Łukasz Rybak

Państwowa Wyższa Szkoła Zawodowa w Skierniewicach
Wydział Nauk Przyrodniczych i Technicznych, Instytut Informatyki i Matematyki Stosowanej

lrybak@pwsz.skierniewice.pl

ORCID 0000-0002-2920-7326

Janusz Dudczyk

Państwowa Wyższa Szkoła Zawodowa w Skierniewicach
Wydział Nauk Przyrodniczych i Technicznych, Instytut Informatyki i Matematyki Stosowanej

jdudczyk@pwsz.skierniewice.pl

ORCID 0000-0001-7169-6824

DOI: 10.13166/JMS/111174
JOURNAL OF MODERN SCIENCE TOM 2/41/2019, S.127–140

User experience in the aspect of threats to digital security

User experience w aspekcie zagrożenia dla bezpieczeństwa cyfrowego

Abstract

Aim

Characterization of user experience as a threat to cyber security and determination of the level of awareness of users of social networks in the aspect of sharing their data in the network are the goal of the research presented in the article.

Methods

In order to investigate the indicated problem, we applied one of the qualitative research methods - an individual in-depth interview based on the original scenario. The motivation to use this method is the need to receive the most detailed information from users. The research group includes 12 people aged between 19 and 25, who use social media on a daily basis.

Results

From the interviews we have obtained information about the respondents' knowledge about the data they provide and we have determined which data is actually made available by them in the network. On this basis, we have determined the level of awareness of users in the examined aspect. In addition, we obtained information about the motivation of the respondents to share data on portals of

this class, this allowed us to characterize the user experience as a threat to the security of the network.

Summary

The results of the research have shown that people who use social media on a daily basis show incomplete awareness of the data they provide on sites of this class. The direct cause of this phenomenon is the high level of usability of these systems and the positive user experience exerted by them. These factors make users willingly use social networking sites, while providing data about themselves, as a result of this fact they become the target of people using social engineering, eg in the process of agitation, and this is a threat to digital security.

Streszczenie

Cel

Celem badań przedstawionych w artykule jest scharakteryzowanie *user experience* jako czynnika zagrażającego cyberbezpieczeństwu i określenie poziomu świadomości użytkowników portali społecznościowych w aspekcie udostępniania przez nich swoich danych w sieci.

Metody

W celu zbadania określonego problemu zastosowano jedną z jakościowych metod badań, tj. indywidualny wywiad pogłębiony oparty na autorskim scenariuszu. Motywacją do wykorzystania wskazanej metody jest potrzeba otrzymania jak najbardziej szczegółowych informacji od użytkowników. Do grupy badawczej należy 12 osób w wieku od 19 do 25 lat, które na co dzień korzystają z portali społecznościowych.

Wyniki

Z przeprowadzonych wywiadów uzyskano informacje dotyczące wiedzy respondentów o danych, jakie udostępniają, i ustalono, jakie dane są faktycznie przez nich udostępniane w sieci. Na tej podstawie określono poziom świadomości użytkowników w badanym aspekcie. Ponadto pozyskano informacje na temat motywacji osób badanych do udostępniania danych na portalach tej klasy, to pozwoliło na scharakteryzowanie *user experience* jako czynnika zagrażającego bezpieczeństwu w sieci.

Podsumowanie

Wyniki przeprowadzonych badań dowiodły, że osoby na co dzień korzystające z portali społecznościowych wykazują niepełną świadomość na temat udostępnianych przez nich danych w serwisach tej klasy. Bezpośrednią przyczyną tego zjawiska jest wysoki poziom użyteczności tych systemów i wywierane przez nie pozytywne wrażenia użytkownika. Te czynniki sprawiają, że użytkownicy chętnie korzystają z serwisów społecznościowych, jednocześnie udostępniając dane na swój temat, w następstwie tego faktu stają się oni celem osób wykorzystujących socjotechniki, np. w procesie agitacji, a to stanowi zagrożenie dla bezpieczeństwa cyfrowego.

