowiących zagrożenie dla poczucia bezpieczeństwa informacyjnego, dotyczą konieczności (lub ewentualnie dobrowolnego) podania danych osobowych w miejscu publicznym. Studenci spotykali się z takimi przypadkami w ośrodku zdrowia, na poczcie, w aptece, w której musieli podać na głos swoje dane osobowe:

> Realizowanie recepty w aptece. Aby zrealizować receptę konieczne jest podanie numeru PESEL, jednak stojąc przy okienku i podając go wszystkie osoby stojące w kolejce za mną go słyszą.

> Podczas robienia zakupów w sklepie Delikatesy Centrum, aby skorzystać z promocji podałam na głos swój nr telefonu w zamian za numer „delikarty".

Jeden z respondentów był także przypadkowym świadkiem podawania danych osobowych podczas rozmowy telefonicznej innej osoby:

> 25.01.2022 – Mężczyzna w sklepie Żabka rozmawiała przez telefon. Rozmówca podał dwa nazwiska oraz numery telefonu, następnie w celu sprawdzenia poprawności zapisanych informacji mężczyzna odczytał na głos numery oraz nazwiska.

Studenci stwierdzali, że dopiero po pewnym czasie i przeanalizowaniu sytuacji podawania danych osobowych w miejscu publicznym, zdawali sobie sprawę z istnienia zagrożenia: „Sądzę, że moje bezpieczeństwo informacyjne zostało naruszone, sama się do tego przyczyniłam."

Kilkukrotnie we wpisach studentów występowały także zagrożenia powiązane z transakcjami finansowymi – zagrożenia przy korzystaniu z kart płatniczych oraz zagrożenia związane z korzystaniem z bankomatu. Kilkoro studentów poczuło się niekomfortowo, gdy kolejna osoba czekająca w kolejce (w sklepie lub do bankomatu) podeszła zbyt blisko i miała możliwość zobaczenia danych wpisywanych na terminalu płatniczym lub w bankomacie.

Wśród innych zagrożeń dla poczucia bezpieczeństwa informacyjnego, które wystąpiły w świecie rzeczywistym, wskazywano fałszywe akcje charytatywne lub reklamowe (mające na celu wyłudzenie danych osobowych lub pieniędzy), kradzież lub awarię sprzętu, zgubienie dokumentów oraz brak dostępu do Internetu.

Tabela 1. Zagrożenia wpływające na poczucie bezpieczeństwa informacyjnego – analiza wpisów z pamiętników studentów

Rodzaj zagrożenia		**Reakcja studenta**
ZAGROŻENIA W CYBERPRZESTRZENI		
NIECHCIANE WIADOMOŚCI (SPAM / PHISHING) (34)	wiadomości mailowe (19) – podszywanie się pod zaufaną firmę (5) – fałszywa faktura (1) – konieczność zapłaty za zamówienie (3) – otrzymanie nagrody / spadku (3) – o charakterze erotycznym / matrymonialnym (2) – oferta marketingowa (2)	– ignorowanie wiadomości (7) – ostrzeżenie innych osób (4) – konsultacja z informatykiem (1) – zweryfikowanie zabezpieczeń swojego konta mailowego (2) – usuwanie wiadomości (4) – utrata pieniędzy (1)
	sms (10) – problem z przesyłką (7) – oferta marketingowa (1)	– kliknięcie w link (1) – obawa przed złośliwym oprogramowaniem (1) – blokada numeru (4) – oddzwonienie na dany numer (1) – ignorowanie wiadomości (2) – usuwanie wiadomości (2)
	w mediach społecznościowych / komunikatorach internetowych (5)	– utrata pieniędzy (1) – zablokowanie konta nadawcy wiadomości (4)
ZMANIPULOWANE / NIEPOKOJĄCE TREŚCI W INTERNECIE (12)	– na portalach informacyjnych (2) – w mediach społecznościowych (3) – memy internetowe (1) – informacje o wyciekach danych (5) – publikowane przez znajome osoby (2) – oficjalne informacje (1)	– ignorowanie wiadomości (1) – weryfikacja informacji w innym źródle (2)
REKLAMY INTERNETOWE (W TYM REKLAMY SPERSONALIZOWANE) (13)	– w formie włączających się filmów (1) – przypomnienia / wyskakujące okienka (11) – reklamy o treści erotycznej (1) – związane z lokalizacją GPS (3) – związane z wyszukiwanymi informacjami (6)	– ignorowanie reklam (2) – blokowanie reklam (2)
SPERSONALIZOWANE TREŚCI W INTERNECIE (2)	– w serwisie YT (2) – związane z wcześniejszymi wyszukiwaniami (2)	
PRÓBA WŁAMANIA NA KONTO / NIEAUTORYZOWANA PRÓBA LOGOWANIA (6)	– w serwisie Facebook (4) – konto Google (1) – w serwisie Instagram (1)	– weryfikacja zabezpieczeń konta (2) – zmiana hasła (2)

