Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej Nr 52

IV Konferencja

eTechnologie w Kształceniu Inżynierów eTEE'2017

Politechnika Gdańska, 27-28 kwietnia 2017

NAUCZANIE ZAGADNIEŃ CYBERBEZPIECZEŃSTWA W UNII EUROPEJSKIEJ – TRENDY, WYZWANIA

Rafał LESZCZYNA

Politechnika Gdańska, Wydział Zarządzania i Ekonomii
e-mail: rle@zie.pg.gda.pl

Streszczenie: Znaczenie edukacji, szkoleń i podnoszenia świadomości zagadnień cyberbezpieczeństwa jest dziś, w erze społeczeństwa informacyjnego powszechnie uznane. W ostatnich latach w Unii Europejskiej pojawiło się wiele nowych inicjatyw związanych między innymi z rozwijaniem programów uniwersyteckich, przygotowywaniem specjalistycznych i profilowanych szkoleń, uruchamianiem masowych otwartych kursów online, a także badaniami opinii publicznej oraz ekspertów. Odbyła się również niezwykle interesująca debata dotycząca skuteczności i zasadności kształcenia zasad cyberbezpieczeństwa oraz przeprowadzono ankietę w instytucjach edukacyjnych dotyczących cech wzorcowego kursu w tej dziedzinie. W artykule przedstawiono te inicjatywy i związane z nimi wyzwania, a także trendy i perspektywiczne kierunki rozwoju nauczania zagadnień cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo, bezpieczeństwo informacji, nauczanie, podnoszenie świadomości, masowe otwarte kursy online.

1. WPROWADZENIE

Internet oraz technologie informacyjne stały się nieodłącznym składnikiem życia codziennego, a zarazem elementem definiującym współczesne społeczeństwo, związanym z powstaniem nowego nurtu społecznego nazywanego *społeczeństwem wiedzy*, lub *społeczeństwem informacyjnym*. Nurt ten charakteryzuje się przewagą treści symbolicznych nad materialnymi oraz znacząco zwiększonymi możliwościami kreowania i przetwarzania informacji, gdzie wiedza oraz umiejętności jej wykorzystywania odgrywają kluczową rolę przy podejmowaniu decyzji i wprowadzaniu zmian. Ewolucyjnym rozwinięciem społeczeństwa wiedzy jest *społeczeństwo sieciowe*, podkreślające dodatkowo dominującą rolę struktur sieciowych w organizacji społeczeństwa [1, 2].

Obok wielu korzyści związanych z nowym nurtem społecznym, takich jak zwiększenie możliwości komunikacyjnych, czy wzrost zasięgu demokracji bezpośredniej (tzw. „cyberdemokracja"), pojawiły się również wyzwania dotyczące między innymi umiejętności niezbędnych do prawidłowego funkcjonowania i pracy. Dla przykładu, rynek pracy społeczeństwa informacyjnego cechuje się dużym zapotrzebowaniem na specjalistów z branży IT, które wciąż znacząco przewyższa możliwości dostarczenia specjalistów przez system edukacyjny. Potrzebne są też nowe umiejętności niezwiązane z pracą czy kompetencjami zawodowymi, ale z codziennym życiem. Narodziny Internetu Rzeczy, inteligentnych samochodów, mieszkań, sieci energetycznych, etc. wymagają umiejętności obsługi urządzeń mobilnych i nowych technologii w codziennych czynnościach [1, 2]. *E-umiejętności* to „umiejętności wykorzystywania i posługiwania się w życiu codziennym oraz działalności społecznej i gospodarczej technologiami informacyjnymi. Pojęcie e-umiejętności obejmuje kompetencje w zakresie tworzenia i użytkowania technologii informacyjnych i komunikacyjnych" [3]. Udane innowacje w sektorze IT wymagają interdyscyplinarnych umiejętności rozwiązywania problemów, dobrego zrozumienia zagadnień związanych z przedsiębiorczością, zdolności komunikacyjnych, w tym znajomość języków obcych. W szerszym kontekście można je rozpatrywać jako kluczowe kompetencje wszystkich obywateli w społeczeństwie wiedzy. Te kluczowe kompetencje powinny zostać dostarczone w ramach kształcenia ustawicznego. Edukacja i szkolenia są kluczowymi instrumentami kształcenia e-umiejętności i wyrównywania różnic w funkcjonowaniu w społeczeństwie wiedzy [1].

Kwestią, która nabrała szczególnie dużego znaczenia w społeczeństwie informacyjnym, jest *bezpieczeństwo informacyjne*, lub *cyberbezpieczeństwo* związane między innymi z ochroną prywatności, czy danych osobowych [1]. Informacje są bezpieczne, gdy zapewniono ich *poufność*, *integralność* i *dostępność*. Poufność dotyczy zagwarantowywania, że informacja jest dostępna wyłącznie dla osób do tego upoważnionych, a dostępność, że upoważnieni użytkownicy posiadają dostęp do informacji i powiązanych zasobów, kiedy istnieje taka potrzeba. Natomiast informacja jest integralna, gdy: odpowiada rzeczywistości i jest kompletna [4]. Innymi słowy, informacja jest nieuszkodzona, niezniekształcona.

