FOLIA 257

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 8 (2018)
ISSN 2082-0917
DOI 10.24917/20820917.8.13

Paulina Motylińska
Uniwersytet Pedagogiczny w Krakowie

Kształcenie w zakresie bezpieczeństwa informacji i ochrony prywatności w Internecie – oczekiwania studentów

Wstęp

Powszechne wykorzystanie nowoczesnych technologii, mnogość dostępnych źródeł informacji oraz obecność technologii informacyjno-komunikacyjnych w wielu dziedzinach życia takich jak gospodarka czy nauka, wymusza konieczność nieustannego kształcenia się członków społeczeństwa. Wzrost znaczenia wiedzy i edukacji jest także jedną z cech społeczeństwa informacyjnego. Zdobywanie i rozwijanie kompetencji informacyjnych i cyfrowych, które pozwalają na swobodne poruszanie się w świecie informacji i nowych technologii, jest istotne do efektywnego funkcjonowania we współczesnym społeczeństwie. Niewątpliwie naruszenia bezpieczeństwa informacji, szczególnie w środowisku Internetu, są coraz bardziej powszechne (np. według *Raportu o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku* liczba zgłoszeń incydentów komputerowych stale wzrasta[1], a firma Kaspersky Lab zajmująca się bezpieczeństwem systemów informatycznych informuje, że w drugim kwartale 2018 r. wykryła prawie 963 milionów cyberataków, co stanowi 20% więcej niż w pierwszym kwartale 2018 r.[2]), przez co posiadanie odpowiednich kompetencji w zakresie zarządzania bezpieczeństwem informacyjnym wydaje się być niezbędne. Znaczenie edukacji dla zapewnienia bezpieczeństwa, także bezpieczeństwa informacyjnego, wielokrotnie podkreślane jest w literaturze przedmiotu i dokumentach strategicznych. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) od lat wskazuje w swoich raportach na konieczność uwzględnienia aspektu edukacji w strategiach cyberbezpieczeństwa oraz promowania świadomości w zakresie bezpieczeństwa informacji i danych osobowych[3].

[1] CERT, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku*, 2017, Warszawa, https://www.csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/ 958,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2017-roku.html [dostęp: 04.09.2018].

[2] Kaspersky Lab, *Szkodliwe programy w II kwartale 2018 r.: Polska w czołówce krajów z największą liczbą mobilnych trojanów bankowych*, 06.08.2018, https://www.kaspersky.pl/o-nas/informacje-prasowe/2998/szkodliwe-programy-w-ii-kwartale–2018-r-polska-w-czolowce-krajow-z-najwieksza-liczba-mobilnych-trojanow-bankowych [dostęp: 04.09.2018].

[3] ENISA, *Collaborative Solutions For Network Information Security in Education*, 2012, https://www.enisa.europa.eu/publications/collaborative-solutions-for-network-information-security-in-education [dostęp: 30.09.2018].

Artykuł prezentuje propozycję zajęć „Bezpieczeństwo informacji i ochrona prywatności w Internecie", realizowanych w ramach nieobligatoryjnego kursu ogólnouczelnianego na Uniwersytecie Pedagogicznym im. Komisji Edukacji Narodowej w Krakowie w roku akademickim 2017/2018. Tematyka zajęć została opracowana na podstawie wybranych modeli kształcenie kompetencji informacyjnych i cyfrowych oraz porównana z zidentyfikowanymi oczekiwaniami edukacyjnymi uczestników kursu. Na początku zajęć (w marcu 2018 r.) wszyscy uczestnicy kursu zostali poproszeni o sformułowanie wypowiedzi na forum dyskusyjnym działającym w ramach platformy e-learningowej Uniwersytetu Pedagogicznego. Udział w dyskusji wzięło 31 osób. Studenci udzielili odpowiedzi na pytanie dotyczące szczególnie dla nich interesujących zagadnień związanych z bezpieczeństwem informacji i ochroną prywatności w Internecie, które chcieliby szerzej omówić w trakcie zajęć. Analiza wypowiedzi studentów została zawarta w artykule. Poznanie oczekiwań studentów względem zawartości merytorycznej kursu jest pierwszym etapem zmian udoskonalających program kursu, tak, aby dostosować go do potrzeb i zainteresowań jego uczestników.