Keywords: *user experience, usability, cybersecurity, social media, digital security*

Słowa kluczowe: *doświadczenie użytkownika, użyteczność, cyberbezpieczeństwo, media społecznościowe, bezpieczeństwo cyfrowe*

Wprowadzenie

Poziom narodowego bezpieczeństwa cyfrowego jest silnie uzależniony od współpracy całego społeczeństwa. Zatem manipulacja decyzjami i działaniami ludzi może stanowić istotne, wielowymiarowe zagrożenie dla stabilnego funkcjonowania państwa. Należy zwrócić szczególną uwagę na dynamikę zmian zachodzących we współczesnym świecie, których efektem jest powstawanie nowych zagrożeń wewnętrznych i zewnętrznych mających bezpośredni wpływ na rozwój wielu krajów. W dobie wspomnianych metamorfoz ważnym celem dla każdego państwa staje się budowanie wewnętrznej świadomości społeczeństwa dotyczącej współczesnych zagrożeń (Wiśniewski, 2013, s. 303–317).

W artykule opisano rozważania na temat zagrożeń cybernetycznych, dla których podstawą jest proces analizy pojęcia „informacja" będącego produktem procesu interpretacji danych, w trakcie którego odbiorca poprzez analizę nadaje im znaczenie (Rybak, Dudczyk, Jezierski, 2018, s. 5–7). Formułowane są one w postaci elementarnych wniosków, w związku z tym ich wymiana jest bardziej przejrzysta w porównaniu do „danych surowych". Informacje w korelacji z doświadczeniem, świadomością i znajomością określonych faktów kreują wiedzę (Dudczyk, 2010, s. 5–17). W cywilizacji zdominowanej przez informacje w kontekście serwisów społecznościowych „zaszumienie" kontinuum rozumienia człowieka może być narzędziem zagrażającym bezpieczeństwu państwa (Dudczyk, Matuszewski, 2005).

W dalszej części artykułu przedstawiono globalne medium informacji, jakim są serwisy społecznościowe, jako narzędzie inżynierii społecznej w procesie agitacji. Ponadto przybliżono metodę i zasady projektowania tego typu portali, w których podkreślono rolę użytkownika w procesie ich wytwarzania. Badania opisane w artykule obrały dwa główne cele. Pierwszym z nich jest scharakteryzowanie doświadczeń użytkownika UX (ang. *user experience*) jako czynnika zagrażającego cyberbezpieczeństwu poprzez poznanie i analizę determinantów zachęcających ludzi do udostęp-

niania danych w serwisach społecznościowych. Natomiast drugim celem przeprowadzonych badań jest sprawdzenie, czy użytkownicy portali społecznościowych dysponują świadomością w aspekcie udostępniania przez nich swoich danych w sieci.

Serwisy społecznościowe jako narzędzie inżynierii społecznej

Obecnie doświadcza się dynamicznego rozwoju sektora teleinformatycznego ICT (ang. *information and communicaion technologies*). Zdeterminował on wykreowanie się społeczeństwa informacyjnego, w którym najważniejszy podmiot stanowi informacja. Na uwagę zasługuje jej polimorficzna funkcjonalność, ponieważ z jednej strony może ona być narzędziem produkcyjnym, ale jednocześnie może stanowić zagrożenie dla funkcjonowania państwa (Wiśniewski, 2013, s. 303–317).

W świecie zdominowanym przez informacje zagrożenia cybernetyczne odbijają silne piętno na działaniach osób i organizacji rządowych w cyberprzestrzeni. Ataki cybernetyczne obnażają słabe punkty w metodach ochrony danych, bezpieczeństwie infrastruktury oraz stosowanych politykach przetwarzania danych w instytucjach państwowych i firmach prywatnych (Mataracioglu, Ozkan, 2011, s. 1–7). Na przestrzeni lat Internet stał się środkiem masowego przekazu. Jego użytkowanie obecnie wykracza poza samo wyszukiwanie informacji. Cyberprzestrzeń oferuje użytkownikom m.in. dostęp do serwisów społecznościowych, gdzie mogą oni w czasie rzeczywistym wymieniać się informacjami (Mataracioglu, Ozkan, 2011, s. 1–7).

