



REGIONAL
CYBER LABS



RAPORT
NOWE OTWARCIE
W EDUKACJI
O CYBERBEZPIECZEŃSTWIE
2020-2021



REGIONAL
CYBER LABS



THE BRIDGE
FOUNDATION



CYBER SECURITY
CHALLENGE
PL/2020

NOWE OTWARCIE W EDUKACJI O CYBERBEZPIECZEŃSTWIE



REGIONAL
CYBER LABS



Ogólnopolski raport opinii środowiska studenckiego promujący perspektywę interdyscyplinarnego podejścia do edukacji o ekosystemie cyberbezpieczeństwa.

Projekt zrealizowany w ramach aktywności wojewódzkich Cyber Labów – nowatorskiej platformy na rzecz edukacji o cyberbezpieczeństwie. Profil zaangażowanych uczelni: techniczne, prawnicze, biznesowe, medyczne i wojskowe.



THE BRIDGE
FOUNDATION



REGIONAL
CYBER LABS

SŁOWO WSTĘPNE

Dynamiczny rozwój zaawansowanych technologii, a wraz z nim postępujący proces cyfryzacji gospodarki i społeczeństw wprowadzają zmiany we wszystkich dziedzinach życia, w tym w systemie edukacji. Efekty tych przemian zależne będą od sposobu zarządzania transformacją cyfrową, gdzie szkolnictwo wyższe odgrywa znaczącą rolę.

Implementacja w programach uczelni treści, umożliwiających studentom nabycie oczekiwanych przez szeroki krąg interesariuszy kompetencji i umiejętności stanowi kompleksowe wyzwanie.

Raport jest zaproszeniem do dyskusji dla środowisk studenckich, akademickich, instytucji publicznych i sektora prywatnego. Przedstawione przez studentów rekomendacje mogą – w korzystny sposób - przyczynić się do zwiększenia sprawności reagowania systemu edukacji na potrzeby rynku pracy, poprzez wdrażanie polityki edukacyjnej sprzyjającej transformacji cyfrowej.

Reprezentowane w raporcie kierunki studiów: IT, prawo, biznes, medycyna i wojskowość wpisane są w fundamenty cyfrowej transformacji na, co najmniej, najbliższe 10 lat. Przegląd tych specjalności pod kątem wyzwań powstałych z korelacji postępu technologicznego i cyberbezpieczeństwa daje możliwości na wzmocnienie, i głębsze wykorzystanie kapitału intelektualnego studentów. Czynnikiem kluczowym w tym procesie jest wyeksponowanie wzajemnie wzbogacającej relacji wykładowca-student.

Fundamentem do przygotowania raportu stał się potencjał wykreowany przez turniej CyberSecurity Challenge PL2020, zrealizowany z patronatem Ministerstwa Cyfryzacji, Rządowego Centrum Bezpieczeństwa i ISSA Polska. Turniej integrował studentów pięciu dziedzin: IT, prawa, biznesu, medycyny i wojskowość. 16 wojewódzkich, interdyscyplinarnych zespołów wcieliło się w rolę tzw. tiger groups - doradców rządu podczas cyberkryzysu, dotyczącego różnych obszarów funkcjonowania państwa.

To innowacyjne ćwiczenie, gromadzące wyróżniających się studentów z 65 uczelni, adresowało wymiar strategiczno-technologiczny, regulacyjny i komunikacyjny kryzysu. Nabyte przez uczestników kompetencje stworzyły potencjał do dalszych działań, w tym do zainicjowania aktywności wojewódzkich Cyber Labów.

Raport jest pierwszym projektem wypracowanym przez wojewódzkie Cyber Laby – agorę dla młodych liderów/liderek zainteresowanych domeną cyberbezpieczeństwa w kontekście studiowanej domeny. Współtwórcy dokumentu wywodzą się z grona uczestników turnieju, kół naukowych propagujących tematykę cyberbezpieczeństwa i z rekomendacji wykładowców akademickich.

Dziękuję zaangażowanym w powstanie dokumentu stronom, instytucjom, ekspertom, ambasadorom, a w szczególności studentom! To ich dedykacja i profesjonalizm umożliwiły przygotowanie raportu. Tworząc go zainwestowali w dobro wspólne w ujęciu generacyjnym. Uwzględniając wymiar swojego pokolenia, mieli też na uwadze spektrum społeczne problematyki, dające ująć się w stwierdzeniu, że cyberbezpieczeństwo dotyczy nas wszystkich – od juniora do seniora.

Zapraszając Państwa do lektury i dyskusji postępuję się przemością, iż edukacja o wyzwaniach związanych z cyberbezpieczeństwem jest jak maraton, a nie sprint. Wymaga zintegrowanego podejścia i stawiania pytań generujących nowe myślenie i działanie.

*Margo Koniuszewski
Prezes Fundacji The Bridge*

ZASIĘG LOKALNY I MIĘDZYNARODOWY



REGIONAL
CYBER LABS

#RegionalCyberLabsPL20/21
@CyberPoland



Raport wpisuje się w dyskurs dotyczący modelowania edukacji o cyberbezpieczeństwie w ujęciu lokalnym i międzynarodowym. Lokalnie realizuje założenia Strategii Cyberbezpieczeństwa RP 2019/24 i Strategii Bezpieczeństwa Narodowego (aspekt cyberbezpieczeństwa). Buduje świadomość i kompetencje społeczne w zakresie cyberbezpieczeństwa, wzmacniania rozwój krajowego systemu cyberbezpieczeństwa, promując dobre praktyki.

W wymiarze międzynarodowym wpływa na kształtowanie polityki sprzyjającej globalnej transformacji cyfrowej. Realizuje cele stawiane Polsce przez organizacje międzynarodowe UE, ONZ, OECD i NATO, w obszarach prowadzenia działań z zakresu edukacji i budowania interdyscyplinarnych kompetencji, wymiany wiedzy i doświadczeń między akademią, biznesem, instytucjami publicznymi, organizacjami pozarządowymi i międzynarodowymi.



THE BRIDGE
FOUNDATION



REGIONAL
CYBER LABS



Rekomendacje studentów eksponujące w programach studiów tematykę ekosystemu cyberbezpieczeństwa (jego interdyscyplinarne ujęcie) powstały w drodze przeglądu programów nauczania w danej domenie: IT, prawo, biznes, medycyna i wojskowość. Dokument zawiera też komentarze środowiska akademickiego i ekspertów.

W ramach domeny, studenci przygotowali indywidualne analizy, które następnie poddano grupowym konsultacjom. W efekcie wypracowano zbiorczy dokument, prezentujący opinie danej domeny.

Rekomendacje powstały w sposób autonomiczny, bez ingerencji w prace studentów środowiska akademickiego. Nauczyciele akademicki, wspierający projekt występowali w roli tutorów.

Każdą z domen reprezentowało dwoje koordynatorów - liderów grup zarządzających procesem powstania rekomendacji.

KOORDYNATORZY DOMEN



Cyberbezpieczeństwo to kluczowy element ogólnego bezpieczeństwa w 21 wieku.

AGATA ZALEWSKA, **Ambasadorka #WarmińskoMazurskieCyberLab**

Studentka Wydziału Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego

W dobie z informatyzowanego świata potrzeba interdyscyplinarnej edukacji o cyberbezpieczeństwie.

ANDRZEJ PORĘBSKI, **Ambasador #MałopolskieCyberLab**

Student Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego i Wydziału Zarządzania Akademii Górniczo-Hutniczej



Transformacja cyfrowa stwarza szanse i wyzwania. By z niej korzystać konieczna jest dobra nawigacja.

NATALIA BRONDER, **Ambasadorka #OpolskieCyberLab**

Studentka Wydziału Elektrotechniki Automatyki i Informatyki Politechniki Opolskiej

Projekt ma zasięg ogólnopolski, ale równolegle rezonuje międzynarodowo.

MATEUSZ JACHNIAK, **Ambasador #DolnośląskieCyberLab**

Student Wydziału Podstawowych Problemów Techniki Politechniki Wrocławskiej



Multiplikujemy doświadczenie zdobyte w turnieju Cybersecurity Challenge PL2020.

MARTA LEWANDOWSKA, **Ambasadorka #WielkopolskieCyberLab**

Studentka Wydziału Inżynierii Zarządzania Politechniki Poznańskiej

Wychodzimy poza tradycyjne schematy myślenia i działania.

KAMIL CHMURA, **Ambasador #LubelskieCyberLab**

Student Wydziału Ekonomicznego Uniwersytetu M. Curie-Skłodowskiej w Lublinie



Synergia płynąca z projektu jest konkretnym, innowacyjnym aktywem.

JULIA MAKUCH, **Ambasadorka #DolnośląskieCyberLab**

Studentka Wydziału Lekarskiego na Uniwersytecie Medycznym we Wrocławiu

Ten dokument to nowe otwarcie w edukacji o cyberbezpieczeństwie.