Modele i standardy kształcenia

W celu usprawnienia i udoskonalenia procesów edukacyjnych w zakresie zdobywania kompetencji informacyjnych i cyfrowych tworzy się modele i standardy kształcenia oraz katalogi ramowe. Wykorzystanie modeli, standardów i katalogów pozwala m.in. na łatwiejsze zaplanowanie procesu edukacyjnego oraz zidentyfikowanie potrzeb i luk w wiedzy uczniów i studentów. Modele, standardy i katalogi mogą także bezpośrednio pomóc w określeniu tematyki i celów zajęć edukacyjnych. W wielu modelach kształcenia kompetencji cyfrowych (w przeciwieństwie do modeli kształcenie kompetencji informacyjnych[4]) uwzględnione zostały grupy kompetencji powiązanych z bezpieczeństwem i ochroną prywatności w Internecie.

W Programie Ramowym Kompetencji Cyfrowych DigComp 2.1. (ang. *The Digital Competence Framework for Citizens*) z 2017 r., który powstał w ramach unijnego projektu DigComp, kompetencje cyfrowe zostały podzielone na pięć głównych obszarów[5]. Jednym z tych obszarów jest właśnie „bezpieczeństwo". W DigComp 2.1 kompetencje w zakresie zapewnienia bezpieczeństwa obejmują m.in. umiejętność zabezpieczenia urządzeń elektronicznych (np. mobilnych), ochrony informacji, danych osobowych i prywatności w Internecie oraz dbanie o zdrowie i środowisko podczas korzystania z technologii cyfrowych[6].

---

[4] P. Motylińska, *Zarządzanie bezpieczeństwem informacji jako element kompetencji informacyjnych i cyfrowych*, [w:] *Kultura informacyjna w ujęciu interdyscyplinarnym: teoria i praktyka.* T. 2, Batorowska H., Kwiasowski Z. (red.), Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie. Instytut Bezpieczeństwa i Edukacji Obywatelskiej. Katedra Kultury Informacyjnej i Zarządzania Informacją, Kraków 2016, s. 201–210.

[5] S. Carretero, R. Vuorikari, Y. Punie, *DigComp 2.1. The Digital Competence Framework for Citizens: with eight proficiency levels and examples of use*, Publications Office of the European Union, Luxembourg 2017.

[6] Ibidem, s. 36–39.

Jednym z kompleksowych polskich opracowań zawierającym wykaz kompetencji, które są istotne dla współczesnego człowieka, jest Katalog Kompetencji Medialnych, Informacyjnych i Cyfrowych[7]. Katalog został opracowany przez Fundację Nowoczesna Polska, a najnowsza wersja Katalogu pochodzi z 2014 r. Wykaz kompetencji dotyczących bezpieczeństwa i ochrony prywatności w Internecie można znaleźć w dwóch działach: „bezpieczeństwo" i „mobilne bezpieczeństwo". Kompetencje medialne, informacyjne i cyfrowe w zakresie bezpieczeństwa obejmują m.in. umiejętność zachowania odpowiedniego poziomu anonimowości i prywatności w sieci, stosowanie podstawowych zasad bezpiecznego korzystania z mediów (w tym z Internetu) oraz dbałość o bezpieczne korzystanie z urządzeń mobilnych. W każdej z tych grup znajdziemy wykaz kompetencji dla osób będących na różnych poziomach edukacji, także dla studentów. W Katalogu wyróżniono także „standard edukacji medialnej, informacyjnej i cyfrowej", czyli zbiór kompetencji, które powinien posiadać dorosły człowiek funkcjonujący we współczesnym świecie. Standard ten wydaje się być szczególnie pomocny przy ustalaniu celów i efektów kształcenia dla kursów przeznaczonych dla studentów.