Badania Eurobarometru [5] ujawniły, że jedynie mniej niż połowa (47%) obywateli Unii Europejskiej uważa, że jest dobrze poinformowana o zagrożeniach cyberbezpieczeństwa [5]. Badania ujawniły też różnice socjodemograficzne związane z dostępem do Internetu w zależności od wieku użytkowników, poziomu ich edukacji i zatrudnienia. 83% badanych, którzy zakończyli edukację w wieku 20 lat lub więcej korzysta z Internetu codziennie, a już tylko 60% w przypadku ukończenia edukacji między 16 a 19 rokiem życia i 23% poniżej 16 lat. Większe wykorzystanie

Internetu obserwuje się także wśród studentów i pracowników biurowych. 95% studentów, 91% kadry kierowniczej i 85% pozostałych pracowników biurowych codziennie korzysta z Internetu. Niezależnie od wieku, profilu zawodowego, czy poziomu wykształcenia wszyscy powinni mieć zagwarantowane bezpieczeństwo podczas korzystania z usług online dzięki uświadomieniu potencjalnych zagrożeń oraz zapewnieniu adekwatnych umiejętności [6]. Tymczasem znajomość zagadnień cyberbezpieczeństwa wciąż pozostaje w rękach specjalistów pomimo tego, że pierwszą linią obrony przed cyber zagrożeniami jest uświadamianie wszystkich użytkowników i zdobywanie przez nich umiejętności ochrony urządzeń, danych, czy tożsamości online. [6, 7].

Edukacja jest kluczowym elementem cyberbezpieczeństwa, co zostało potwierdzone w Europejskiej Agendzie Cyfrowej oraz strategiach cyberbezpieczeństwa państw członkowskich [1]. Zalecane jest traktowanie cyberbezpieczeństwa jako dobra publicznego [8]. W tym podejściu instytucje ustawodawcze i wykonawcze powinny ustanowić standardy oraz uregulowania prawne dotyczące działań cyberbezpieczeństwa na tej samej zasadzie jak propagowane są procedury i praktyki ochrony zdrowia. Jednostki edukacyjne mają tutaj kluczową rolę w podnoszeniu świadomości wśród obywateli i kształtowaniu właściwych zachowań związanych z bezpieczeństwem. Zagadnienia cyberbezpieczeństwa powinny stać się częścią akademickich programów kształcenia. Zalecane jest włączenie do ogólnego programu kształcenia nauczania zasad i wyzwań bezpieczeństwa informacji i prywatności [9].

2. DYSKUSJA O NAUCZANIU ZAGADNIEŃ CYBERBEZPIECZEŃSTWA

W 2013 roku miała miejsce niezwykle ciekawa dyskusja między Bruce Schneierem a Irą Winkelerem dotycząca celowości i zasadności prowadzenia szkoleń oraz podnoszenia świadomości z zakresu bezpieczeństwa informacji [10, 11]. Schneier i Winkler są ekspertami z dziedziny cyberbezpieczeństwa, autorami książek opisujących zagadnienia bezpieczeństwa oraz kryptografii, które stały się fundamentalnymi przewodnikami w dziedzinie bezpieczeństwa informacyjnego zarówno dla ekspertów jak i zwykłych użytkowników na całym świecie.

Według Bruce Schneiera szkolenia w zakresie bezpieczeństwa są stratą czasu, a środki finansowe idące na ten cel, mogłyby być lepiej spożytkowane w innych obszarach. Zdaniem eksperta zainteresowanie przemysłu szkoleniami służy odwróceniu uwagi od źle zaprojektowanych systemów bezpieczeństwa [11]. Na poparcie swoich dość kontrowersyjnych tez, Schneier wskazuje przykłady z życia codziennego, związane z propagowaniem zdrowego trybu życia, czy walki z AIDS, które odnosi do dziedziny bezpieczeństwa. Według autora, problem z edukacją cyberbezpieczeństwa związany jest między innymi z faktem, że w codziennym użytkowaniu komputera, potencjalne efekty niewłaściwych zachowań, wydają się być abstrakcyjne i mało prawdopodobne, a z drugiej strony stosowanie dobrych praktyk bezpieczeństwa jest czasochłonne i wymaga podejmowania niełatwych decyzji. Scheier uważa, że zamiast uczyć użytkowników bezpiecznych procedur korzystania z komputerów i Internetu, należy budować bezpieczne komputery i tak zarządzać Internetem by był on bezpieczny. Zdaniem specjalisty, gdyby inżynierowie bezpieczeństwa wykonali to zadanie, kształcenie i poszerzanie świadomości użytkowników odbywałoby się samoistnie i nieformalnie, bez potrzeby kursów, na zasadzie wzajemnego uczenia się od siebie [11].