Echem dla wspomnianego faktu są dane Eurostatu, które donoszą, iż w 2016 roku z Internetu korzystało 82% mieszkańców Unii Europejskiej, natomiast jego codzienne użytkownie zadeklarowało 71% respondentów. Te same statystyki informują, że w czołówce aktywności sieciowej użytkowników było korzystanie z serwisów społecznościowych. Ponad połowa, bo aż 52% osób, używała Internetu, odwiedzając Facebooka lub Twittera. Analiza danych Eurostatu pozwala również na stwierdzenie, iż w 2016 ponad połowa polskiego społeczeństwa przekazywała dane osobowe drogą elektroniczną (European Statistical Office, 2018, s. 127–138).

Inżynierię społeczną można zdefiniować jako zespół technik, których efektem zastosowania jest pozyskanie informacji, a następnie ich wykorzystanie do wpływania na decyzje osób, których te informacje dotyczą. Inżynieria społeczna stanowi bardzo skuteczne narzędzie godzące w bezpieczeństwo przetwarzania danych, a w szerszej perspektywie też w bezpieczeństwo funkcjonowania państwa (Workman, 2007, s. 315–331). Wynika to z faktu, iż wykorzystuje ona wiele działań do manipulacji społeczeństwa (Mataracioglu, Ozkan, 2011, s. 1–7). Badania donoszą, że człowiek stanowi bardziej znaczący czynnik w kontekście ochrony danych niż środki *stricte* techniczne (Kumar, Chaudhary, Kumar, 2015, s. 15–19).

Przykładem prezentującym skalę problemu oraz praktyczne wykorzystanie serwisów społecznościowych jako narzędzia inżynierii społecznej był skandal związany z działaniami Cambridge Analytica podczas wyborów prezydenckich w Stanach Zjednoczony w 2016 roku. Czynności socjotechniczne polegały na rozwiązaniu testu osobowości przez użytkowników Facebooka. Na podstawie zebranych danych możliwe było określenie ich preferencji i późniejsze prezentowanie określonych treści, których celem było wpływanie na opinię odbiorców. Należy podkreślić, że aplikacja poza informacjami o jej posiadaczu pobierała również dane o osobach należących do jego kręgu (Zuckerberg, 2018).

Metoda projektowania zorientowanego na użytkownika w kontekście zdobywania zaufania

Na przełomie ostatnich lat można zaobserwować proces kreowania się rynku konsumenta. Upowszechnienie się zdobyczy technologicznych zdeterminowało stan, w którym użytkownicy interaktywnych systemów zbudowali świadomość dostępu do mnogości konkurencyjnych rozwiązań. W związku ze wskazanymi zmianami obecnie wybierają oni optymalne, pod kątem samodzielnie ustalanych kryteriów, systemy spośród wielu produktów o różnej jakości (Rybak, 2017, s. 8–11).

Wzrost świadomości użytkowników spowodował, iż poza osiągnięciem celu równie istotny stał się sam proces i okoliczności jego realizacji. W wyniku tego wybór aplikacji często wynika nie tylko z oferowanych przez system funkcjonalności czy jego ceny, ale także emocji, jakie generowane są po stro-