Ramowy Katalog Kompetencji Cyfrowych opracowany przez grupę polskich badaczy w 2015 r.[8] jest kolejnym przykładem narzędzia przydatnego w planowaniu zajęć edukacyjnych i szkoleń. Katalog został podzielony na 9 podstawowych obszarów (takich jak m.in. edukacja, sprawy codzienne i finanse), w których wykorzystanie określonych kompetencji cyfrowych może przynieść wymierne korzyści, np. umiejętność wypełnienia i złożenia zeznania podatkowego drogą elektroniczną powoduje wymierną korzyść – brak konieczności wychodzenia z domu w celu załatwienia spraw urzędowych[9]. W Katalogu nie wyodrębniono obszaru związanego z bezpieczeństwem, jednak jedną z określonych korzyści posiadania i wykorzystywania kompetencji cyfrowych jest dbanie o prywatność podczas korzystania z mediów cyfrowych[10]. Zgodnie z Ramowym Katalogiem, osoba kompetentna cyfrowo potrafi m.in. korzystać z trybu prywatnego w przeglądarkach i ustawień prywatności w mediach społecznościowych. Twórcy Katalogu zwracają także uwagę na to, że bezpieczeństwo w korzystaniu z technologii cyfrowych ma istotne znaczenie dla procesu rozwijania kompetencji cyfrowych[11].

Konkretne kompetencje dotyczące bezpieczeństwa informacyjnego (np. umiejętność zabezpieczenia urządzeń cyfrowych, ochrony prywatności w Internecie, korzystanie z ustawień prywatności i trybu prywatnego) zawarte w modelach, standardach kształcenia oraz katalogach ramowych kompetencji są dobrym wyznacznikiem do określania treści realizowanych podczas zajęć dydaktycznych.

---

[7] Fundacja Nowoczesna Polska, *Katalog Kompetencji Medialnych, Informacyjnych i Cyfrowych*, 2014, http://edukacjamedialna.edu.pl/media/chunks/attachment/ Katalog_kompetencji_medialnych_2014.pdf [dostęp: 01.09.2018].

[8] J. Jasiewicz i in., *Ramowy Katalog Kompetencji Cyfrowych, Centrum Cyfrowe Projekt Polska*, Warszawa 2015, https://mc.bip.gov.pl/rok–2015/ ramowy-katalog-kompetencji-cyfrowych.html [dostęp: 01.09.2018].

[9] Ibidem, s. 11.

[10] Ibidem, s. 20–21.

[11] Ibidem, s. 62–64.

Oczekiwania studentów

W ramach kursu „Bezpieczeństwo informacji i ochrona prywatności w Internecie" realizowanego w formie zajęć ogólnouczelnianych na Uniwersytecie Pedagogicznym w Krakowie w roku akademickim 2017/2018 poproszono studentów o wskazanie tematów związanych z bezpieczeństwem informacji i ochroną prywatności w Internecie, które są dla nich szczególnie interesujące, i jednocześnie – które chcieliby szerzej omówić na zajęciach. Na forum dyskusyjnym na platformie e-learningowej zebrano wypowiedzi 31 studentów. Wypowiedzi przeanalizowano i pogrupowano tematycznie. Część studentów wskazywała więcej niż jeden interesujący dla nich temat. Wypowiedzi studentów można podzielić według następujących tematów:

- Bezpieczeństwo w kontekście korzystania z mediów społecznościowych.
- Kradzież tożsamości.
- Zagrożenia w Internecie.
- Podpis elektroniczny.
- Ochrona danych osobowych.
- Inwigilacja w Internecie i pozyskiwanie informacji przez służby.
- Bezpieczeństwo mobilne.

W tabeli 1 zaprezentowano wybór wypowiedzi studentów dotyczących interesujących dla nich zagadnień z zakresu bezpieczeństwa informacji i ochrony prywatności w Internecie. Wypowiedzi zostały pogrupowane tematycznie i prezentowane są w oryginalnym brzmieniu.