W odpowiedzi, Ira Winkler po pierwsze zwraca uwagę na różnicę między szkoleniem a podnoszeniem świadomości, gdyż Schneier używa dość mylącego terminu „szkolenie świadomości bezpieczeństwa" (ang. „security awareness training"). Zadaniem szkoleń jest dostarczenie pewnego ograniczonego zbioru wiedzy oraz sprawdzenie jego przyswojenia. 10-minutowe sesje z nagraniami wideo i testem, odbywające się tylko raz w roku są przykładem źle opracowanych szkoleń i w ich kontekście można częściowo zgodzić się z krytyką Shneiera. Szczególnie, że nierzadko tego typu szkolenia uznawane są przez kierownictwo firm za wystarczające działania popularyzujące bezpieczeństwo informacji. Podnoszenie świadomości ma natomiast zmienić zachowania i przyzwyczajenia użytkowników, co w konsekwencji podnosi kulturę bezpieczeństwa. Jest to proces ciągły [10].

Choć trudno precyzyjnie ocenić, czy podnoszenie świadomości jest opłacalne w znaczeniu rachunku korzyści i kosztów, gdyż trudno wskazać koszt unikniętych incydentów i awarii, to istnieje wiele przykładów pokazujących skuteczne kampanie podnoszące świadomość bezpieczeństwa. Praktycznie każdy może też wskazać przykłady sytuacji, gdy uniknięto problemów dzięki zastosowaniu dobrych praktyk bezpieczeństwa [10]. Bezpieczeństwo polega na ograniczaniu ryzyka. Nie ma idealnych zabezpieczeń, które chroniłyby przed wszystkim zagrożeniami i mało prawdopodobne, że udałoby się takie stworzyć. Nawet zalecane przez ekspertów stosowanie zbiorów zabezpieczeń nie obniża ryzyka do zera. Dlatego trudno zgodzić się z opinią Schneiera, że bezpieczeństwo powinno opierać się wyłącznie na ich skuteczności. Oznacza to, że prawidłowe strategie bezpieczeństwa powinny uwzględniać niedoskonałości zabezpieczeń poprzez włączanie procesów budowania świadomości wśród użytkowników [10].

Schneier wskazuje potrzebę ochrony przed zagrożeniam z zewnątrz. Tymczasem największe straty związane z bezpieczeństwem przyniosły zdarzenia będące wynikiem błędów, nieświadomych i niezamierzonych, ale również intencjonalnych działań użytkowników wewnętrznych organizacji. Świadomość zagadnień cyberbezpieczeństwa obniża prawdopodobieństwo błędów i działań niezamierzonych, a jednocześnie pomaga ocenić pracownikom, kiedy zgłaszać potencjalnie niebezpieczne działania innych, co pozwala uchronić przed zagrożeniami intencjonalnymi [10].

Kształcenie i uświadamianie jest również sposobem na nawiązanie kontaktu ze zwykłymi użytkownikami, zmniejszenie dystansu oraz niwelowanie barier związanych na przykład z niezrozumieniem działań i procedur wprowadzanych przez ekspertów cyberbezpieczeństwa. W przeciwieństwie do rozwiązań czysto informatycznych – pozwala też ochronić zasoby informacyjne niebędące zasobami informatycznymi, jak na przykład wydrukowane dokumentacje projektowe, papierowe dokumenty księgowe etc. [10].

Winkler odnosi się także do pozostałych kwestii przywołanych przez Schneiera i przytacza szereg innych argumentów na korzyść kształcenia i podnoszenia świadomości. Swoją argumentację podsumowuje

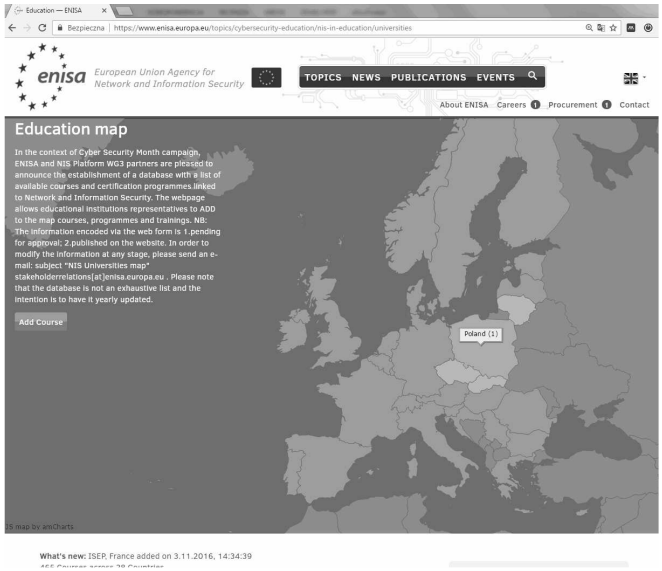
stwierdzeniem, że choć niestety istnieje wiele złych programów podnoszenia świadomości bezpieczeństwa, to obok nich powstało również wiele niezwykle skutecznych. Nawet najlepsze programy będą miały swoje słabe strony, tak jak inne zabezpieczenia. Jednak nie jest to uzasadnieniem dla rezygnowania zarówno z jednych jak i drugich, ani tworzenia wyższych standardów dla tych pierwszych. Szczególnie, że cechują się one niższym kosztem, a wskazywana alternatywa (perfekcyjne zabezpieczenia) jest mało rzeczywista [10].