MATEUSZ GUZIAK, **Ambasador #PomorskieCyberLab**

Student Wydziału Lekarskiego na Gdańskim Uniwersytecie Medycznym



REKOMENDACJE STUDENTÓW

W procesie przygotowania raportu uczestniczyło 132 studentów, reprezentujących 35 uczelni. Rekomendacje poszczególnych domen, z komentarzami środowisk akademickich i eksperckich zaprezentowano w rozdziałach: Technologie Informacyjne, Biznes, Medycyna, Prawo i Wojskowość.

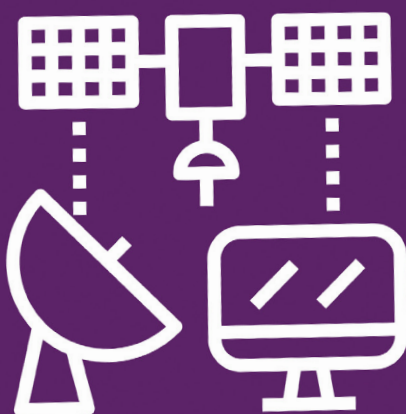


#EkosystemCyberbezpieczeństwa





3 TECHNOLOGIE INFORMACYJNE



Mateusz Rędzia

Politechnika Wrocławska
Wydział Elektroniki

REKOMENDACJE DOMENA IT

Materiał źródłowy zgromadzony w ramach analizy programów nauczania, dokonanej przez studentów dziesięciu polskich uczelni o profilu technicznym. Reprezentowane uczelnie: Politechnika Krakowska, Politechnika Lubelska, Politechnika Łódzka, Politechnika Opolska, Politechnika Poznańska, Politechnika Śląska, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, Uniwersytet Warmińsko-Mazurski, Politechnika Wrocławska, Uniwersytet Zielonogórski.

Aktualny stan nauczania na temat cyberbezpieczeństwa

Należyta edukacja sektora IT w dziedzinie cyberbezpieczeństwa jest jednym z kluczowych elementów prawidłowego funkcjonowania gospodarki. Poziom kwalifikacji specjalistów, odpowiedzialnych za tworzenie, nadzorowanie, zarządzanie oraz przeprowadzanie audytów systemów cyfrowych, przekłada się na bezpieczeństwo cyfrowe sektora przedsiębiorstw i sektora publicznego.

Z punktu widzenia studentów uczelni technicznych obecny stan nauczania o cyberbezpieczeństwie jest niezadowalający w dwóch wymiarach: w sposobie nauczania, jak i w zakresie przekazywanej wiedzy. Sugerowanym jest wprowadzenie kompleksowych zmian.

Największe wyzwanie, w edukacji w tej domenie, stanowi według nas niewystarczająca liczba przedmiotów poruszających kwestie bezpieczeństwa cyfrowego. W programach studiów kierunków informatycznych brakuje modułów, pozwalających na dostarczenie wiedzy z tego zakresu. Nauczyciele akademicki, wykładający na pojawiających się na nie-licznych uczelniach kursach dotyczących cyberbezpieczeństwa, z reguły adresują jedynie podstawy tej jakże szerokiej dziedziny. W kontekście postępującego procesu globalnej cyfryzacji potrzeba nauczania o cyberbezpieczeństwie wydaje się nam być kluczową na wszystkich kierunkach informatycznych, a nie tylko związanych bezpośrednio z cyberbezpieczeństwem.

Poświęcenia uwagi wymaga kwestia przekazywania zdezaktualizowanej wiedzy. Na zajęciach prezentowane są przestarzałe technologie i rozwiązania niemające już praktycznego zastosowania w sektorze IT. W tym miejscu należy jednak zauważyć, iż wiedza z zakresu cyberbezpieczeństwa (a przynajmniej niektórych jego dziedzin) dość szybko ulega dezaktualizacji, dlatego rozwiązanie tej kwestii będzie dużym wyzwaniem.

Problem stanowi też brak holistycznego podejścia do kwestii cyberbezpieczeństwa podczas nauczania przedmiotów informatycznych. Programy przewidują często stosowanie narzędzi (bibliotek, funkcji, elementów języków programowania), których używanie jest niepożądane ze względu na potencjalne luki bezpieczeństwa. Studenci korzystający z takich rozwiązań wypracowują sobie niewłaściwe praktyki, jednocześnie nie będąc świadomymi zagrożeń jakie mogą płynąć z ich zastosowania. Warty dodania jest fakt, iż podczas omawiania języków programowania nie jest przekazywana wiedza dotycząca wad i luk, jakie w tych narzędziach występują, a które mogą doprowadzić do potencjalnych, niepożądanych incydentów w obszarze cyberbezpieczeństwa.

REKOMENDACJE DOMENA IT

Istotnym problemem w nauczaniu o cyberbezpieczeństwie, przed którym stoi wiele uczelni, jest nieprzywiązywanie należytej uwagi do praktycznych umiejętności studentów. Często, opuszczając mury uczelni, dyplomowany specjalista nie miał styczności z symulacjami cyberataków na systemy informatyczne. Korzystnym dla poprawy umiejętności studentów byłoby włączenie do programów przedmiotów modułów pozwalających na tego typu ćwiczenia.

Integralny element naszej analizy stanowi fakt w jaki sposób uczelnie przechowują, przetwarzają i zabezpieczają dane studentów. Niejednokrotnie na uczelniach wyższych łamana była ustawa dotycząca ochrony danych osobowych. Przykład może stanowić wyciek danych z Politechniki Warszawskiej, czy nagminnie pojawiający się problem publikowania ocen studentów wraz z ich imionami, nazwiskami i numerami indeksów. Ten stan rzeczy jest niekorzystny nie tylko ze względów wizerunkowych dla danej instytucji. Łamanie norm dotyczących ochrony danych osobowych może stwarzać u studentów mylne wrażenie jakoby kwestie bezpieczeństwa danych cyfrowych można było traktować marginalnie.

Analizując proces nauczania tej dziedziny eksponujemy obszary z potencjałem do modyfikacji lub usprawnienia. System oświaty ma do zaadresowania wiele wyzwań. Naszą analizę i rekomendacje oferujemy jako narzędzie, które może być pomocne w tym procesie.

Główne kierunki koniecznych zmian

W tej części raportu prezentujemy aspekty, na które zwracamy szczególną uwagę w kontekście promocji edukacji o cyberbezpieczeństwie. Chcielibyśmy zaproponować je jako formę dialogu ze środowiskiem akademickim, mającego na celu ustawiczne podnoszenie jakości kształcenia. W naszym rozumieniu wzorowym i najbardziej efektywnym podejściem byłoby wyrobienie u słuchaczy umiejętności myślenia „jak cyberprzestępca”, tak by zawsze być o krok do przodu i działać według schematu proaktywnego, próbującego wyprzedzić zagrożenia. Analogią, w tym miejscu, jest przytoczenie historii Franka Abagnale’a z popularnego filmu „Złap mnie jeśli potrafisz” - jednego z najstydniejszych fałszerzy pieniędzy, który po otrzymaniu wyroku współpracował z FBI jako doradca w sprawie oszustw czekowych.

1 — Rozpowszechnienie wiedzy na temat luk w zabezpieczeniach systemów

Dydaktyka, zarówno wykłady, jak i ćwiczenia powinny poruszać tematykę luk w zabezpieczeniach systemów i sposobach adresowania tych dysfunkcji. Fundament w dziedzinie bezpieczeństwa komputerowego stanowi koncepcja nazwana „triadą CIA”¹ i związana z nią definicja poufności, integralności oraz dostępu do informacji. Jako społeczeństwo zawdzięczamy nasz rozwój (indywidualne i instytucjonalne) informacji przechowywanej, przetwarzanej i wymienianej. Informacja jest towarem, który można nabyć, pozwalającym na osiągnięcie określonych korzyści, dlatego należy ją chronić.

Najważniejszą rolę pełnią tu zabezpieczenia oraz ochrona przed osobami nieupoważnionymi. W tym celu koniecznym jest wykonywanie testów i przeprowadzanie kontroli bezpieczeństwa zgodne z wzorcami badań technicznych.

¹ W Stallings, Kryptografia i bezpieczeństwo sieci komputerowych (Gliwice: Helion, 2012).

REKOMENDACJE DOMENA IT

Przerwanie dostępu do informacji lub fałszowanie danych może spowodować wymierne straty zarówno finansowe, jak i utraty reputacji. Dlatego istotną, jeśli chodzi o funkcjonowanie organizacji, jest edukacja o tzw. planach nagłych wydarzeń lub planach awaryjnych (ang. contingency plan). Dzięki posiadaniu dokumentacji, określającej zachowanie poszczególnych grup i jednostek m.in. w przypadku naruszenia bezpieczeństwa, możliwym jest ograniczenie negatywnego wpływu incydentu i opisanie procesu rekonwalescencji. Wiedzę o przedstawionych wyżej zagadnieniu mógłby podnosić kurs o nazwie „Zgodność i Bezpieczeństwo Operacyjne”.