Tabela 1. Tematy, które studenci chcieliby omówić na zajęciach z bezpieczeństwa informacji i ochrony prywatności w Internecie – wybór wypowiedzi studentów

1. Bezpieczeństwo w kontekście korzystania z mediów społecznościowych
Jeśli chodzi o temat, który chciałabym omówić ochronę danych w portalach społecznościowych.
Chciałabym zgłębić swoją wiedzę w zakresie bezpieczeństwa danych na popularnych portalach społecznościowych.
Jeśli chodzi o temat, który bym chciał, żeby został poruszony na zajęciach, to o serwisach typu, Facebook, Twitter itp.
Temat, jaki chciałabym omówić na zajęciach to ochrona naszych danych na portalach społecznościowych (np. Facebook, Instagram).
Chciałabym, aby na zajęciach została poruszona kwestia naszych danych w portalach społecznościowych i co należy robić, aby nie zostały one wykorzystane w niewłaściwy sposób.
Jak uchronić się przed niewłaściwym wykorzystywaniem danych osobowych przez portale społecznościowe.
Tematem, który mnie interesuje jest udostępnianie profili m.in. facebookowych czy instagramowych wielu aplikacjom. Czy jest to bezpieczne, mimo ze niewiele informacji o mnie widnieje na profilu podstawowym?
2. Kradzież tożsamości
Jak walczyć z kradzieżą tożsamości w internecie.

Ponieważ na własnej skórze doświadczyłam kradzieży tożsamości, chciałabym dowiedzieć się, co możemy zrobić, aby chociaż w niewielkim stopniu zwiększyć swoje bezpieczeństwo i uniemożliwić innym osobom ingerencję w tą sferę.

Na tych zajęciach również chciałabym się dowiedzieć jak uchronić nas od kradzieży naszej tożsamości.

3. Zagrożenia w Internecie

Chciałbym mieć większą wiedzę na temat zagrożeń, jakie czekają na mnie w sieci. Nie znam wszystkich, ponieważ ludzie potrafią wymyślać coraz bardziej wyrafinowane sposoby pozyskiwania moich danych.

Na zajęciach chciałbym dowiedzieć się o zagrożeniach, jakie czekają na nas w internecie.

Ważnym tematem jest właśnie znajomość możliwych, potencjalnych zagrożeń, jakie mogą czekać na nas korzystając z Internetu tzn. zwrócić uwagę na to, co może nam zagrażać i wypływać z sieci, a także z czego nie korzystać, na jakie strony nie wchodzić i na co zwracać uwagę, aby sobie nie zaszkodzić, poprzez np. ściągnięcie na swój komputer czy inne urządzenie wirusa lub dać komuś pełny dostęp do naszych prywatnych danych.

Na zajęciach chciałbym poznać sposoby, dzięki którym są wykradane nasze dane, myślę że taka wiedza pomoże mi zabezpieczyć się w przyszłości.

4. Podpis elektroniczny

Jeśli chodzi o materiał, który mnie interesuje i chciałbym, aby został poruszony na zajęciach szerzej to dotyczy on podpisu cyfrowego.

Temat, który mnie interesuje to: elektroniczny podpis, czy jest to bezpieczna metoda podpisywania dokumentów przez Internet oraz czy łatwo jest wykraść dane i wykorzystać ten podpis.

5. Ochrona danych osobowych

Na zajęciach chciałbym uzyskać więcej informacji na temat ochrony swoich danych osobowych.

6. Inwigilacja w Internecie i pozyskiwanie informacji przez służby

Interesuje mnie, jak wielką możliwość inwigilacji mają służby bezpieczeństwa, a także wielkie międzynarodowe korporacje jak Google czy Facebook.

Chciałbym omówić temat „Użycie prywatnych danych z sieci przez służby specjalne".

Chciałbym się więcej dowiedzieć o metodach inwigilacji stosowanych przez Google.

Ciekawi mnie temat, ile informacji inwigilują takie witryny jak Facebook, Twitter itp. Czy i gdzie informacje, które tam udostępniamy są wykorzystywane.

7. Bezpieczeństwo mobilne

Tematy z bezpieczeństwa, które mnie interesują to ochrona danych i ogólnie ochrona telefonów komórkowych i zagrożenia związane właśnie z urządzeniami mobilnymi.