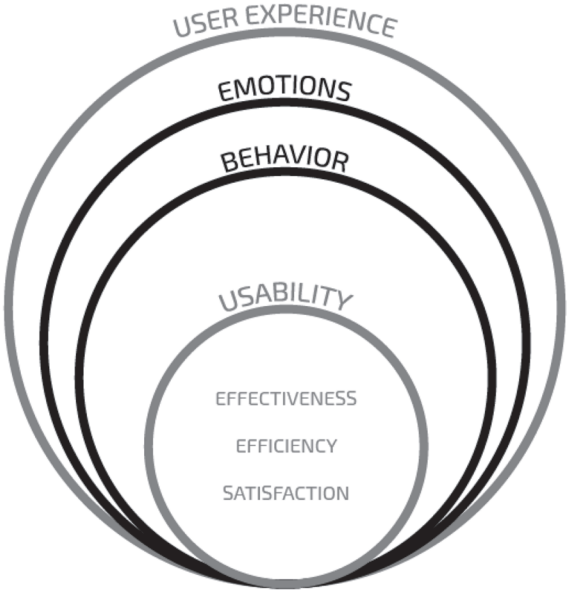
nie użytkownika w wyniku interakcji. W związku z tym celem stworzenia konkurencyjnego produktu kluczowym zadaniem dla zespołu projektowego stało się przeprowadzenie szerokiej analizy użyteczności (ang. *usability*) projektowanego rozwiązania. Proces i metody projektowania oprogramowania zorientowanego na użytkownika definiuje międzynarodowy standard ISO 9241-210 (International Organization for Standardization, 2018), wydany przez Międzynarodową Organizację Normalizacyjną ISO (ang. *International Organization for Standardization*) (Rybak, 2017, s. 8–11). Zawiera on zalecenia i wymagania dotyczące zasad ergonomii w procesie komunikacyjnym pomiędzy człowiekiem a systemem oraz reguły projektowania oprogramowania zorientowanego na użytkownika. Implementacja dobrych praktyk opisanych w ISO 9241-210 i ISO 9241-11 (International Organization for Standardization, 2018) tworzy środowisko sprzyjające wytwarzaniu interaktywnych systemów o wysokiej użyteczności. Jednakże należy zwrócić uwagę, że żaden ze wspomnianych standardów jednoznacznie nie definiuje konkretnych procesów ani metod weryfikacji systemu w kryteriach: składowych użyteczności i oceny projektu (Rybak, 2017, s. 8–11).

Na bazie wymienionych standardów można wyspecyfikować następujące, kluczowe składowe użyteczności:

- skuteczność (ang. *effectiveness*), czyli dokładność i kompletność realizowanych zadań;
- wydajność (ang. *efficiency*) – relację wykorzystanych zasobów do dokładności i kompletności realizowanych zadań;
- satysfakcję (ang. *satisfaction*) opisywaną jako wolność od dyskomfortu i pozytywne wrażenia użytkownika wywołane interakcją z systemem (Brooke, 1996, s. 189–194).

Rozszerzeniem pojęcia użyteczności, która definiuje jakość komunikacji użytkownika z systemem, są wrażenia użytkownika UX (ang. *user experience*). Obejmują one emocje towarzyszące odbiorcy w kontakcie z produktem, fizyczne i psychiczne reakcje człowieka oraz ogół zachowań występujących przed użytkowaniem systemu, w trakcie korzystania oraz po jego użytkowaniu. Składowe UX zwizualizowano na rysunku 1 (Andrzejczak, 2015, s. 35–38).

Rysunek 1.
Składowe User Experience UX



Źródło: Opracowanie własne

W myśl pryncypium metody projektowania zorientowanego na odbiorcę użytkownik końcowy produktu powinien brać czynny udział w procesie jego wytwarzania, na możliwie największej liczbie etapów projektu (Rybak, 2017, s. 8–11).