2 — Informowanie o aktualnych problemach związanych z tematyką cyberbezpieczeństwa i zapoznanie ze źródłami informacji przydatnymi dla programistów

Istotny element stanowi popularyzacja wiarygodnych źródeł edukacji pozaakademickiej (np. sprawdzone, profesjonalne portale tematyczne) oraz wyrobienie u studentów nawyku tzw. self-education. Przyszli programiści posiadając dostęp do różnych źródeł są w stanie nabywać nową wiedzę, podnosić kwalifikacje i dzielić się wiedzą. Stały dostęp do aktualnych informacji o problematyki związanej z cyberbezpieczeństwem to w naszej opinii fundament we współczesnym świecie. Tworząc nowe narzędzia oraz budując społeczności zrzeszające specjalistów chętnych do dzielenia się swoim doświadczeniem, bezpośrednio umacniamy bezpieczeństwo cyfrowe.

3 — Doskonalenie kadr akademickich i zmiany w sylabusie

Globalny proces cyfryzacji czyni Informatykę jedną z najprężniej rozwijających się dziedzin. Pojawiające się z dnia na dzień nowe technologie i języki programowania w szybkim tempie zmniejszają grono użytkowników starszych rozwiązań, usuwając kolejne języki z listy najpopularniejszych. Z tego powodu kluczową jest umiejętność adaptacji do nowo powstających technologii, szczególnie w kontekście oczekiwań płynących z rynku pracy. Pracodawcy wymagają, od przyszłych pracowników, znajomości nowych języków programowania, frameworków czy bibliotek.

Uwzględniając tempo, zmieniających się na rynku IT trendów, pozycje w sylabusach powinny podlegać procesowi przeglądu i systematycznej aktualizacji w formie dodawania nowych przedmiotów lub rozszerzania tematyki już istniejących kursów. Aktualizacja sylabusu pozwoli na przekazywanie studentom wiedzy i doświadczeń, pożądanych przez szybko ewoluujący rynek pracy. Narzędziem do selekcji materiałów, które miałyby zostać dodane do programu nauczania, mogłaby stać się analiza popularności danej technologii (tempo przybywania aktywnych użytkowników).

Implementacja zmian w toku nauczania, wymaga równoległe ciągłego doszkalania kadry akademickiej. Ważnym jest, by wykładowcy monitorowali informacje dotyczące nowych technologii i cyberbezpieczeństwa w obrębie swoich specjalizacji i przekazywali te nowości podczas zajęć.

W efekcie tego dwubiegowego procesu, z jednej strony kształcenie wykładowców, z drugiej zaś samokształcenie się studentów powstanie innowacyjny efekt synergiczny polegający na obopólnym uczeniu.

REKOMENDACJE DOMENA IT

W nauce zjawisko to opisane jest jako „obdarzanie obopólne” – czynnik kluczowy dla rozwoju wzajemnie wzbogacającej relacji mistrz-uczeń, w której obie strony interakcji stanowią dla siebie źródło inspiracji i nieustannego rozwoju.

4 — Tworzenie oprogramowania z myślą o bezpieczeństwie użytkowników, w tym wykorzystaniem danych wrażliwych

Nagminnym stał się proceder wyłudzenia danych osobowych i wykorzystywania ich niezgodnie z przeznaczeniem. Według raportu CERT Polska² phishing, czy ogólnie wyłudzenie informacji, to najczęściej występujący w Polsce typ ataku. W tym kontekście istotny element stanowi kształcenie z zakresu bezpieczeństwa danych przechowywanych w Internecie. Wskazaniem byłoby włączenie zagadnień związanych z architekturą baz danych, zasad przetwarzania i bezpiecznego przechowywania danych osobowych, w tym analizy wybranych elementów Ogólnego rozporządzenia o ochronie danych RODO, do sylabusu przedmiotu o nazwie „Sposoby Ochrony Danych w Sieci”.

5 — Bezpieczeństwo haseł

Tematyka ta powinna być podnoszona zarówno wśród użytkowników Internetu, jak i twórców oprogramowania, włączając zgłębiających domenę studentów.

Mnogość posiadanych przez użytkowników kont, do których logowanie następuje przez hasła niejednokrotnie stanowi słaby punkt w zabezpieczeniach. Jednym z najistotniejszych tematów jest stosowanie i przechowywanie odpowiednich haseł z użyciem menedżerów haseł oraz wykorzystanie uwierzytelniania dwuskładnikowego (2FA).

Równie fundamentalnym zagadnieniem w kontekście bezpieczeństwa jest instalowanie oprogramowania z wiarygodnych i zweryfikowanych źródeł.

6 — Zagrożenia związane z sieciami publicznymi i wykorzystaniem danych wrażliwych

Już od najmłodszych lat, poczynając od edukacji szkolnej, przy wsparciu kampanii społecznych, powinniśmy dążyć do uświadamiania, czym są dane wrażliwe, dlaczego są bardzo ważnym elementem prywatności i bezpieczeństwa osobistego oraz w jaki sposób powinno się je chronić. Społeczeństwo winno być świadome kwestii używania danych osobowych i danych wrażliwych w miejscach, które nie wzbudzają pełnego zaufania, tj. niezauważanych portalach internetowych, formularzach oraz publicznych i otwartych sieciach Wi-Fi.

Zagadnienie to dotyczy także obecnych i przyszłych administratorów danych osobowych, oraz twórców oprogramowania i osób zajmujących się utrzymaniem systemów informatycznych. Należy stawiać na większe wymagania dotyczące architektury bazy danych, przetwarzania i bezpiecznego przechowywania tylko niezbędnych danych wrażliwych.

² „Krajobraz bezpieczeństwa polskiego internetu, Raport roczny 2019 z działalności CERT Polska”, 2019, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf.

REKOMENDACJE DOMENA IT

Opisane poniżej wyzwania wraz z propozycjami ich zaadresowania
oznaczone są piktogramami



Wyzwanie



Stan Pożądany



Rekomendacje



Nieprzywiązywanie należytej wagi do zagadnienia „nadawania uprawnień” w procesie nauki o projektowaniu aplikacji oraz zbyt duże uprawnienia użytkowników w różnych aplikacjach/systemach, które nie są im potrzebne do wykonywania powierzonych zadań. Dotyczy to zarówno całych systemów operacyjnych i ciągłego korzystania z konta Administratora (Admin), jak i projektowania/korzystania z aplikacji, w których brakuje podziału na więcej ról niż Admin oraz Użytkownik.



Użytkownicy posiadają jedynie minimalne uprawnienia wystarczające do wykonywania określonych zadań.



Uwzględnianie kwestii uprawnień dla różnych typów kont użytkowników podczas projektowania aplikacji na zajęciach. Należy uświadamiać ten aspekt twórcom oprogramowania (np. moderator nie powinien móc usuwać kont wszystkich użytkowników), jak i jego użytkownikom. Studenci powinni rozumieć istotę wpływu na bezpieczeństwo systemu tzw. least privilege policy. Redukcja dostępu do różnych części systemu powoduje mniejsze szkody w przypadku przejęcia danego konta lub wykonania z jego poziomu złośliwego kodu. Ciągłe korzystanie z kont z uprawnieniami Admina (czy to w systemie operacyjnym, czy w przypadku aplikacji X) jest często wygodne, jednak stanowi poważny problem z punktu widzenia bezpieczeństwa systemu. Słuchacze powinni być świadomi zagrożeń związanych z używaniem aplikacji/systemu, przy korzystaniu z kont z największymi uprawnieniami. Najlepsze efekty wyrobienia stosowania dobrych praktyk przy tym zagadnieniu przynosi nauczanie oparte o konkretne przykłady. Podczas kursu studenci powinni być poinformowani, w jaki sposób korzystać z systemu lub projektować aplikacje, by zachować możliwość wykorzystania mechanizmów grup/rol/innych ograniczeń dostępu i w dalszym ciągu móc wykonywać wszelkie potrzebne operacje.



Wykładowcy przedstawiają nieaktualne podejście do cyberbezpieczeństwa. Przekazywana wiedza oparta jest często na niestosowanych już technologiach czy praktykach.



Prezentowanie aktualnej wiedzy w oparciu o najnowsze technologie, praktyki i główne trendy w branży IT w zakresie cyberbezpieczeństwa.