Źródło: opracowanie własne 2018

Zagadnieniem, które zdecydowanie najczęściej pojawiało się w wypowiedziach studentów (wystąpiło w 1/3 wszystkich wypowiedzi) jest bezpieczeństwo w kontekście korzystania z mediów społecznościowych. Studenci chcieliby wiedzieć, w jaki sposób mogą zadbać o bezpieczeństwo informacji publikowanych w serwisach społecznościowych oraz w jaki sposób publikowane przez nich informacje i materiały mogą zostać wykorzystane np. przez podmioty współpracujące z danym serwisem. Odsetek młodych osób korzystających z portali społecznościowych, szczególnie z Facebooka, jest bardzo wysoki (wg raportu GUS „Społeczeństwo informacyjne w Polsce" w 2017 r. aż 92,6% uczniów i studentów w Polsce biorących udział

w badaniu deklarowało korzystanie z serwisów społecznościowych[12]), dlatego nie dziwi więc zainteresowanie studentów kwestią bezpieczeństwa w tym kontekście.

Studenci zadeklarowali również zainteresowanie tematyką kradzieży tożsamości w Internecie, a w szczególności – ochroną przed tego typu zagrożeniem. Jedna ze studentek stwierdziła nawet, że w przeszłości doświadczyła kradzieży tożsamości. Nierozważne publiczne udostępnianie prywatnych informacji i danych osobowych m.in. w mediach społecznościowych może zwiększać ryzyko kradzieży tożsamości. Wydaje się zatem, że w trakcie zajęć warto omówić ze studentami powiązania między bezpiecznym korzystaniem z mediów społecznościowych a ochroną przed kradzieżą tożsamości.

Studenci chcieliby również wiedzieć więcej na temat potencjalnych zagrożeń, które związane są z użytkowaniem Internetu. Wśród szczególnie interesujących dla nich zagrożeń studenci wymieniali nieuprawnione pozyskiwanie danych osobowych i prywatnych informacji. Kilkoro studentów w swoich wypowiedziach uwzględniło także zagadnienie podpisu cyfrowego i poziomu bezpieczeństwa danych chronionych takim podpisem.

Można zauważyć także znaczne zainteresowanie studentów tematyką wykorzystywania Internetu, w tym mediów społecznościowych, przez służby specjalne w celu pozyskiwania informacji oraz zagadnieniem gromadzenia danych o użytkownikach przez popularne serwisy i usługi internetowe (np. Facebook, Google).

W zestawieniu tematów zajęć wymienionych przez studentów pojawił się także temat bezpieczeństwa technologii mobilnych. Bezpieczeństwo urządzeń i aplikacji mobilnych jest istotnym zagadnieniem z punktu widzenia bezpieczeństwa informacyjnego, a jak wynika z badania dotyczącego technologii mobilnych przeprowadzonego wśród studentów przez Tomasza Parysa[13], 59% badanych studentów obawia się utraty danych podczas korzystania z technologii mobilnych, a 51% – bycia śledzonym lub inwigilowanym. Sposobem na zmniejszenie tych obaw może być właśnie odpowiednia edukacja.

Propozycja tematyki zajęć „Bezpieczeństwo informacji i ochrona prywatności w Internecie"

Sylabus zajęć „Bezpieczeństwo informacji i ochrona prywatności w Internecie" został opracowany przed poproszeniem studentów o wskazanie zagadnień, które chcieliby omówić, jednak można zauważyć, że tematyka zajęć (zaprezentowana w tabeli 2) w dużej mierze pokrywa się z zidentyfikowanymi oczekiwaniami uczestników kursu. Podczas realizowania poszczególnych bloków zagadnień, prezentowano studentom rzeczywiste przykłady naruszeń bezpieczeństwa w sieci oraz

[12] Główny Urząd Statystyczny, *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2013–2017*, Warszawa, Szczecin 2017, s. 135. http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-wyniki-badan-statystycznych-z-lat-2013-2017,1,11.html [dostęp: 01.09.2018].