3. NAUCZANIE CYBERBEZPIECZEŃSTWA W EUROPIE

W 2015 roku Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) przeprowadziła badania jakościowe mające na celu identyfikację kierunków studiów dotyczących tematyki cyberbezpieczeństwa i prywatności na europejskich uniwersytetach [1]. Z badań tych oraz aktualnej analizy informacji dostępnych w Internecie [12–16] wynika, że na studiach pierwszego stopnia dostępne są kierunki dotyczące zagadnień cyberbezpieczeństwa, natomiast brakuje propozycji związanych z ochroną prywatności. Propozycje takie pojawiają się na studiach drugiego stopnia i są najczęściej powiązane z innymi kierunkami, takimi jak bezpieczeństwo informacji, czy informatyka. Niestety wciąż jest ich niewiele. Na przykład w Wielkiej Brytanii zidentyfikowano tylko jeden program studiów jawnie odnoszący się do tematyki prywatności. Dostępne programy studiów koncentrują się przede wszystkim na zagadnieniach z obszaru informatyki, bezpieczeństwa informacji, cyberprzestępczości i cyberbezpieczeństwa. Istnieją również kursy dotykające tematyki prawnych uregulowań dotyczące prywatności, marketingu i etyki [1].

W Polsce przedmioty dotyczące cyberbezpieczeństwa prowadzone są przede wszystkim na kierunkach studiów związanych z informatyką. W Akademii Marynarki Wojennej podczas nauczania bezpieczeństwa systemów teleinformatycznych stosuje się metody aktywizacji i zwiększania motywacji studentów opartych na grywalizacji [17]. Na Politechnice Gdańskiej do programu nauczania studentów na kierunku zarządzanie wprowadzono przedmiot zarządzanie bezpieczeństwem informacji. Znaczna część absolwentów kierunku obejmie w przyszłości kierownicze lub administracyjne stanowiska i będzie miało bezpośredni wpływ na kształt cyberbezpieczeństwa w organizacjach. Zachęca się, aby taki podstawowy kurs wprowadzono do programów wszystkich szkół wyższych o podobnym profilu [18].

W październiku 2014 roku w kontekście Europejskiego Miesiąca Cyberbezpieczeństwa, ENISA wraz z partnerami, udostępniła bazę danych kursów uniwersyteckich, szkoleń i programów certyfikacyjnych związanych z bezpieczeństwem sieci i informacji. Dostępna jest także strona internetowa, za pomocą której możliwe jest dodanie do bazy nowego kursu (rys. 1) [19]. Na dzień 7 lutego 2017, w bazie zarejestrowanych jest 465 kursów w 28 państwach członkowskich. Analiza zamieszczonych w serwisie danych wskazuje, że większość kursów dedykowanych jest profesjonalistom. Widoczne jest również, że oferta szkoleń wciąż pozostaje stosunkowo ograniczona i warto byłoby ją rozszerzyć.



Rys. 1. Mapa kursów uniwersyteckich, szkoleń i programów certyfikacyjnych związanych z bezpieczeństwem sieci i informacji. Źródło: [19]

4. MASOWE OTWARTE KURSY ONLINE

Poza szkolnictwem wyższym, istnieje szereg możliwości uzyskania szkolenia w zakresie ochrony prywatności i danych, skierowanego zarówno do specjalistów pracujących w różnych sektorach (np. służba zdrowia, edukacja), przedsiębiorców, a także dla ogółu społeczeństwa. Masowe otwarte kursy online mogą stanowić obiecujące podejście do kształcenia na odległość modułów bezpieczeństwa sieci i informacji dla dużych grup odbiorców [1].

Masowe kursy online swoją treścią i zakresem merytorycznym przypominają przedmioty uniwersyteckie, ale różnią się modelem świadczenia usług, sposobem oceniania i współpracy. Dostarczane są za pośrednictwem dedykowanych platform online, dopasowanych do potrzeb odbiorców i operatorów. W większości przypadków są one dostępne darmowo na zasadach licencji otwartej, jednak istnieją również rozwiązania płatne. Kursy najczęściej dostarczane są przez czołowe uniwersytety europejskie, co rodzi przesłankę, że oferowane treści oraz model nauczania i oceniania będą wysokiej jakości [6, 20].