WŁAMANIE NA KONTO (3)	– w grze komputerowej (1) – w serwisie Facebook (1) – w serwisie Instagram (1)	– kontakt z pomocą techniczną serwisu (1)
PRÓBA OSZUSTWA W MEDIACH SPOŁECZNOŚCIOWYCH (6)	– fałszywe zaproszenia do grup (3) – fałszywe wiadomości z prośbą o przesłanie pieniędzy przez BLIK (1) – otrzymanie podejrzanych linków od znajomych (1) – zaproszenie do znajomych przez fałszywe konta (1)	– brak akceptacji dołączenia do grupy (1) – zablokowanie użytkownika (1) – usunięcie wiadomości (1)
PRÓBA OSZUSTWA PODCZAS ZAKUPÓW ELEKTRONICZNYCH (10)	– fałszywa wiadomość od kupującego (8) – nieotrzymanie towaru / towar niezgodny z umową (2)	– podanie danych osobowych (1) – dodatkowy kontakt z kupującym (1) – zignorowanie wiadomości (2) – rezygnacja z korzystania z serwisu (2) – zgłoszenie sprawy na policję (1) – zgłoszenie sytuacji administracji serwisu (1) – usunięcie wiadomości (1)
ZŁOŚLIWE OPROGRAMOWANIE (2)	– keylogger (1) – zainfekowana witryna (1)	– skanowanie programem antywirusowym (2)
NADMIERNE UPRAWNIENIA APLIKACJI (2)	– zezwolenie na dostęp do zdjęć (1) – zezwolenie na dostęp do lokalizacji (2)	– rezygnacja korzystania z aplikacji (1) – zablokowanie dostępu (1)
PRZYPADKOWE UDOSTĘPNIENIE DANYCH OSOBOWYCH (2)	– numeru telefonu (1) – wydarzeń w kalendarzu (1)	– edycja postu z danymi (1) – weryfikacja zabezpieczeń konta (1)
KRADZIEŻ TOŻSAMOŚCI (1)	– kradzież zdjęć z mediów społecznościowych (1) – fałszywe konto (1)	
PODŁĄCZENIE DO PUBLICZNEJ SIECI WI-FI (1)		
ZAGROŻENIA W ŚWIECIE RZECZYWISTYM		
NIECHCIANE POŁĄCZENIA TELEFONICZNE (17)	– próba wyłudzenia danych osobowych (11) – treści reklamowe (3) – przekierowanie połączenia (2)	– odmowa podania danych (8) – wzięcie udziału w loterii (1) – blokowanie numerów (7) – ostrzeżenie innych osób (1)
FAŁSZYWE AKCJE CHARYTATYWNE / MARKETINGOWE (3)	– zbieranie pieniędzy na akcję charytatywną (2) – zbieranie danych osobowych (2)	– weryfikacja legalności zbiórki (1) – wezwanie służb (1)
NADMIAR INFORMACJI (3)	– w telewizji (2) – sensacyjne wiadomości (1)	– korzystanie tylko z wybranych źródeł informacji (1) – weryfikacja informacji (2)