[13] T. Parys, *Technologie mobilne – bariery zastosowań w ocenie użytkowników indywidualnych – wyniki badań 2016*, „Studia Informatica Pomerania" 2016, nr 3(41), s. 22.

podawano wykazy dodatkowych lektury, tak, aby studenci mogli rozszerzyć swoją wiedzę w zakresie szczególnie dla nich interesujących tematów. Omówiono kwestie ochrony prywatności podczas korzystania z mediów społecznościowych, wskazano potencjalne zagrożenia dla bezpieczeństwa w sieci oraz poinstruowano studentów, w jaki sposób mogą zadbać o odpowiedni poziom bezpieczeństwa podczas korzystania z Internetu. Na zajęciach pominięto jednak zagadnienie pozyskiwania informacji z Internetu przez służby specjalne – uznano, że tematyka wywiadu i analizy informacji w tym kontekście nie wpisuje się w cele ogólnouczelnianego kursu nastawionego na rozwijanie podstawowych kompetencji cyfrowych studentów. Po analizie wypowiedzi studentów można jednak wnioskować, że kurs dotyczący działalności służb specjalnych wzbudziłby zainteresowanie.

Tabela 2: Tematyka zajęć „Bezpieczeństwo informacji i ochrona prywatności w Internecie"

	Bezpieczeństwo informacji i ochrona prywatności w Internecie – tematy zajęć
1.	Wprowadzenie do zagadnień bezpieczeństwa informacji i ochrony prywatności w Internecie. Stosowana terminologia, problemy definicyjne, podstawowa literatura.
2.	Potencjalne zagrożenia dla bezpieczeństwa informacji i prywatności w Internecie, zagrożenia wynikające z rozwoju technologii informacyjnej, przestępczość komputerowa (cyberprzestępczość), m.in. wyłudzanie informacji, *skimming*, *phishing*, wyciek informacji.
3.	Socjotechniki a bezpieczeństwo informacji – manipulacje stosowane przy wyłudzaniu informacji.
4.	Cyfrowe ślady, dane nieświadomie pozostawiane w Internecie, dane gromadzone przez wyszukiwarki.
5.	Prywatność w mediach społecznościowych – udostępnianie danych osobowych i prywatnych informacji, ustawienia prywatności, regulaminy.
6.	Hasła dostępu do kont elektronicznych – statystyki dotyczące najczęściej wykorzystywanych haseł, zasady budowania skutecznych haseł dostępu.
7.	Zasady bezpiecznego korzystania z Internetu w praktyce – jak dbać o prywatność w sieci, chronić swoje dane i udostępniane informacje.

Źródło: opracowanie własne 2018

Podsumowanie

Porównanie zawartości merytorycznej kursu „Bezpieczeństwo informacji i ochrona prywatności w Internecie", zaprojektowanego z wykorzystaniem modeli i katalogów ramowych kompetencji cyfrowych, z wykazem interesujących dla studentów tematów wskazało, że treści kursu nie odbiegały znacznie od oczekiwań studentów. Modele i standardy kształcenia kompetencji informacyjnych i cyfrowych mogą zatem stanowić efektywne narzędzie wykorzystywane do projektowania kursów edukacyjnych.

Przedstawiony w artykule kurs ogólnouczelniany miał na celu przekazanie studentom podstawowej wiedzy i umiejętności w zakresie ochrony bezpieczeństwa informacji i prywatności w Internecie, pozwalających na dostrzeganie zagrożeń dla bezpieczeństwa informacji i zastosowanie wybranych technik ochrony w codziennym życiu osobistym i zawodowym. Po ukończeniu kursu student powinien aktywnie wykorzystywać podstawowe narzędzia i techniki ochrony informacji

i prywatności w Internecie, w tym m.in. budować odpowiednio silne hasła dostępu do kont elektronicznych oraz zadbać o zapewnienie sobie odpowiedniego poziomu prywatności w Internecie (np. podczas korzystania z mediów społecznościowych i narzędzi wyszukiwania informacji). Studenci oceniający zakończone zajęcia stwierdzili m.in. że „kurs jest doskonałym przypomnieniem na jakie zagrożenia możemy natrafić przez nieuwagę oraz brak rozwagi", „wiedza zdobyta na kursie uświadomiła mi, że dla bezpieczeństwa w sieci warto poświęcić chwilę uwagi i przeczytać regulamin, zanim się go zaakceptuje" i „kurs uświadomił mi, że nie stosuję się do wszystkich zasad bezpiecznego korzystania z Internetu".