Jak się okazuje, masowe kursy online charakteryzują się wysokim współczynnikiem zapisów, natomiast niskim poziomem ukończenia [21]. Jednak, zdaniem niektórych miarą sukcesu nie powinien być współczynnik ukończenia kursów, tylko darmowy dostęp do wysokiej jakości materiałów edukacyjnych i sposobów kształcenia dla studentów z mniej uprzywilejowanych części świata, takich jak Indie, Chiny i Afryka [22]. Przykładem jest historia Amola Bhave, 17-letniego studenta z Indii, który został przyjęty na Massachusetts Institute of Technology, najlepszą na świecie uczelnię wg QS World University Rankings 2016-2017 [23], po uzyskaniu 97 procent punktów w otwartym kursie elektroniki i obwodów. Według studenta, masowe kursy online będą miały znaczący wpływ na Indie. Szczególnie ekscytującą cechą kursu, w którym uczestniczył Bhave była jego praktyczna natura – „oglądanie eksperymentów wykonywanych przed twoimi oczami" [22].

Według badania Li i Wana [21], różnica między uczestnikami kończącymi otwarte kursy online, a tymi którzy je porzucają, polega na większej motywacji do

samodoskonalenia, posiadanie wcześniejszych doświadczeń uczenia się i brak trudności w uczeniu się. Inne dane wskazują, że studenci, którzy kończą kursy, często posiadają już tytuł zawodowy. Warto to wziąć pod uwagę podczas tworzenia otwartego kursu z dziedziny cyberbezpieczeństwa i prywatności.

Masowe kursy online mogą stać się ciekawą ścieżką kształcenia w dziedzinie bezpieczeństwa sieci i informacji. Do tego stopnia, że Wielka Brytania wprowadziła je do swojej Narodowej Strategii Cyberbezpieczeństwa, gdzie zapisano, że rząd Wielkiej Brytanii koordynuje utworzenie kursu cyberbezpieczeństwa. Kurs ten powstał w 2014, a w roku ubiegłym pojawiła się jego uaktualniona wersja „Wprowadzenie do cyberbezpieczeństwa: bądź bezpieczny online" (rys. 2) zawierająca m.in. poprawione zadania sprawdzające wiedzę [24]. Kurs ma na celu wyjaśnienie zagadnień bezpieczeństwa online i przedstawienie podstawowych technik ochrony. Nie wymaga posiadania wcześniejszej wiedzy z zakresu cyberbezpieczeństwa, przewidziany jest na 8 tygodni, po 3 godziny tygodniowo, a po jego uzyskaniu otrzymuje się cyfrową odznakę ułatwiającą potencjalnym pracodawcom rozpoznanie umiejętności kandydata. Kurs jest całkowicie bezpłatny [24]. Oprócz kursu podstawowego rząd brytyjski wsparł stworzenie tematycznych kursów dla biznesu, dedykowanych konkretnym rodzajom przedsiębiorstw, czy grupom pracowników [25]. Podobne inicjatywy popierane są przez Komisję Europejską. W 2013 roku powstała europejska platforma kursów masowych OpenupEd, która obecnie oferuje ponad 200 szkoleń.

Rys. 2. Strona początkowa masowego kursu otwartego „Wprowadzenie do cyberbezpieczeństwa: bądź bezpieczny online" opracowanego w Wielkiej Brytanii. Źródło: [24]

5. SZKOLENIA DLA MŚP

Małe i średnie przedsiębiorstwa (MŚP) stały się celami szkodliwych działań online, a natężenie cyberprzestępczości doświadczanej przez MŚP stale rośnie. Wraz z brakiem wiedzy i świadomości problemu, może to mieć poważny wpływ na rozwój gospodarczy Unii Europejskiej – zwłaszcza, że zdecydowana większość wszystkich przedsiębiorstw europejskich to MŚP. Niestety, analizy dotyczące szkoleń cyberbezpieczeństwa w przedsiębiorstwach sektora prywatnego, takich jak MŚP, oraz w mniejszym stopniu organizacjach sektora publicznego, pokazują, że nie są one w stanie lub nie chcą finansować szkoleń i akcji uświadamiających w zakresie cyberbezpieczeństwa. Ponadto, małe i średnie przedsiębiorstwa, które aktywnie chcą poszerzyć swoją wiedzę i zrozumienie bezpieczeństwa informacji są kierowane w stronę wdrożenia standardu zarządzania bezpieczeństwem informacji ISO/IEC 27001, co jest zbyt kosztowne i w większości przypadków niekonieczne. To właśnie ten brak wiedzy i świadomości oraz zbyt zbiurokratyzowany proces certyfikacji, a także brak środków finansowych są kluczowymi aspektami problemu niskiego poziomu bezpieczeństwa MŚP. Rozwiązaniem mogłoby być utworzenie kursu dopasowanego do realiów pracy MŚP [6]. Proponowany program szkolenia przedstawia Tablica 1.