Indywidualny wywiad pogłębiony jako narzędzie do weryfikacji świadomości użytkowników serwisów społecznościowych

W przeprowadzonym badaniu wzięło udział 12 osób w wieku od 19 do 25 lat, które na co dzień korzystają z portali społecznościowych. Z uwagi na fakt, iż celem badań jest poznanie świadomości użytkowników oraz dokonanie charakterystyki zagrożenia, jakim jest *user experience*, zastosowano dwa narzędzia badawcze. Głównym z nich jest indywidualny wywiad pogłębiony IDI (ang. *Individual In-Depth Interview*) będący jakościową meto-

dą badawczą. Cechą charakterystyczną tej techniki jest udział małej liczby respondentów i wysoki stopień zaangażowania zarówno osoby badanej, jak i moderatora. To metoda, która umożliwia szczegółowe poznanie doświadczeń, reakcji behawioralnych osób badanych oraz ich determinantów, co jest głównym celem niniejszej pracy. W porównaniu do innych metod badawczych, np. ankiety, IDI dostarcza o wiele bardziej szczegółowych informacji. Jest to zdeterminowane faktem, że indywidualny wywiad pogłębiony przebiega w swobodnej atmosferze, co zapewnia bardziej komfortowe warunki respondentom niż przy okazji wypełniania ankiety (Boyce, Neale, 2006, s. 3–9).

Ponadto w badaniach wykorzystano kwestionariusz SUS (ang. *System Usability Scale*), którego zastosowanie pozwoliło na zestawienie rzeczywistej skali użyteczności badanych serwisów społecznościowych z subiektywną oceną doświadczeń użytkowników uzyskaną podczas przeprowadzania indywidualnego wywiadu pogłębionego. Badanie Skali Użyteczności Systemu zostało opracowane w 1986 roku, obecnie stanowi standard branżowy i może być stosowane przy niewielkich próbach badawczych (usability.gov). Popularność tego badania jest zdeterminowana jego największymi zaletami – szybkością przeprowadzenia oraz uniwersalnością. Realizacja polega na eksploracji testowanego systemu przez użytkowników. Celem uzyskania dodatkowych wyników te czynności mogą być także obserwowane i rejestrowane. Po zakończeniu interakcji odbiorcy wypełniają kwestionariusz składający się z 10 pytań. Kwestionariusz został zaprojektowany w taki sposób, że pytania negatywne są rozlokowane naprzemiennie z pytaniami mającymi wymiar pozytywny. Wskazane podejście, polegające na naprzemiennym ułożeniu pytań, wymaga od respondentów zaangażowania w badanie i jednocześnie pozwala na późniejszą weryfikację, czy dana osoba w pełni świadomie dokonała oceny testowanego produktu (Lewis, Sauro, 2009, s. 94–103). Posiadając wyniki kwestionariusza, kolejno stosuje się ściśle określony algorytm wyznaczenia skali użyteczności systemu, który przedstawiono na listingu 1.

Listing 1.
Zaimplementowany algorytm wyznaczania SUS w rankingu percentylowym

```
answers[10];
sum = 0;
for (i = 0; i < 10; i++)
  if (i % 2 != 0) sum += answers[i] - 1
  else sum += (answers[i] - 5) * -1
sus = sum * 2.5
```

Źródło: Opracowanie własne na podstawie usability.gov

Po wykonaniu stosownych obliczeń na wyjściu algorytm zwraca liczbę z przedziału 0–100, która stanowi poziom użyteczności testowanego systemu (Rybak, 2017, s. 8–11).

Poniżej przedstawiono ramowy scenariusz pojedynczego badania, które zostało podzielone na 3 części. Na wstępie sekwencyjnie zadawano badanym pytania dotyczące ogólnej formy korzystania przez nich z serwisów społecznościowych:

1. *Co Pan sądzi o serwisach społecznościowych?*
2. *Jak często korzysta Pan z serwisów społecznościowych?*
3. *Dlaczego tak chętnie korzysta Pan z serwisów społecznościowych?*
4. *Jakie dostrzega Pan zalety i wady serwisów społecznościowych?*
5. *Jaki wpływ serwisy społecznościowe mają na Pana życie?*
6. *Jakie informacje na swój temat udostępnia Pan w serwisach społecznościowych?*
7. *Jakie dostrzega Pan zalety i wady serwisów społecznościowych?*

Kolejnym etapem badania była 5-minutowa sesja, podczas której użytkownicy otrzymali zadanie skorzystania ze swojego profilu w dowolnym serwisie społecznościowym. Badanym nie wskazano żadnych konkretnych czynności, aby czuli oni pełną swobodę działania w celu poznania ich przyzwyczajeń związanych z eksploracją informacji za pośrednictwem *social media*. Po zakończeniu respondenci uzupełnili kwestionariusz SUS.