ZMANIPULOWANE TREŚCI W MEDIACH TRADYCYJNYCH (9)	– w telewizji (9)	– weryfikacja informacji (1)
ZAGROŻENIA PRZY PŁATNOŚCI KARTĄ (2)	– podglądanie wpisywania numeru PIN przez osobę postronną (2)	
ZAGROŻENIA PRZY KORZYSTANIA Z BANKOMATU (3)	– podejrzenie nakładki sczytującej dane z karty (1) – podglądanie wpisywanego numeru PIN (2)	– poinformowanie ochrony (1)
PUBLICZNE PODAWANIE DANYCH OSOBOWYCH (6)	– konieczność podania numeru PESEL (2) (apteka) – konieczność podania danych osobowych (2) (poczta, ośrodek zdrowia) – usłyszenie danych osobowych podawanych przez inną osobę (1) – podanie numeru telefonu (1)	
KRADZIEŻ SPRZĘTU (1)	– kradzież telefonu komórkowego (1)	– zgłoszenie sprawy na policję (1)
AWARIA SPRZĘTU (1)	– awaria laptopa (1)	– oddanie sprzętu do serwisu (1)
ZGUBIENIE DOKUMENTÓW (1)	– zgubienie portfela (1)	– zgłoszenie w banku (1)
BRAK DOSTĘPU DO INTERNETU (1)	– awaria sieci (1)	

Źródło: Opracowanie własne, 2022.

Dyskusja i wnioski

Analiza zgromadzonych wpisów z pamiętników studentów pozwoliła na sformułowanie kilku ogólnych wniosków. Po pierwsze, zagrożenia wpływające na poczucie bezpieczeństwa informacyjnego można podzielić na dwie główne grupy: 1) zagrożenia w cyberprzestrzeni, oraz 2) zagrożenia w świecie rzeczywistym – przy czym zdecydowana większość opisywanych przez respondentów sytuacji miała miejsce w cyberprzestrzeni. Po drugie, wśród najczęściej charakteryzowanych zagrożeń znalazły się niechciane wiadomości, w tym spam i phishing (analizy dotyczące tej grupy zagrożeń stanowiły aż 24% wszystkich charakterystyk) oraz niechciane połączenia telefoniczne (analizy dotyczące tej grupy zagrożeń stanowiły 12% wszystkich charakterystyk). Po trzecie, w stosunkowo dużej grupie wpisów wskazywano na zagrożenia związane z kontaktem z informacją niskiej jakości, informacją zmanipulowaną lub spersonalizowaną, zarówno w Internecie, jak i w mediach tradycyjnych. Wydaje się zatem, że część studentów poprawnie rozumie pojęcie „bezpieczeństwa informacyjnego", nie traktując go jedynie jako „ochrony informacji przed zagrożeniami". Po czwarte, studenci deklarują, że ich reakcje na pojawiające się sytuacje zagrożenia były świadome, rozważne i ostrożne – m.in. wskazywano, że wiadomości phishingowe najczęściej były ignorowane lub usuwane, podczas rozmów telefonicznych odmawiano podania danych osobowych, informowano inne osoby

o wystąpieniu zagrożenia lub zgłaszano sytuację odpowiednim służbom. Tylko nieliczni studenci wskazywali, że skutkiem wystąpienia zagrożenia były realne konsekwencje (np. utraty środków finansowych).

Zagrożenia, które wpływają na poczucie bezpieczeństwa informacyjnego, zidentyfikowane przez studentów, można także w większości przyporządkować do czterech podstawowych grup zagrożeń bezpieczeństwa informacyjnego określonych przez P. Bączka (2006). Bączek (2006) dzieli te zagrożenia na zagrożenia losowe, tradycyjne zagrożenia informacyjne, zagrożenia technologiczne oraz zagrożenia odnoszące się do praw obywatelskich osób lub grup społecznych. W tabeli 2 wskazano przykłady przyporządkowania zagrożeń, których doświadczyli respondenci, do czterech grup zagrożeń bezpieczeństwa informacyjnego.