Tablica 1. Program powszechnego szkolenia zarządzania bezpieczeństwem informacji dopasowanego do realiów pracy małych i średnich przedsiębiorstw. Źródło: [6]

1	Szacowanie ryzyka
2	Polityki bezpieczeństwa
3	Identyfikacja zasobów informacyjnych
4	Zagadnienia związane z pracownikami
5	Bezpieczeństwo fizyczne
6	Kontrola dostępu
7	Zarządzanie operacyjne
8	Wykrywanie złośliwego oprogramowania
9	Monitorowanie i ochrona systemów
10	Kopie zapasowe
11	Reagowanie na incydenty
12	Przywracanie gotowości do pracy po awarii i ciągłość działania

Tak zaprojektowany przedmiot jest możliwym do wdrożenia przez małe i średnie przedsiębiorstwa rozwiązaniem, które zasadniczo podniesie bezpieczeństwo posiadanych zasobów informacyjnych. Przewidywane jest opracowanie specjalnego standardu dla MŚP, analogicznego do ISO/IEC 27001, ale dopasowanego do sytuacji mniejszych firm [6].

6. CHARAKTERYSTYKA WZORCOWEGO KURSU CYBERBEZPIECZEŃSTWA

W 2012 roku ENISA przeprowadziła badanie skierowane do instytucji edukacyjnych w Unii Europejskiej, mające na celu identyfikację elementów wzorcowego szkolenia z zakresu cyberbezpeczeństwa [26]. Ankietowani (z Grecji, Hiszpanii, Holandii, Irlandii, Niemiec, Polski i Rumunii) reprezentowali różne obszary nauczania bezpieczeństwa sieci i informacji: technologie bezpiecznej identyfikacji, testowanie penetracyjne, audyty bezpieczeństwa, audyty zgodności z ISO/IEC 27001, ocena bezpieczeństwa, bezpieczeństwo informacji, prawo technologii informacyjnych, bezpieczeństwo informacji osobistych, świadomość prywatności, systemy informacyjne w biznesie, projektowanie bezpiecznych systemów informacyjnych, obsługa incydentów, zarządzanie kryzysowe, ciągłość działania, zarządzanie nadużyciami wewnętrznymi, zarządzanie zmianą, równowaga między życiem zawodowym a osobistym, bezpieczeństwo e-kształcenia, systemy uczące się, techniki rozpoznawania wzorców, technologie identyfikacji radiowej (RFID) i poszerzanie świadomości.

Z odpowiedzi wynika, że aby przeprowadzić najlepsze szkolenie w zakresie cyberbezpieczeństwa, nauczyciel powinien uwzględnić następujące komponenty [26]:

- krótkie wprowadzenie,
- praktyczne laboratoria,
- rzeczywiste scenariusze i przykłady z życia codziennego,
- sesje szkoleniowe ciągłego kontaktu obejmujące odgrywanie scenek, symulacje/emulacje, pracę zespołową, budowanie zespołów, zasady zarządzania projektami
- konkurs hackerski – praktyczny kurs ochrony,
- grę biznesowa zamiast egzaminów,
- odtwarzanie nagrań wideo
- proporcje 20 minut teorii, 30 minut praktyki, 10-20 odpowiedzi na pytania.

Ankietowani wskazali następujące kierunki i trendy nauczania bezpieczeństwa informacyjnego [26]:

- dotyczące treści kształcenia: systemy cyber-fizyczne, prywatność i zaufanie, kryptografia, bezpieczeństwo oprogramowania, użyteczne bezpieczeństwo, bezpieczeństwo w chmurze, bezpieczeństwo Internetu i infrastruktur, międzynarodowe standardy (np. ITIL, ISO/IEC 20000, ISO/IEC 27000),
- oraz metod kształcenia: e-kształcenie, m-learning, testy online, spotkania z mentorem, zajęcia laboratoryjne.

Praktycznie wszyscy ankietowani wskazali potrzebę poszerzania świadomości w dziedzinie bezpieczeństwa informacji osobistych oraz doradztwa prawnego w zakresie zachowań nielegalnych. Zauważa się rosnące zapotrzebowanie na kursy kończące się otrzymaniem międzynarodowego certyfikatu [26].