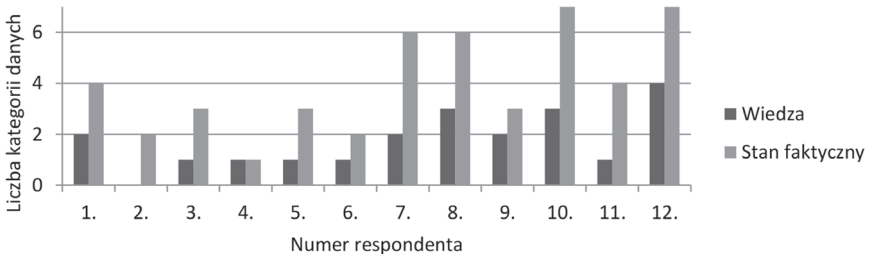
Ostatnim etapem badania była wspólna weryfikacja profilu osoby badanej pod kątem udostępnianych przez nią danych. Po niej moderator zadał kolejne pytania w ramach wywiadu pogłębionego, które zaprezentowano poniżej.

1. *Czy udostępnia Pan informacje o miejscu zamieszkania?*
2. *Czy udostępnia Pan informacje o zatrudnieniu?*
3. *Czy udostępnia Pan informacje o wykształceniu i umiejętnościach?*
4. *Czy udostępnia Pan informacje o członkach rodziny?*
5. *Czy korzysta Pan z opcji „meldowania się" w lokalizacjach?*
6. *Czy udostępnia Pan informacje o swoich zainteresowaniach?*
7. *Czy udostępnia Pan informacje o wydarzeniach, w którym brał lub planuje wziąć udział?*

Wyniki

Wykres 1.

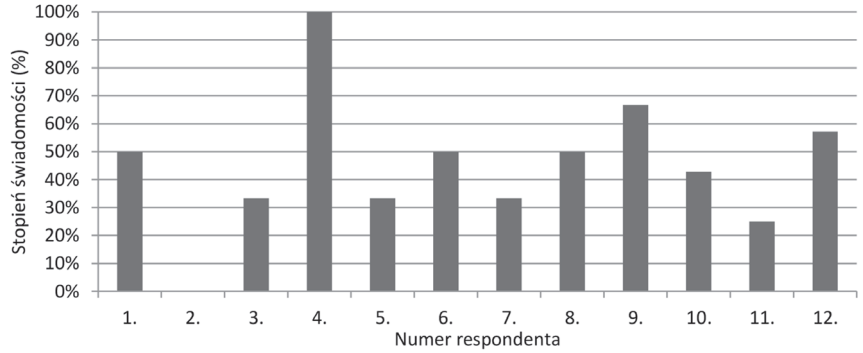
Stosunek poziomu wiedzy użytkowników do stanu faktycznego zagadnienia w aspekcie liczby kategorii danych udostępnianych w serwisie społecznościowym



Źródło: Opracowanie własne

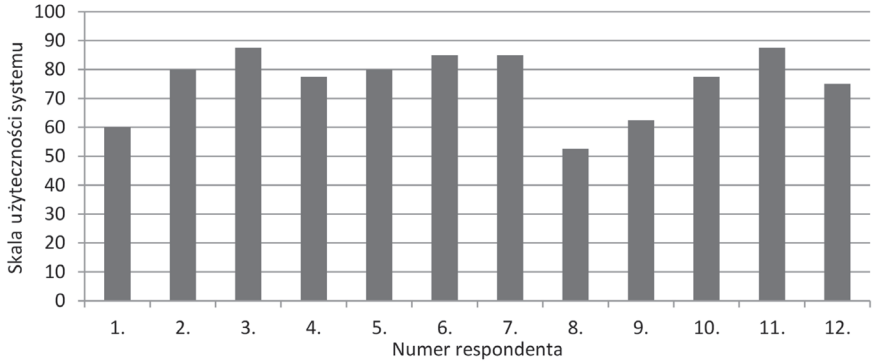
Wykres 2.