Zarządzające kadrą akademicką jednostki organizacyjne powinny kłaść większy nacisk na jakość i aktualność przekazywanej wiedzy na temat cyberbezpieczeństwa. Doskonalenie pod kątem stosowania nowych technologii, języków oraz dobrych praktyk powinno być wdrażane już na poziomie tych jednostek. Wykładowcy oraz prowadzący ćwiczenia i laboratoria winni wykorzystywać aktualne i powszechnie uznane technologie w nauczaniu przedmiotów, których cyberbezpieczeństwo jest ważnym elementem lub składową. Zwiększony powinien być także nacisk na nowe podejścia do praktyk związanych z zapewnieniem bezpieczeństwa systemów.

REKOMENDACJE DOMENA IT

-  *Kadra prowadząca zajęcia z nauki programowania i języków programowania często wykorzystuje biblioteki, funkcje, praktyki lub inne elementy języka programowania, które zostały wycofane z ogólnego użytku lub ich zastosowanie jest niewskazane³. Taka praktyka może powodować błędy lub luki w tworzonej oprogramowaniu. Studenci przyzwyczajeni do korzystania z takich funkcji lub praktyk tworzą kod podatny na ataki. Przykładem tego typu funkcji są `strcpy()` i `gets()` w języku C⁴.*
 -  *Studenci uczeni są programowania z naciskiem na dobre praktyki programowania, będąc równolegle świadomymi wad i luk w używanych przez nich językach programowania.*
 -  *Kadra powinna na bieżąco monitorować trendy i informacje dotyczące luk bezpieczeństwa w wykładanych przez nich językach programowania. Wszelkie informacje dotyczące luk w danym języku programowania mogłyby zostać przedstawione w formie ciekawostek na zajęciach. W trakcie nauki, w przypadku wykorzystania niebezpiecznych funkcji lub powielania niezalecanych praktyk programowania prezentowanych przez wykładowców, studenci powinni być zawsze informowani o zagrożeniach i konsekwencjach ich użycia. Kluczowym jest, by od początku nauki danej technologii słuchacze byli uczeni tworzenia bezpiecznego i wolnego od błędów kodu.*
-
-  *Wykładowcy przedmiotów związanych z tworzeniem aplikacji internetowych, systemów operacyjnych lub baz danych nie kładą należytego nacisku na dobre praktyki i techniki przeciwdziałania atakom i wykorzystaniu luk w tworzonej programie. Gromadzona przez studentów wiedza na temat technologii internetowych nie obejmuje informacji dotyczących praktyk bezpiecznego programowania, wymaganych w tworzonych komercyjnie aplikacjach internetowych⁵. W wykładanych przedmiotach poświęca się też za mało uwagi tematami takim jak replikacja danych, systemy o wysokiej dostępności i innym technologiom, które umożliwiają efektywne tworzenie kopii zapasowych oraz zapewniają ciągłość działania w razie ataku lub awarii.*
 -  *Przekazywanie studentom dobrych praktyk tworzenia bezpiecznych aplikacji internetowych oraz zapoznanie słuchaczy z częstymi atakami w technologiach internetowych lub bazodanowych. Studenci znają techniki replikacji i propagacji danych oraz tworzenia kopii zapasowych. Umieją konfigurować macierze RAID oraz znają podstawy konceptu baz danych o wysokiej dostępności.*
 -  *Przedmioty związane z bazami danych poza odmianami SQL powinny poruszać koncept systemów i baz danych o wysokiej dostępności takie jak np. Dynamo⁶. Nauczyciele akademicki winni wzbogacić przedmioty związane z systemami operacyjnymi o techniki replikacji danych i tworzenia kopii zapasowych. W wyniku czego studenci pozyskają wiedzę nt. zalecanych reguł tworzenia kopii zapasowych, takie jak np. 3-2-1 Backup Rule⁷. Kadra powinna przywiązywać dużą wagę do tworzenia bezpiecznego kodu aplikacji internetowych oraz prezentować studentom (na przykładach) znane ataki na aplikacje internetowe oraz sposoby przeciwdziałania.*

³Ajay Bandi, Abdelaziz Fellah, i Harish Bondalapati, „Embedding Security Concepts in Introductory Programming Courses” (School of Computer Science and Information Systems Northwest Missouri State University Maryville, b.d.), <https://www.nwmissouri.edu/csis/msacs/PDF/Fall%202019/p78-bandi.pdf>.

⁴Robert C. Seacord, Secure Coding in C and C++ (2nd. ed.) (Addison-Wesley Professional, 2013).

⁵„De Zan, Tommaso & Franco, Fabio. (2020). Cybersecurity skills development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database.”

⁶Amazon, „Dynamo: Amazon's Highly Available Key-value Store”, b.d., <https://www.allthingsdistributed.com/files/amazon-dynamo-sosp2007.pdf>.

⁷„3-2-1 Backup Rule: The Rule of Thumb to Solve Your Data Loss Problems”, udostępniono 29 lipiec 2020, <https://securityboulevard.com/2020/05/3-2-1-backup-rule-the-rule-of-thumb-to-solve-your-data-loss-problems/>.

REKOMENDACJE DOMENA IT



Nauka projektowania rozwiązań informatycznych zogniskowana jest zwykle na zapewnieniu odpowiednich funkcjonalności pod kątem użytkowym (User Experience – UX). W procesie projektowania brak nacisku na dostarczenie funkcjonalności, które są odpowiednio zabezpieczone pod kątem cyberbezpieczeństwa. Proces projektowania funkcjonalności oraz interfejsu użytkownika (UI) często ogranicza się do spełnienia wymagań projektowych. Powoduje to tworzenie aplikacji, które mogą być z pozoru przyjazne użytkownikowi, jednak często pomijana jest w nich kwestia zastosowania odpowiednich zabezpieczeń. Przeważnie kwestia bezpieczeństwa rozwiązań informatycznych jest ściśle kojarzona z back-endem, czyli techniczną implementacją funkcjonalności w warstwie przetwarzania danych, jednak część odpowiedzialna za interfejs użytkownika oraz doświadczenia użytkownika jest równie istotna⁸.



Absolwenci kierunków informatycznych posiadają wiedzę na temat dobrych praktyk i technik projektowania funkcjonalności, które nie prowadzą do luk w bezpieczeństwie działania logiki aplikacji. Posiadają wiedzę na temat projektowania UX i UI zarówno intuicyjnego, ergonomicznego, użytecznego, jak i zapobiegającego wykonywaniu przez użytkownika działań mogących narazić jego dane na szkodę - utratę lub przechwycenie.



W przedmiotach, skupiających się na procesie projektowania systemów informatycznych lub posiadających takie elementy, powinno kłaść się większy nacisk na zabezpieczenie tworzonych rozwiązań. Uwzględnienie bezpieczeństwa w procesie projektowania UX i UI winno stanowić jeden z początkowych etapów projektowania rozwiązania. Rozbudowane systemy, które są w zaawansowanym stadium implementacji, są zdecydowanie trudniejsze i bardziej kosztowne w kontekście uzupełnienia braków w bezpieczeństwie konkretnych funkcjonalności.

Jednocześnie należy pamiętać, iż zbyt rozbudowane mechanizmy zapewnienia bezpieczeństwa mogą prowadzić do nadmiernego skomplikowania sposobu działania użytkownika w systemie. W takich sytuacjach częstą praktyką użytkowników jest próba wyłączenia lub omijania uciążliwych zabezpieczeń. Dla użytkownika systemu najważniejsze jest, by mechanizmy zapewniające bezpieczeństwo działały w jak najmniej widoczny sposób. W tym kontekście ważny jest także aspekt finansowy – im więcej czasu użytkownik przeznacza na spełnienie wymagań bezpieczeństwa, tym droższa jest praca w systemie. W podejściu do projektowania UX/UI konieczne jest więc zachowanie równowagi pomiędzy ergonomicznością, przejrzystością i intuicyjnością a zastosowaniem odpowiednich zabezpieczeń. Nie można jednak z tego równania wykluczyć aspektu cyberbezpieczeństwa.



Programy nauczania na kierunkach informatycznych często nie zawierają tematyki związanej z technikami przeprowadzenia ataków na systemy sieciowe. Częstym jest, iż specjaliści IT, nawet z dużym doświadczeniem w komercyjnym wytwarzaniu i administrowaniu oprogramowaniem, nie mieli styczności z praktycznym przeprowadzaniem ataków na systemy informatyczne. W Stanach Zjednoczonych w programach nauczania jedynie 1 na 36 najlepszych kierunków informatycznych wymaga od studentów zaliczenia przedmiotu związanego z cyberbezpieczeństwem⁹.



Absolwenci kierunków informatycznych posiadają teoretyczną oraz praktyczną wiedzę na temat sposobów przeprowadzania ataków na systemy informatyczne. Dzięki tej wiedzy są w stanie lepiej projektować i programować rozwiązania zabezpieczone pod kątem cyberbezpieczeństwa.