Tabela 2. Przykłady zagrożeń wpływających na poczucie bezpieczeństwa informacyjnego w podziale na grupy

Rodzaje zagrożeń bezpieczeństwa informacyjnego (według Bączek, 2006)	Zagrożenia wpływające na poczucie bezpieczeństwa informacyjnego według studentów (przykłady)
I. Zagrożenia losowe	– awaria sprzętu – brak dostępu do Internetu
II. Tradycyjne zagrożenia informacyjne	– nadmiar informacji – zmanipulowane treści w Internecie i mediach tradycyjnych
III. Zagrożenia technologiczne	– włamanie na konto – otrzymywanie niechcianych wiadomości (phishing) – oszustwa w Internecie
IV. Zagrożenia odnoszące się do praw obywatelskich osób lub grup społecznych	– personalizowanie treści w Internecie (w tym reklam) w oparciu o wcześniejsze działania użytkownika

Źródło: Opracowanie własne, 2022

E. Musiał (2020, s. 181–182) zwraca uwagę, że we współczesnym świecie, wśród istotnych zagrożeń bezpieczeństwa informacyjnego znajdują się utrata lub upublicznienie informacji i danych osobowych oraz manipulacja przekazem informacji w mediach. Obie grupy zagrożeń zostały także zaobserwowane przez studentów jako te, które wpływają na ich poczucie bezpieczeństwa informacyjnego – studenci opisywali zagrożenia przypadkowego lub celowego podawania danych osobowych publicznie, a także kontaktu ze zmanipulowanymi treściami w Internecie i telewizji.

Uzyskane wyniki potwierdzają także ustalenia poczynione we wcześniejszej pracy autorek (Pieczka, Motylińska, 2021), dotyczące samej definicji poczucia bezpieczeństwa informacyjnego. Pojęcie to zostało definiowane jako stan, w którym użytkownik informacji nie odczuwa zagrożeń wynikających: a) z kontaktu z informacją niskiej jakości oraz b) z utraty całości bądź części zgromadzonych zasobów informacyjnych. Zagrożenia dla poczucia bezpieczeństwa informacyjnego doświadczane przez studentów zdecydowanie można powiązać zarówno z sytuacjami kontaktu z informacją niskiej jakości (w tym z informacją zmanipulowaną oraz spersonalizowaną zamykającą użytkownika w bańce filtrującej) oraz sytuacjami utraty

posiadanych lub zgromadzonych zasobów informacyjnych (np. utraty danych do logowania wyłudzonych od użytkownika z wykorzystaniem wiadomości phishingowych lub utraty dostępu do zasobów na skutek awarii urządzenia).

Poczucie bezpieczeństwa informacyjnego może być zaburzone na skutek wystąpienia licznych zagrożeń, zwłaszcza tych, które pojawiają się w cyberprzestrzeni. Zagrożenia wpływające na poczucie bezpieczeństwa informacyjnego obejmują zarówno naruszenia bezpieczeństwa danych osobowych i prywatnych informacji użytkowników, jak i naruszenia związane z bezpośrednim kontaktem użytkownika z informacjami niskiej jakości. Identyfikacja konkretnych zagrożeń dostrzeganych przez użytkowników oraz stworzenie ich rejestru niezbędne są do zaplanowania odpowiednich działań prewencyjnych służących eliminacji ryzyk ich wystąpienia lub powstania negatywnych skutków zagrożenia. W dalszych badaniach konieczne jest także sprawdzenie, jakie zagrożenia wpływające na poczucie bezpieczeństwa informacyjnego doświadczane są przez inne grupy społeczne – doświadczanie zagrożeń może być uzależnione m.in. od wieku, poziomu wykształcenia, podejmowanej aktywności w cyberprzestrzeni i świecie rzeczywistym, czy wykonywanej pracy zawodowej.

Bibliografia

Bączek, P. (2016). *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*. Wydawnictwo Adam Marszałek.

Fehler, W. (2016). O pojęciu bezpieczeństwa informacyjnego. W: M. Kubiak, S. Topolewski (red.), *Bezpieczeństwo informacyjne w XXI wieku* (s. 25–43). Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach.

Ilvonen, I. (2011). Information Security Culture or Information Safety Culture – What do Words Convey?. W: *European Conference on Information Warfare and Security* (s. 148–VII). Academic Conferences International Limited.