Poziom świadomości poszczególnych respondentów dotyczący udostępniania danych w serwisach społecznościowych



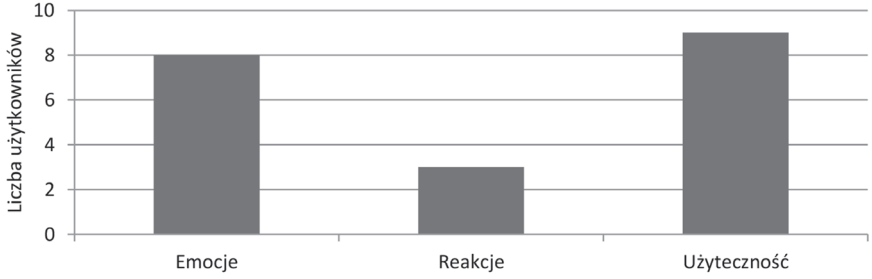
Źródło: Opracowanie własne

Wykres 3.
Skala użyteczności serwisu społecznościowego Facebook według poszczególnych respondentów



Źródło: Opracowanie własne

Wykres 4.
Wpływ składowych User Experience na uczestników badania



Źródło: Opracowanie własne

Podsumowanie

Na podstawie uzyskanych wyników, które zwizualizowano na wykresach 1 i 2, można wnioskować, że ponad połowa (55%) wszystkich danych zamieszczanych w serwisach społecznościowych jest udostępniana w sposób nieświadomy. Na tej podstawie orzeka się, że osiągnięto pierwszy postawiony cel badawczy, tj. określono stopień świadomości użytkowników w kwestii udostępniania przez nich danych w Internecie.

Ponadto poczyniony wywiad pogłębiony dostarczył informacje dotyczące tego, jakie cechy serwisów społecznościowych składają się na ich użyteczność i jednocześnie determinują użytkowników do udostępniania tam swoich danych. Na tej podstawie stwierdza się, że drugi cel badawczy został osiągnięty – scharakteryzowano *user experience* jako zagrożenie dla bezpieczeństwa cyfrowego, a szczególnie dla bezpieczeństwa użytkowników o niskiej świadomości.

Na podstawie analizy danych zwizualizowanych na wykresie 4 stwierdza się, że najsilniejszym czynnikiem zachęcającym użytkowników do udostępniania danych w serwisach społecznościowych jest ich użyteczność.

Z dokonanego przeglądu literatury, w ramach którego dokonano analizy danych udostępnianych przez Europejski Urząd Statystycznych (Eurostat), można stwierdzić, że w dobie egzystowania społeczeństwa informacyjnego udostępnianie danych w Internecie jest procesem nieuniknionym.

W nawiązaniu do poprzedniego stwierdzenia i przyjęcia hipotezy, że społeczeństwo może egzystować bez potrzeby transmisji danych – nieudostępnianie danych w użytecznych serwisach społecznościowych nie jest rozwiązaniem wskazanego w artykule problemu. Działania, których celem jest wzrost poziomu bezpieczeństwa cyfrowego społeczeństwa, powinny koncentrować się wokół budowania świadomości użytkowników Internetu, np. poprzez prowadzenie kampanii medialnych.

Literatura

Andrzejczak, J. (2015). *Interaktywna wizualizacja informacji wyszukanej w cyfrowych zbiorach danych*. Rozprawa doktorska, Politechnika Łódzka WFTIMS.

Boyce, C., Neale, P. (2006). *Conducting in-depth interviews: A Guide for Designing and Conducting In-Depth Interviews for Evaluation Input.* Pathfinder International Tool Series: Monitoring and Evaluation 2, May.