⁸ DARKreading, „User-Friendly Cybersecurity: Is a Better UX the Key to a Better Defense?”, udostępniono 29 lipiec 2020, https://www.darkreading.com/edge/theedge/user-friendly-cybersecurity-is-a-better-ux-the-key-to-a-better-defense-/b/did/1337699?_mc=rss%

⁹ Krutz, Daniel & Richards, Thomas., „Cyber security education: why don't we do anything about it?”, ACM Inroads, 8(4):5-5, 10.1145/3132217 (2017).

REKOMENDACJE DOMENA IT



Program nauczania powinien być rozszerzony o moduły lub nowe przedmioty skupiające się na praktycznych sposobach atakowania systemów informatycznych. Zajęcia winny obejmować zarówno aspekty teoretyczne, jak i praktyczne. Teoria powinna zawierać informacje odnośnie najczęściej wykorzystywanych typów ataków oraz tego, z jakimi aspektami działania systemów informatycznych się one wiążą - np.: przesył danych z wykorzystaniem protokołów HTTP/TCP, obsługa bazy danych czy informacje tymczasowe przechowywane w przeglądarkach lub plikach programów. W zajęcia praktyczne w integrowane powinny zostać próby ataków na przygotowane systemy informatyczne obciążone typowymi lukami w zabezpieczeniach. Symulacje powinny być reprezentatywne dla realiów rynkowych. Dodatkowy element zajęć stanowić może aspekt zabezpieczenia atakowanych aplikacji. Przykład atakowanej, w ramach zajęć aplikacji to WebGoat¹⁰, zawiera ona typowe podatności oraz informacje o nich.

WSPÓŁAUTORZY RAPORTU „DOMENA IT”

Natalia Bronder — Wydział Elektrotechniki Automatyki i Informatyki, Politechnika Opolska
Irmína Chmielowska — Wydział Podstawowych Problemów Techniki, Politechnika Wrocławska
Paweł Cyprys — Wydział Podstawowych Problemów Techniki, Politechnika Wrocławska
Jakub Czyszczonik — Wydział Podstawowych Problemów Techniki, Politechnika Wrocławska
Bartosz Drzazga — Wydział Podstawowych Problemów Techniki, Politechnika Wrocławska
Piotr Dudek — Wydział Inżynierii Elektrycznej i Komputerowej, Politechnika Krakowska
Mateusz Gąsior — Wydział Informatyki, Elektrotechniki i Automatyki, Uniwersytet Zielonogórski
Mariusz Górny — Wydział Inżynierii Elektrycznej i Komputerowej, Politechnika Krakowska
Mateusz Jachniak — Wydział Podstawowych Problemów Techniki, Politechnika Wrocławska
Michał Kobielski — Wydział Mechaniczny Technologiczny, Politechnika Śląska
Kilian Koziół — Wydział Matematyki i Informatyki, Uniwersytet Warmińsko-Mazurski w Olsztynie
Emanuel Krzysztoń — Kolegium III Uniwersytet Kazimierza Wielkiego w Bydgoszczy
Piotr Ładoński — Wydział Elektrotechniki, Elektroniki, Informatyki i Automatyki, Politechnika Łódzka
Grzegorz Maksim — Wydział Elektrotechniki i Informatyki, Politechnika Lubelska
Rafał Sawicki — Wydział Podstawowych Problemów Techniki, Politechnika Wrocławska
Gabriel Tański — Wydział Podstawowych Problemów Techniki, Politechnika Wrocławska
Jan Ziemniewicz — Wydział Informatyki i Telekomunikacji, Politechnika Poznańska

¹⁰ OWASP WebGoat, „Learn the hack - Stop the attack”, udostępniono 29 lipiec 2020, <https://owasp.org/wwwproject-webgoat/>.



” dr inż. Wojciech Wodo

Gratuluję studentom dobrze i skrupulatnie przeprowadzonej analizy. Płynące z niej wnioski i rekomendacje pokrywają się z opiniami ekspertów z branży cyberbezpieczeństwa (vide cytowane raporty). Zaprezentowane aspekty usprawnienia edukacji w zakresie cyberbezpieczeństwa poparte są konkretnymi pomysłami i rozwiązaniami.

Dynamika rozwoju technologii wpływa na szybką dezaktualizację wiedzy i stosowanych rozwiązań. Obecnie jedno z najważniejszych zagrożeń stanowi ignorowanie tego faktu przez użytkowników. Remedium na ten stan rzeczy powinien być stały element edukacyjny podnoszący świadomość w domenie cyberbezpieczeństwa (awareness training).

Tak jak niegdyś umiejętność obsługi komputera była rzadkością, a dziś jest obowiązkiem, tak obecnie powinniśmy zdefiniować nowe kompetencje człowieka przyszłości, a może już człowieka teraźniejszości (człowieka funkcjonującego w przestrzeni dwóch światów: realnego i cybernetycznego). Do zbioru tych kompetencji będzie należeć m.in. poruszanie się po cyfrowym świecie i korzystanie z jego usług w sposób świadomy i bezpieczny. Dziś nikogo nie dziwi płatność bezgotówkowa smartfonem czy zegarkiem, wysyłanie zeznania podatkowego przez Internet czy składanie wniosków podpisanych profilem zaufanym przez ePUAP, ale czy rozumiemy jakie niebezpieczeństwa są związane z tymi usługami i jak ich uniknąć?

Studenci wskazali phishing jako jeden z fundamentalnych ataków w dzisiejszym cyberświecie. Jest to proceder prowadzony w zautomatyzowany sposób na masową skalę, ale to tylko czubek góry lodowej. Koniecznym jest zdefiniowanie umiejętności i nowych kompetencji, które powinien posiadać każdy korzystający z internetu i cyfrowych usług. Kluczowe jest również wdrożenie programu kształcenia w tym temacie od samego początku systemu edukacji (szkoły podstawowej).

Autorzy poruszyli również problem związany z niewystarczającym poziomem dydaktyki w zakresie cyberbezpieczeństwa w kursach na kierunkach ICT. Jako nauczyciel akademicki muszę się z tym zgodzić, jednakże z drugiej strony musimy spojrzeć na problem szerzej.

Jeśli podejmiemy decyzję o włączeniu pewnych elementów kształcenia do kursów, to koniecznym staje się usunięcie z nich innych treści, gdyż liczba godzin jest ściśle określona przez standardy kształcenia. Kolejna sprawa dotyczy tego czy powinniśmy uczyć większej liczby elementów ale mniej szczegółowo (podejście T-shape), czy może węższej grupy elementów, za to bardziej szczegółowo (I-shape). Niestety oba wspomniane podejścia wykluczają się nawzajem. Ważna jest też kwestia z jakim poziomem wiedzy i świadomości studentów pracujemy, kiedy przychodzą na uczelnię. Jeśli na poprzednich etapach edukacji nie zdobędą oni podstaw, to nie ma na czym oprzeć dalszych elementów wiedzy i umiejętności.

W pełni podpisuję się pod rekomendacjami studentów odnoszącymi się do minimalizacji uprawnień użytkowników i wprowadzaniu polityk typu (least privilege policy) czy podejścia opt-in, nie opt-out. Z zasady powinniśmy ograniczać uprawnienia użytkowników do niezbędnego minimum, a jeśli pojawia się konieczność ich eskalowania, to decyzję powinna podejmować odpowiednia osoba na wniosek zainteresowanej strony.

Projektując i tworząc systemy informatyczne powinno uwzględniać się aspekty bezpieczeństwa od samego początku procesu projektowego, na równi z innymi elementami wchodzącymi w skład systemu. Podejście security, safety and privacy by design zapewni nam, że funkcje bezpieczeństwa nie będą doklejane na szybko po zbudowaniu całego rozwiązania, zaś będą integralną i przemyślaną częścią całości. Jeśli nie nauczymy naszych absolwentów kierunków informatycznych, elektronicznych, telekomunikacyjnych i pokrewnych takiego podejścia, to sami sobie szykujemy tykającą bombę.

Wojciech Wodo

Asystent w Katedrze Podstaw Informatyki Politechniki Wrocławskiej,
laureat TOP 500 Inovators, stypendysta Uniwersytetu Kalifornijskiego Berkley.



Milena Bobińska

Wojskowa Akademia Techniczna
Wydział Bezpieczeństwa, Logistyki i Zarządzania

REKOMENDACJE DOMENA BIZNES

Materiał źródłowy zgromadzony w ramach analizy programów nauczania, dokonanej w kooperacji studentów z ośmiu wydziałów biznesowo-ekonomicznych. Reprezentowane uczelnie: Uniwersytet Gdański, Uniwersytet Łódzki, Uniwersytet Marii Curie-Skłodowskiej w Lublinie, Uniwersytet Mikołaja Kopernika w Toruniu, Politechnika Poznańska, Politechnika Rzeszowska, Uniwersytet Warmińsko-Mazurski, Uniwersytet Wrocławski.