Kisilowska, M. (2010). *Biblioteka w sieci – sieć w bibliotece*. Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich.

Korzeniowski, L.F. (2012). *Podstawy nauk o bezpieczeństwie*. Difin.

Kozłowski, R. (2013). Ewolucja struktur organizacyjnych powodowanych wdrożeniem zaawansowanych technologii informacyjnych na przykładzie operatora telekomunikacyjnego. W: M. Matejun, K. Szymańska (red.), *Perspektywy rozwoju przedsiębiorczości w warunkach niepewności i ryzyka* (s. 172–180). Wydawnictwo Politechniki Łódzkiej.

Liderman, K. (2012). *Bezpieczeństwo informacyjne*. Wydawnictwo Naukowe PWN.

Łabędź, K. (2018). Poczucie bezpieczeństwa we współczesnym społeczeństwie polskim. *Facta Simonidis*, 11(1), 45–64.

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

Pieczka, A., Motylińska, P. (2021). Poczucie bezpieczeństwa informacyjnego. W: P. Korycińska (red.), *Horyzonty informacji 2* (s. 30–46). Uniwersytet Jagielloński, Biblioteka Jagiellońska.

Polończyk, A. (2017). Zagrożenia bezpieczeństwa informacyjnego na przykładzie Krajowej Mapy Zagrożeń Bezpieczeństwa. W: H. Batorowska, E. Musiał (red.), *Bezpieczeństwo informacyjne w dyskursie naukowym* (s. 79–94). Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej. Instytut Bezpieczeństwa i Edukacji Obywatelskiej. Katedra Kultury Informacyjnej i Zarządzania Informacją.

Poniatowski, P. (2021). Niedopuszczalne lub nieuprawnione przetwarzanie danych osobowych – aspekty prawnokarne. *Prokuratura i Prawo*, 10, 62–95.

Popiołek, M. (2018). Indywidualne zarządzanie prywatnością w serwisach społecznościowych – zarys problemu w kontekście rozważań dotyczących społeczeństwa informacyjnego. *Nierówności Społeczne a Wzrost Gospodarczy*, 53, 217–226.

Więcaszek-Kuczyńska, L. (2014). Zagrożenia bezpieczeństwa informacyjnego. *Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej*, 2(10), 210-233.

Wildemuth, B. (2009). *Applications of social research methods to questions in information and library science*. Libraries Unlimited.

Biogram autora

Paulina Motylińska – doktor nauk humanistycznych w dyscyplinie bibliologia i informatologia, absolwentka Uniwersytetu Jagiellońskiego w Krakowie, adiunkt w Instytucie Nauk o Bezpieczeństwie Uniwersytetu Pedagogicznego w Krakowie. Wśród jej zainteresowań naukowych znajdują się: bezpieczeństwo informacji i ochrona prywatności w Internecie, poczucie bezpieczeństwa informacyjnego, kompetencje informacyjne i cyfrowe w społeczeństwie informacyjnym. Autorka prac naukowych: m.in. *Poczucie bezpieczeństwa informacyjnego* (współautor A. Pieczka, 2021), *Ewaluacja jakości informacji jako komponent zachowania bezpieczeństwa informacyjnego* (współautor A. Pieczka, 2020), *Informacja zdrowotna: zawartość stron internetowych podmiotów leczniczych* (2020).

Anna Pieczka – magister, absolwentka Uniwersytetu Jagiellońskiego w Krakowie, asystent w Instytucie Historii i Archiwistyki Uniwersytetu Pedagogicznego w Krakowie. Wśród jej zainteresowań naukowych znajdują się: zachowania informacyjne użytkowników informacji, kształcenie kompetencji informacyjnych, infobrokering oraz poczucie bezpieczeństwa informacyjnego. Autorka prac naukowych: m.in. *Poczucie bezpieczeństwa informacyjnego* (współautor P. Motylińska, 2021), *Ewaluacja jakości informacji jako komponent zachowania bezpieczeństwa informacyjnego* (współautor P. Motylińska, 2020), *Infobrokering w edukacji i informacji o ubezpieczeniach społecznych – możliwość czy konieczność?* (2019).