Znaczenie odpowiedniej edukacji dla zapewnienia bezpieczeństwa, także bezpieczeństwa informacji i bezpieczeństwa podczas korzystania z technologii cyfrowych, jest niewątpliwie wysokie. Do oceny potrzeb edukacyjnych, projektowania programów kształcenia i materiałów edukacyjnych, planowania szkoleń i samooceny kompetencji informacyjnych i cyfrowych warto natomiast wykorzystywać opracowane już modele i standardy kształcenia. Jak wynika z przeanalizowanych wypowiedzi uczestników kursu „Bezpieczeństwo informacji i ochrona prywatności w Internecie" studenci wyrażają chęć poszerzania swojej wiedzy i zdobywania nowych umiejętności w zakresie zapewnienia bezpieczeństwa informacyjnego w środowisku Internetu.

Bibliografia

Carretero, S., Vuorikari, R., Punie, Y., *DigComp 2.1. The Digital Competence Framework for Citizens: with eight proficiency levels and examples of use*, Publications Office of the European Union, Luxembourg 2017.

CERT, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku*, 2017, Warszawa, https://www.csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/ 958,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2017-roku.html [dostęp: 04.09.2018].

ENISA, *Collaborative Solutions For Network Information Security in Education*, 2012, https://www.enisa.europa.eu/publications/ collaborative-solutions-for-network-information-security-in-education [dostęp: 30.09.2018].

Fundacja Nowoczesna Polska, *Katalog Kompetencji Medialnych, Informacyjnych i Cyfrowych*, 2014, http://edukacjamedialna.edu.pl/media/chunks/attachment/ Katalog_kompetencji_medialnych_2014.pdf [dostęp: 01.09.2018].

Główny Urząd Statystyczny, *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2013–2017*, Warszawa, Szczecin 2017, http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/ spoleczenstwo-informacyjne-w-polsce-wyniki-badan-statystycznych-z-lat–2013–2017,1,11.html [dostęp: 01.09.2018].

Jasiewicz, J. i in., *Ramowy Katalog Kompetencji Cyfrowych, Centrum Cyfrowe Projekt Polska*, Warszawa 2015, https://mc.bip.gov.pl/rok–2015/ramowy-katalog-kompetencji-cyfrowych.html [dostęp: 01.09.2018].

Kaspersky Lab, *Szkodliwe programy w II kwartale 2018 r.: Polska w czołówce krajów z największą liczbą mobilnych trojanów bankowych*, 06.08.2018, https://www.kaspersky.pl/o-nas/informacje-prasowe/2998/ szkodliwe-programy-w-ii-kwartale-2018-r-polska-w-czolowce-krajow-z-najwieksza-liczba-mobilnych-trojanow-bankowych [dostęp: 04.09.2018].

Motylińska P., *Zarządzanie bezpieczeństwem informacji jako element kompetencji informacyjnych i cyfrowych*, [w:] *Kultura informacyjna w ujęciu interdyscyplinarnym: teoria i praktyka.* T. 2, Batorowska H., Kwiasowski Z. (red.), Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie. Instytut Bezpieczeństwa i Edukacji Obywatelskiej. Katedra Kultury Informacyjnej i Zarządzania Informacją, Kraków 2016.

Parys T., *Technologie mobilne – bariery zastosowań w ocenie użytkowników indywidualnych – wyniki badań 2016*, „Studia Informatica Pomerania" 2016, nr 3(41).

Education in the field of information security and protection of privacy on the Internet – students' expectations

Abstract

The article presents the „Information security and privacy protection on the Internet" course content. The course was offered by the Pedagogical University of Cracow. Topics covered in the course have been designed based on information and digital literacy standards and then confronted with students' expectations. Students were asked which topics they would like to discuss in class, so the article includes the analysis of students' statements regarding their interests in information security and privacy protection on the Internet.

Słowa kluczowe: bezpieczeństwo informacji, Internet, kompetencje cyfrowe, kształcenie wyższe

Keywords: information security, Internet, digital literacy, higher education

Paulina Motylińska
Asystent w Instytucie Bezpieczeństwa i Edukacji Obywatelskiej Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie. Zainteresowania naukowe: zarządzanie bezpieczeństwem informacji, kompetencje informacyjne i cyfrowe.