Aktualny stan nauczania na temat cyberbezpieczeństwa

Edukacja w dziedzinie cyberbezpieczeństwa jest obecnie kluczowa. Studenci kierunków biznesowo-ekonomicznych powinni posiadać wiedzę, pozwalającą im na skuteczne rozumienie procesu zarządzania cyber-ryzykiem oraz wyrobienie umiejętności reagowania na zagrożenia pochodzące z cyberprzestrzeni. Podejmowane, w tym zakresie, na uczelniach pionierskie inicjatywy edukacyjne i czynione próby implementacji zagadnienia do programów nauczania, stanowią bazę do promocji problematyki wśród kadry akademickiej i społeczności studenckiej.

Z przeprowadzonych analiz wynika, że 4 na 10 studentów kierunków biznesowych ma styczność, w toku nauki, z zagadnieniami związanymi z cyberbezpieczeństwem. Przez to stwierdzenie rozumieć należy pojawienie się tematyki na przedmiotach danych kierunków, np. Ekonomia, Finanse i Rachunkowość czy Zarządzanie. Z kolei 2 na 10 studentów stwierdza, że na ich wydziałach, w ramach innych niż studiowane przez nich kierunki, realizowane są przedmioty powiązane z tematyką cyberbezpieczeństwa.

Powyższe statystyki wskazują na brak wystarczającej uwagi w zakresie rozwoju sylabusów programowych pod kątem implementacji kontekstu dynamicznie postępującego procesu cyfryzacji. Nowoczesna edukacja wymaga, by przekazywana wiedza była jak najbardziej aktualna (poruszała trendy światowe), a proces jej transferu uwzględniał aspekt łatwości przyswojenia materiału dla studentów.

W naszej opinii nauczanie o cyberbezpieczeństwie wymaga zaadresowania poniższych kwestii, które traktować należy w kategoriach wyzwań stojących przed systemem edukacji:

- uwzględnienie tematyki cyberbezpieczeństwa na kierunkach biznesowo-ekonomicznych w całej Polsce, obecnie domena jest pomijana,
- implementację zagadnień związanych z cyberbezpieczeństwem w materiale omawianym na przedmiotach ściśle powiązanych z tą tematyką lub stanowiących dobre miejsce na ich ekspozycję, np.: Informatyka dla Ekonomistów, Technologie Informacyjne, Informatyka i Systemy Informacyjne Zarządzania, Informatyka w Zarządzaniu,
- podjęcie przez uczelnie współpracy z wyspecjalizowaną w temacie kadrą,
- wykorzystanie potencjału kadry z kierunków IT (danej uczelni) do edukacji studentów kierunków biznesowych,
- wkomponowanie tematyki cyberbezpieczeństwa w organizowane na uczelniach symulacje biznesowe,
- umożliwienie studentom wyboru tematyki pracy dyplomowej w temacie cyberbezpieczeństwa w ujęciu funkcjonowania organizacji biznesowych.

REKOMENDACJE DOMENA BIZNES

W kontekście podejmowania wyzwań warto wskazać na uczelnie, gdzie podnoszona jest omawiana problematyka:

- *specjalizacja Cyberbezpieczeństwo na kierunku Bezpieczeństwo Wewnętrzne oraz kierunek studiów podyplomowych Cyberbezpieczeństwo i Ochrona Zasobów Informacyjnych na Politechnice Rzeszowskiej,*
- *przedmiot Cyberbezpieczeństwo na kierunku Finanse i Rachunkowość na Uniwersytecie Ekonomicznym we Wrocławiu, przedmiot Cyberprzestrzeń Szanse i Zagrożenia - Podstawowe Zagadnienia na Uniwersytecie Marii Curie-Skłodowskiej w Lublinie,*
- *obecność elementów nauk o cyberbezpieczeństwie w sylabusach przedmiotów pokrewnych, np.: Bankowość na Uniwersytecie Ekonomicznym we Wrocławiu oraz Zwalczanie Przestępczości i Ochrona Własności Intelektualnej na Politechnice Rzeszowskiej,*
- *obecność kadry posiadającej specjalistyczną wiedzę, umożliwiającą kształcenie studentów w dziedzinie cyberbezpieczeństwa - kontekst przedsiębiorstw i finansów na Uniwersytecie Ekonomicznym we Wrocławiu,*
- *inicjowanie współpracy między uczelniami a przedsiębiorstwami, w tym podnoszące temat wydarzenia na Uniwersytecie Ekonomicznym we Wrocławiu.*

Funkcjonujące na uczelniach, o profilu biznesowo-ekonomicznym, podejście do tematyki cyberbezpieczeństwa wymaga podjęcia działań naprawczych. W ujęciu holistycznym, w systemie edukacji zauważalny jest brak wielu podstawowych elementów, bez których niemożliwe jest wykształcenie nowoczesnej kadry menadżerskiej, rozumiejącej mechanizmy operowania ekosystemu cyberbezpieczeństwa. Jak przedstawiamy powyżej występują też pozytywne, aczkolwiek tyczą się one pojedynczych uczelni i nie mają odzwierciedlenia w całościowym ujęciu problemu.

Główne kierunki koniecznych zmian

Prezentowana przez nas ta część raportu, ma na celu zwrócenie uwagi środowiska akademickiego uczelni biznesowo-ekonomicznych na aspekt implementacji w programach nauczania problematyki dotyczącej cyberbezpieczeństwa, jako kluczowego wyzwania dla biznesu w erze transformacji na gospodarkę 4.0. Proces ten został znacząco przyspieszony przez pandemię koronawirusa COVID-19^{11 12}.

Przegląd, pod tym kątem programów nauczania, ma także swoje umocowanie w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, adresującej interdyscyplinarne ujęcie procesu edukacji związanej z problematyką cyberbezpieczeństwa – od edukacji wczesnoszkolnej po uczelnie wyższe. W dokumencie kładziony jest nacisk na obszary zarządzania bezpieczeństwem informacji, ochronę danych osobowych, czy rozwój nowych technologii.

REKOMENDACJE DOMENA BIZNES

Współczesny, innowacyjny biznes wymaga zarówno nowatorskich rozwiązań, jak i wyspecjalizowanej kadry. Zwiększenie świadomości i wiedzy studentów w temacie cyberbezpieczeństwa, wywrze pozytywny wpływ na funkcjonowanie przedsiębiorstw, zarówno w skali mikro, jak i makro, poczynając od kwestii wykwalifikowanej, świadomej kadry, po zwiększenie konkurencyjności na arenie międzynarodowej¹³. Wiedza i promocja dobrych praktyk przyczynią się również do obniżenia ryzyka związanego z cyberatakami. W toku konsultacji zarysowaliśmy obszary, które należy zaadresować w programach studiów. Propozycje wynikają z analizy zmian w funkcjonowaniu przedsiębiorstw w wyniku postępującego procesu cyfryzacji.

1 — Edukacja z zakresu bezpiecznego poruszania w sieci

Dydaktyka, zarówno wykłady, jak i ćwiczenia powinny uwzględniać klasyfikację i podstawowe kategorie funkcjonujących cyberataków np. phishing, ransomware, malware, wirusy na telefon oraz zapoznawać słuchaczy z przebiegiem ww. ataków, ich następstw i sposobów prewencji.

Kluczowymi są zagadnienia związane z zabezpieczeniem danych wrażliwych oraz kont internetowych, bezpieczeństwem hasła (prezentacja narzędzi do ich tworzenia i przechowywania) oraz zapoznanie z rozwiązaniami typu virtualna sieć prywatna VPN (Virtual Private Network).

Istotną jest także tzw. self-education, mogąca odbywać się poprzez rekomendację przez prowadzących zaufanych portali tematycznych, traktujących o tematyce.

2 — Uwzględnienie roli audytów

Zwiększenie świadomości o wadze audytów oraz ich wpływie na aspekt cyberbezpieczeństwa w organizacjach.

3 — Dokumentacja i akty prawne dotyczące cyberbezpieczeństwa

Zaznajomienie studentów z najważniejszymi regulacjami (Dyrektywa NIS, Rozporządzenie RODO, Ustawa o krajowym systemie cyberbezpieczeństwa), dokumentami i jednostkami organizacyjnymi funkcjonującymi w ramach zarządzania ekosystemem cyberbezpieczeństwa (CSIRT-y, CERT, operator infrastruktury krytycznej, dostawca usług kluczowych).

¹¹Deloitte, „«Nowa normalność» dla sektora usług finansowych w Polsce, Europie i Azji”, https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Brochures/pl_FSI_Webinar_odcinek_nr_2_30.04_final.pdf.

¹² 300RESEARCH, „Efekt zamrożenia. Szansa na radykalną cyfryzację gospodarki”, b.d., https://impactcee.com/reaction/2020/wp-content/uploads/2020/06/raport_cyfryzacja_final.pdf

¹³KPMG, „Barometr cyberbezpieczeństwa. W kierunku rozwiązań chmurowych”, b.d., <https://home.kpmg/content/dam/kpmg/pl/pdf/2020/06/pl-raport-kpmg-barometr-cyberbezpieczenstwa-2020-wkierunku-rozwiazan-chmurowych.pdf>.