Brooke, J. (1996). *SUS: A „quick and dirty" usability scale.* Usability Evaluation In Industry, pp. 189-194, London.

Dudczyk, J. (2010). *Cyberterroryzm a bezpieczeństwo informacji w systemach teleinformatycznych*. Informatyczne metody wspomagania zarządzania (wybrane zagadnienia) – Zeszyt Naukowy WSIZiA, Warszawa, 5–17. ISSN 1641-9707.

Dudczyk, J. (2010). *Steganografia w aspekcie ochrony informacji w urządzeniach i systemach radioelektronicznych*". Informatyczne metody wspomagania zarządzania (wybrane zagadnienia) – Zeszyt Naukowy WSIZiA, Warszawa, s. 122–130. ISSN 1641-9707.

Dudczyk J., Matuszewski J. (2005). *Entropia informacyjna w aspekcie walki sieciocentrycznej*. I Konferencja Naukowa „Urządzenia i Systemy Radioelektroniczne", Soczewka. ISBN 8389399016.

Dudczyk, J., Klimkiewicz, Z. (2009). *Cyberterroryzm w aspekcie entropii informacji*. Konferencja Naukowa „Cyberterroryzm – nowe wyzwania XXI wieku" – praca zbiorowa pod redakcją T. Jemioły, J. Kisielnickiego, K. Rajchela, Warszawa, 18 maja 2009. ISBN 9788374622271.

European Statistical Office: *Digital economy and society statistics – households and individuals*. Eurostat regional yearbook 2018, pp. 127–138, August, 2018, DOI: 10.2785/231975. ISBN 9789279878787.

International Organization for Standardization: *ISO 9241-210:2010 Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems.* March, 2010.

International Organization for Standardization: *ISO 9241-11:2018 Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts.* March, 2018

Jezierski, Z., Dudczyk, J., Rybak, Ł. (2018). *Działania cybernetyczne w wojnie hybrydowej.* Międzynarodowa Konferencja Naukowa „Infrastruktura krytyczna w systemie bezpieczeństwa państwa i społeczeństwa" – II Nyskie Forum Bezpieczeństwa, 24–25 maja 2018 r., Nysa.

Kumar, A., Chaudhary, M., Kumar, N. (2015). *Social Engineering Threats and Awareness: A Survey*, European Journal of Advances in Engineering and Technology 2 (11), pp. 15–19, ISSN: 2394-658X.

Lewis, J.R., Sauro, J. (2009). *The Factor Structure of the System Usability Scale.* Human Centered Design, Lecture Notes in Computer Science, Vol. 5619, s. 94–103, Springer, Berlin, Heidelberg.

Mataracioglu, T., Ozkan, S. (2011). *User awareness measurement through social engineering*, arXiv preprint arXiv:1108.2149.

Rybak, Ł. (2017). *Analiza możliwości prezentacji cech wspólnych dużych zbiorów danych*. Praca magisterska, Politechnika Łódzka WFTIMS.

Rybak, Ł., Dudczyk, J., Jezierski, Z. (2018). *The IT sector as an important element of critical infrastructure*. Międzynarodowa Konferencja Naukowa „Infrastruktura krytyczna w systemie bezpieczeństwa państwa i społeczeństwa", Nysa, 24–25 May.

usability.gov: *System Usability Scale (SUS)*. Pozyskano (01.10.2018) z https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

Wiśniewski, R. (2013). *Społeczeństwo a kształtowanie bezpieczeństwa państwa*. Rocznik Towarzystwa Naukowego Płockiego 5, pp. 303–317. ISSN 0860-5637.

Workman, M. (2007). *Gaining Access with Social Engineering: An Empirical Study of the Threat.* Information Systems Security, Vol. 16, pp. 315-331, DOI: 10.1080/10658980701788165.

Zuckerberg, M. (2018). *Written Testimony to the House of Representatives,* June.