Zapytani o 10 największych wyzwań związanych z cyberbezpieczeństwa ankietowani wymienili zagadnienia [26]:

- prywatności,
- ryzyka związanego z wykorzystaniem nowych technologii,
- interdyscyplinarne (prawne, techniczne, organizacyjne),
- zrozumienia technologii a nie tylko korzystanie z nich,
- trudności z usunięciem z Internetu opublikowanej tam informacji i wynikających z tego konsekwencji nawet w bardzo odległej przyszłości,
- pozyskiwania aktualnych i rzetelnych informacji od prowadzących oraz zagwarantowania ich dobrej orientacji w nowych technologiach (czasem uczeń posiada większą wiedzę niż nauczyciel),
- transpozycji prawdziwych relacji międzyludzkich na rzeczywistość internetową, netykieta (etykieta dotycząca zachowania w Internecie).

Uczestnicy ankiety wyróżnili następujące elementy skutecznego modelu partnerstwa dla promocji bezpieczeństwa w sieci [26]:

- osobisty kontakt użytkownika z prowadzącym zajęcia,
- akredytowani prowadzący posiadający wysokie umiejętności i doświadczenie praktyczne,
- ciągle uaktualniane materiały do zajęć,
- elastyczna struktura zajęć,
- współpraca z przemysłem i instytucjami akademickimi,
- otwartość na zmiany i pozytywne nastawienie dotyczące rozwiązywania problemów,
- zajęcia prowadzone w formie dyskusji,
- pasja i umiejętna komunikacja,
- wysokie standardy etyczne,
- profesjonalizm i doświadczenie w dziedzinie, omawianie rzeczywistych przykładów,
- podejście cechujące się dostarczaniem narzędzi a nie rezultatów,
- partnerstwo publiczno-prywatne w celu finansowania zasobów,
- szkolenia dla prowadzących.

7. WNIOSKI KOŃCOWE

Dyskusja między Bruce Schneierem oraz Irą Winklerem pokazuje, że choć istnieją pewne argumenty przeciwko powszechnemu nauczaniu zasad cyberbezpieczeństwa, to dotyczą one tak naprawdę źle opracowanych szkoleń oraz oparte są na słabej przesłance, iż możliwe jest stworzenie perfekcyjnych zabezpieczeń technicznych. Tymczasem takie zabezpieczenia nie istnieją i mało prawdopodobne, że uda się je stworzyć, dlatego dobre strategie bezpieczeństwa powinny zawierać działania podnoszenia świadomości wśród użytkowników [10, 11]. Działania te znacząco podnoszą poziom bezpieczeństwa w małych i średnich przedsiębiorstwach. Dlatego ważne, aby dotrzeć do nich z odpowiednią, profilowaną ofertą edukacyjną [6].

Kluczowe znaczenie edukacji zostało potwierdzone w Europejskiej Agendzie Cyfrowej oraz strategiach cyberbezpieczeństwa państw członkowskich [1]. Tymczasem wciąż jedynie mniej niż połowa obywateli Unii Europejskiej uważa, że jest dobrze poinformowana o zagrożeniach cyberbezpieczeństwa [5]. Dlatego zagadnienia związane z tym obszarem powinny stać się częścią akademickich programów kształcenia, na różnych kierunkach studiów [9]. W chwili obecnej tego typu programy proponowane są głównie na kierunkach związanych z technologiami informacyjnymi [1, 12–16].

Obiecującym sposobem popularyzacji zasad cyberbezpieczeństwa mogą być także masowe otwarte kursy online [1]. Choć jak dotąd wciąż cechują się niskim poziomem ukończenia przy dużym współczynniku zapisów, to sytuacja ta zmienia się w przypadku uczestników o wysokiej motywacji do samodoskonalenia, posiadających wcześniejsze doświadczenia uczenia się [21]. Mogłoby to wskazywać, że warto tego typu kursy adresować do starszych odbiorców, posiadających wcześniejsze doświadczenia edukacyjne, a być może nawet aktywnych zawodowo.

Powszechne kursy cyberbezpieczeństwa powinny w dużej mierze bazować na ćwiczeniach praktycznych podczas których uczestnicy biorą udział w symulacjach, realizują konkretne scenariusze zdarzeń oraz pracują zespołowo. Zajęcia powinny dotyczyć rzeczywistych sytuacji i przykładów z życia codziennego, i omawiać przede wszystkim zagadnienia prywatności, ryzyka związanego z wykorzystaniem nowych technologii oraz kwestii interdyscyplinarnych (prawnych, technicznych, organizacyjnych) [26].