REKOMENDACJE DOMENA BIZNES

4 — Dane osobowe w sieci

Wyeksponowanie zagadnienia danych poufnych, umieszczanych w sieci i roli administratorów w procesie właściwego ich zabezpieczenia, na podstawie rozporządzenia RODO.

5 — Zarządzanie kryzysowe i ciągłość działania

Wykorzystanie w edukacji studiów przypadków, zapoznających słuchaczy ze schematami reakcji zarządzania cyberkryzysem, z uwzględnieniem rodzaju zaatakowanego podmiotu. Zwrócenie uwagi na kwestie: zgłoszenia incydentu, zastosowania prewencyjnych zabezpieczeń na przyszłość, wprowadzenie systemu dobrych praktyk po ataku.

6 — Elementy cyberkryzysów w symulacjach biznesowych

Ujęcie zagadnień związanych z cyberzagrożeniami w symulacjach biznesowych dla studentów, w trakcie których zarządzają wirtualnym przedsiębiorstwem. Powyższe sugestie wskazują na potrzebę nowelizacji programów nauczania. Oparty na technologii 5G rozwój przemysłu 4.0 stanowi impuls dla systemu edukacji do wprowadzenia koniecznych modyfikacji. Proponowane kierunki zmian, mają na celu wyposażenie przyszłych absolwentów w kompetencje, które pozwolą, im z sukcesem, funkcjonować w konkurencyjnym otoczeniu kreowanym przez gospodarkę cyfrową.

REKOMENDACJE DOMENA BIZNES

Opisane poniżej wyzwania wraz z propozycjami ich zaadresowania
oznaczone są piktogramami



Wyzwanie



Stan Pożądany



Rekomendacje



Brak elementów związanych z tematyką cyberbezpieczeństwa w symulacjach biznesowych typu TEES 6, przeprowadzanych na uczelniach w ramach zajęć obligatoryjnych.



Po zakończeniu symulacji uczestnicy są świadomi, zagrożeń i strat jakie może spowodować cyberatak w firmie (różna struktura własności przedsiębiorstw, w tym notowane na giełdzie). Studenci poznają skutki ataku, rozumieją proces zarządzania kryzysem, w tym elementy klasyfikacji incydentu i jego zgłoszenia (CSIRT NASK, CSIRT MON, CSIRT GOV).



Wywołanie w trakcie ćwiczenia zdarzenia losowego „atak hakerski”. W ramach decyzji menedżerskiej studenci adresują atak, tj. zgłaszają incydent do odpowiedniego podmiotu, decydują o zatrudnieniu dodatkowych specjalistów w celu zwalczania skutków ataku oraz poniesieniu nakładów finansowych na zabezpieczenia, mające na celu chronić firmę przed potencjalnymi atakami w przyszłości.



Niepoświęcanie należytej uwagi edukacji dotyczącej audytów systemów ochrony danych funkcjonujących w przedsiębiorstwach oraz tematów zabezpieczenia systemów informatycznych.



Studenci są świadomi wagi audytów oraz znają podstawowe sposoby zabezpieczania systemów i informacji w organizacji. Zapoznani są także z kwestią zarządzania ryzykiem oraz dobierania odpowiednich akcji korygujących, dopasowanych do typu wykrytych błędów lub potencjalnych zagrożeń. Słuchacze posiadają wiedzę na temat testów penetracyjnych, ich typów oraz zasadności ich przeprowadzenia w przedsiębiorstwach.



Rozszerzenie zakresu materiału o zajęcia omawiające typy audytów, planowanie i organizację systemów IT w przedsiębiorstwach, testy penetracyjne czy zarządzanie ryzykiem w takich systemach. Wdrożenie zajęć praktycznych lub symulacyjnych, imitujących przeprowadzanie tego typu audytów i pentestów (black box, white box i gray box) wraz z wyróżnieniem najważniejszych elementów dotyczących kontroli systemów IT.



Studenci nie otrzymują podstawowej wiedzy nt. bezpiecznego zachowania się w sieci oraz zabezpieczenia swoich danych na smartfonach, komputerach, kontach bankowych i platformach internetowych.



Rozpoczynając pierwszy roku studiów student winien uzyskać wiedzę nt. cyberbezpieczeństwa w sieci. Powinien być także świadomym użytkownikiem Internetu – wiedzieć na jakie typy ataków może być narażony, jak się przed nimi zabezpieczyć, jakimi narzędziami chronić swoje dane wrażliwe czy hasła.



Odbycie przez studentów (na początku pierwszego semestru studiów) szkolenia z podstawowych zasad cyberbezpieczeństwa (2-3 godziny). Zajęcia o charakterze zbliżonym do szkolenia BHP. Udośtępnienie kursów online prezentujących podstawowe cyberataki (phishing, ransomware, malware, wirusy na telefon). Rozwinięcie wiedzy na temat bezpiecznego poruszania się w Internecie oraz sposobów zabezpieczania wrażliwych danych (m.in. VPN i menedżery haseł) powinno zostać wpisane w programy nauczania przedmiotu takiego jak Technologia Informatyczna.

REKOMENDACJE DOMENA BIZNES



Studenci, jako przyszli przedsiębiorcy i menedżerowie, posiadają nikłą wiedzę nt. zabezpieczeń chroniących firmy przed atakami. Według raportu AON Polska w perspektywie trzech lat cyberataki i naruszenia danych będą kluczowym ryzykiem dla przedsiębiorstw działających w Europie. Istotną kwestię stanowi ryzyko dotyczące cyberprzestrzeni oraz różnica w pojmowaniu jego znaczenia w Polsce i na świecie. Polscy przedsiębiorcy uplasowali cyberataki oraz naruszenia danych na 23. miejscu w rankingu ryzyk mogących dotknąć firmę. W rankingu globalnym w perspektywie 2020-23 ryzyko to utrzymuje swoją silną pozycję w pierwszej piątce (4 pozycja Europa, 3 pozycja świat)¹⁴.



Mając na względzie fakt, iż obecnie dane uznawane są jako nowy, strategiczny surowiec, studenci – przyszła kadra menadżerska muszą być świadomi ryzyka związanego z występowaniem cyberataków, znać ich rodzaje, procedury postępowania podczas kryzysu, w tym aspekty dotyczące ciągłości działania oraz rozumieć kompetencje interesariuszy działających w strukturze ekosystemu cyberbezpieczeństwa¹⁵.



Wprowadzenie do sylabusów przedmiotów takich jak Zarządzanie czy Finanse i Rachunkowość, elementów związanych z tematyką cyberbezpieczeństwa. Wykładowcy powinni uświadamiać studentów o konieczności zabezpieczeń przed cyberatakami. W celu osiągnięcia jak najlepszych efektów kształcenia w tym zakresie, warto by uczelnie rozważyły współpracę z profesjonalnymi firmami zajmującymi się cyberbezpieczeństwem, by przedstawiać studentom realne zagrożenia w postaci scenariuszy czy opisów bieżących studiów przypadków. Uczelnie mogłyby także współfinansować certyfikaty EITCA – Europejskiej Akademii Certyfikacji Informatycznej¹⁶, w szczególności te skierowane do biznesu jak EITC/IS/EEIS Bezpieczeństwo informatyczne w gospodarce elektronicznej¹⁷.



Ograniczony wymiar godzin uniemożliwia prowadzącym szczegółowe zaadresowanie tematyki cyberbezpieczeństwa.



Studenci mają stworzoną możliwość udziału w spotkaniach rozwijających tematykę cyberbezpieczeństwa, współorganizowanych przez organizacje studenckie i koła naukowe: warsztaty i prelekcje (współpraca z profesjonalnymi firmami lokalnymi, zajmującymi się cyberbezpieczeństwem).



Władze uczelni aktywizują i wspierają organizacje studenckie, rekomendując przygotowanie wydarzeń o tematyce cyberbezpieczeństwa. Koła naukowe i organizacje studenckie mogą organizować spotkania z ekspertami w ramach działalności statutowej. Uczelnie w celu aktywizacji mogłyby udzielać grantów na realizację ww. celów.



Na przedmiotach związanych z zarządzaniem nie występują elementy zarządzania ryzykiem w przedsiębiorstwie w kontekście cyberbezpieczeństwa.



Studenci, jako przyszła kadra menadżerska, są świadomi, że każda firma jest narażona na ryzyko związane z cyberprzestępczością. Potrafią zidentyfikować to ryzyko, ocenić prawdopodobieństwo jego wystąpienia, ocenić straty, które może przynieść (zarówno w aspekcie materialnym i niematerialnym) sterować nim, monitorować i kontrolować – zgodnie z definicją zarządzania ryzykiem.