8. BIBLIOGRAFIA

1. Anderson P., Paoli S. De, Catalui D.: Status of privacy and NIS course curricula in Member States, 2015.
2. Marian Golka: Czym jest społeczeństwo informacyjne?, Zesz. Ruchu Prawniczego, Ekon. i Socjol. 4, 2005, s. 253–265.
3. Bąkowski A.: Słownik pojęć Portalu Innowacji - E-umiejętności, http://www.pi.gov.pl/parp/chapter_96055.asp?soid=E340D9826BF143D6BDBCD2EA72BA5F6F.
4. ISO/IEC: ISO/IEC 27005:2011: Information technology — Security techniques — Information security risk management, 2011.
5. European Commission: Special Eurobarometer 423: Cyber Security, 2015.
6. Berendt B., Paoli S. De, Laing C., Fischer-Hubner S., Catalui D., Tirtea R.: Roadmap for NIS education programmes in Europe, 2014.
7. Werner Degenhardt: EISAS Large-Scale Pilot - Collaborative Awareness Raising for EU Citizens & SMEs, 2012.
8. Mulligan D. K., Schneider F. B.: Doctrine for Cybersecurity, Daedalus 140, 2011, s. 70–92.
9. McGettrick A., Cassel L. N., Dark M., Hawthorne E. K., Impagliazzo J.: Toward Curricular Guidelines for Cybersecurity, Proc. 45th ACM Tech. Symp. Comput. Sci. Educ. 2014, s. 81–82.
10. Winkler I.: Arguments Against Security Awareness Are Shortsighted - Dark Reading, http://www.darkreading.com/risk/arguments-against-security-awareness-are-shortsighted/d/d-id/1139417?
11. Schneier B.: On Security Awareness Training, http://www.darkreading.com/risk/on-security-awareness-training/d/d-id/1139381?
12. Quora: What are the best cyber security master's in Europe?, https://www.quora.com/What-are-the-best-cyber-security-masters-in-Europe.
13. EC-Council: European University Recognizes Importance of Information Security Education, https://www.eccouncil.org/importance-of-information-security-education/.
14. StudyPortals: Cyber Security, M.Sc. - at Tallinn University of Technology, Tallinn, Estonia - MastersPortal.eu, http://www.mastersportal.eu/studies/10529/cyber-security.html.
15. Lord N.: Cybersecurity Higher Education: The Top Cybersecurity Colleges and Degrees, https://digitalguardian.com/blog/cybersecurity-higher-education-top-cybersecurity-colleges-and-degrees.
16. Keystone Academic Solutions: Best Bachelor Degrees in Cyber Security in Europe 2017, https://www.bachelorstudies.com/Bachelor/IT/Cyber-Security/Europe/.
17. Rodwald P.: Gamifikacja – czy to działa?, EduAkcja. Mag. Edukac. Elektron. 1, 2016, s. 43–50.
18. Leszczyna R.: Nauczanie zarządzania bezpieczeństwem informacji: standardy i sposoby nauczania, Zesz. Nauk. Wydz. Elektrotechniki i Autom. Politech. Gdańskiej 2016, s. 47--53.
19. ENISA: Education map, https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities.
20. Kępińska-Jasny M., Łyp-Wrońska K.: The Conference Power of MOOCs - time for a Polish platform, e-mentor 2015, 2015, s. 40–41.
21. Li Q., Wan F.: A Case Study of the Characteristics of MOOCs Completers: Taking an Online Professional Training MOOC for Example. In: 2016 IEEE 16th International Conference on Advanced Learning Technologies (ICALT). pp. 503–505. IEEE 2016.
22. Haggard S.: The Maturing of the MOOC, 2013.
23. QS Quacquarelli Symonds Limited: QS World University Rankings QS 2016-2017, https://www.topuniversities.com/university-rankings/world-university-rankings/2016.
24. Open University: Introduction to Cyber Security: stay safe online, https://www.futurelearn.com/courses/introduction-to-cyber-security.
25. GOV.UK: Cyber security, https://www.gov.uk/government/policies/cyber-security.
26. Catalui D.: Collaborative Solutions For Network Information Security in Education, 2012.

CYBERSECURITY EDUCATION IN THE EUROPEAN UNION – TRENDS, CHALLENGES

Today, in the era of information society, the importance of cybersecurity education, training and awareness is widely acknowledged. In recent years many new initiatives have been taken in the European Union related to the development of academic programmes, creation of specialised, dedicated trainings, launching massive open online courses (MOOCs) as well as conducting stocktaking studies. There was a very interesting debate about the value of security awareness raising and trainings which provided strong arguments supporting inclusion of educative actions into organisations' cybersecurity strategies. These actions, for instance, significantly improve security level in small and medium enterprises. The indispensable role of user education was confirmed in the European Digital Agenda and cyber security strategies of member states. Relevant courses need to be included into common curricula, not only the programmes for students of information technologies as it is today. A promising direction in popularisation of cybersecurity principles are Massive Online Open Courses (MOOCs). Although generally they expose a low level of completion, they became successful for participants with high self-motivation and previous learning experiences. A survey in educational institutions regarding the characteristics of a model cybersecurity course show that primarily it should rely on practical exercises based on role-playing and simulations, performed in teams. The content of such course should include real-life examples, privacy issues and risks inherent to the use of new technologies, as well as multidisciplinary questions. The paper presents cybersecurity education initiatives together with challenges related to them, and the trends and perspectives in cybersecurity education.

Keywords: cybersecurity, information security, education, awareness raising, massive open online courses, MOOCs.