Aktualizacja programu nauczania o najczęściej występujące źródła ryzyka powiązanego z cyberbezpieczeństwem w przedsiębiorstwach, planowanie reakcji na ryzyko w procesie rozwiązywania zadań typu studium przypadków. Upowszechnienie wiedzy o rekomendowanym posiadaniu w przedsiębiorstwie zestawu materiałów antykryzysowych tzw. crisis pack.

¹⁴ AON Polska, „Zarządzanie ryzykiem i Ubezpieczeniami w Firmach w Polsce- Edycja VI”, b.d., https://aoncomauthoring.blob.core.windows.net/aoncom2017media/aon.com/media/poland/publikacje/raport%202019-2020/raport-grms-polska-2019-20.pdf?utm_source=Aoncom.

¹⁵ Ministerstwo Rozwoju, „Raport Nowy Surowiec - otwarte zasoby danych dla polskiej gospodarki”, b.d., <https://www.gov.pl/web/rozwoj/raport-nowy-surowiec-otwarte-zasoby-danych-dla-polskiej-gospodarki>.

¹⁶ EITCA, „EITCA”, udostępniono 29 lipiec 2020, <https://eitca.pl/is>.

¹⁷ EITCA, „Certyfikat EITC/IS/EEIS”, udostępniono 29 lipiec 2020, <https://pl.eitca.org/certyfikacja/eitciseeigospodarka-elektroniczna-bezpiecze%C5%84stwo-informacji/?v=9b7d173b068d>.

REKOMENDACJE DOMENA BIZNES



Brak świadomości na temat możliwości ubezpieczenia się przed zdarzeniami w cyberprzestrzeni.



Studenci zdają sobie sprawę, że istnieje możliwość transferu ryzyka związanego z cyberbezpieczeństwem. Wiedzą, jak korzystnie skonstruować umowę ubezpieczenia z uwzględnieniem np. utraty przychodów na skutek przerwania ciągłości działania jako następstwa ataku hakerskiego.



Wzbogacenie treści przedmiotów związanych z ubezpieczeniami o informacje związane z transferem ryzyka płynącego z cyberataków.



W procesie nauczania nie poruszany jest temat kosztów, które firma musi ponieść w związku z cyberatakiem. Brakuje również danych o nakładach ponoszonych przez przedsiębiorstwa na rzecz bezpieczeństwa w cyberprzestrzeni.



Studenci mają świadomość, że cyberatak na przedsiębiorstwo jest kosztotwórczy, a negatywne skutki finansowe incydentów mogą być znaczące. Dotyczą one m.in. roszczeń finansowych ze strony osób trzecich (naruszenie rozporządzenia RODO), kosztów związanych z zarządzaniem kryzysowym, utratą przychodu na skutek przerwania ciągłości działania, przywróceniem lub odtworzeniem utraconych danych. Studenci rozumieją koncepcję prewencji, w myśl której koszty działań dążących do poprawy bezpieczeństwa firmy w sieci powinny zostać przewidziane w budżecie.



Prezentacja kosztów, powstałych w wyniku cyberataku na przedsiębiorstwo i zestawienie ich z kosztami prewencji. Kwalifikacja kosztów związanych z obsługą incydentów mogłaby stanowić punkt w sylabusie przedmiotu Rachunkowość.



Brak ekspozycji w toku nauczania, w sposób jednoznaczny, zagadnienia wzrostu wartości aktywów niematerialnych w przedsiębiorstwach i skutków tego zjawiska.



Zrozumienie motywów i celów działania cyberprzestępców, wśród nich oprócz motywu stricte okupowego, wyeksponowanie aspektów dostępu do know-how przedsiębiorstwa, dobytku R&D, zniszczenia wizerunku i reputacji firmy.



Propagowanie teorii „nowej ekonomii”, w myśl której przewaga konkurencyjna przedsiębiorstw, ich innowacyjność i efektywność mają obecnie swoje źródło w aktywach niematerialnych.



Brak ekspozycji tematyki związanej z inżynierią społeczną, w tym m.in. socjotechnik wykorzystywanych przez cyberprzestępców.



Studenci posiadają wiedzę na temat stosowania środków psychologicznych i metod manipulacji mających na celu przekazanie lub wyłudzenie określonych informacji bądź nakłonienie do realizacji określonych działań. Ten typ menadżerskich kompetencji psychologicznych stanowi kluczowy element w procesie decyzyjności podczas zarządzania sytuacją kryzysową.



Wprowadzenie przedmiotu obejmującego ww. aspekty o nazwie „Psychologia w Biznesie” w kontekście prowadzenia nowoczesnego i skoncentrowanego na człowieku przedsiębiorstwa. Powyższe wątki można również zaimplementować do istniejących przedmiotów fakultatywnych.

REKOMENDACJE DOMENA BIZNES

WSPÓŁAUTORZY RAPORTU „DOMENA BIZNES”

Kamil Chmura — Wydział Ekonomiczny, Uniwersytet Marii Curie-Skłodowskiej w Lublinie

Marcin Guzek — Wydział Ekonomii i Finansów, Uniwersytet Ekonomiczny we Wrocławiu

Kamila Kiełczewska — Wydział Nauk Ekonomicznych, Uniwersytet Warmińsko-Mazurski w Olsztynie

Jadwiga Korsznia — Wydział Zarządzania, Politechnika Rzeszowska

Marta Lewandowska — Wydział Inżynierii Zarządzania, Politechnika Poznańska

Paweł Lewandowski — Wydział Zarządzania, Uniwersytet Ekonomiczny we Wrocławiu

Arkadiusz Wawrzyniak — Wydział Zarządzania w Spocie, Uniwersytet Gdański

Wojciech Zajączkowski — Wydział Ekonomii i Finansów, Uniwersytet Ekonomiczny we Wrocławiu



Adam Koniuszewski, FCPA, FCA, CFA

Po raz pierwszy, na skali międzynarodowej, spotykam się z taką inicjatywą. Czyni ona z autorów innowacyjnych trendsetterów. Raport ma potencjał, by stać się punktem odniesienia dla edukacji o cyberbezpieczeństwie na kierunkach biznesowych, nie tylko w Polsce, ale też za granicą. Przedstawiona analiza prezentuje szerokie spektrum praktycznych rekomendacji, od kwestii audytów przez ubezpieczenia od cyberkryzysów. Opracowanie świadczy o zrozumie-

niu założeń funkcjonowania gospodarki cyfrowej, gdzie podstawę stanowi stabilny ekosystem cyberbezpieczeństwa, do budowy którego kluczowym jest jak najszybszy wzrost świadomości omawianych zagadnień.

Ostatnie miesiące ujawniły wyraźny podział między, zmagającą się z trudnościami, tradycyjną gospodarką a prosperującą ekonomią 4.0 i jej bardzo dobrze rozwijającymi się platformami e-handlu, bankowości elektronicznej, e-zdrowia, usługami w chmurze, czy konferencjami online. Prawdziwy przełom, jednak, dopiero przed nami.

Rewolucja 5G, i będąca w planach 6G, radykalnie zwiększy możliwości sieciowe, eliminując opóźnienia transmisji danych. Sieć 5G to fundament umożliwiający funkcjonowanie smart cities, autonomicznych aut oraz inteligentnych fabryk. Zerowa latencja przeniesie wirtualną rzeczywistość poza granice świata gier komputerowych i wkroczy do mainstreamu, umożliwiając np. chirurgowi z Bostonu wykonanie operacji na pacjencie w Tokio przy użyciu telerobotyki. To będzie złota era Internetu Rzeczy (IoT), w której prawie niewyobrażalne dziś rozwiązania będą powszechne i staną się częścią naszej codzienności. Wkroczymy w nową epokę technologicznych innowacji, kreowania wartości i tworzenia dobrobytu.

Równolegle, z tymi imponującymi osiągnięciami, musimy jednak stawić czoła rosnącemu widmu cyberzagrożeń, na które żadne państwa, korporacje czy organizacje nie są odporne. Mimo, że temat cyberwyzwań coraz częściej zajmuje miejsce w agendach spotkań zarządów, w rzeczywistości organizacje walczą, próbując ochronić siebie i swoich klientów, a temat implementacji strategii cyberbezpieczeństwa do ogólnej strategii organizacji nadal jest wyzwaniem. W realiach cyfrowej transformacji zarządy nie zawsze zdają sobie sprawę z tego z czym muszą się zmierzyć, to generuje luki, które z kolei starają się wypełnić audytorzy, doradcy i branża ubezpieczeniowa.

Do realizacji założeń czwartej rewolucji przemysłowej, w cyberprzestrzeni potrzebujemy poczucia stabilności, przewidywalności i zaufania. Są one kluczowe dla bezpieczeństwa narodowego, dobrze prosperującego biznesu i sektora ochrony zdrowia. Dlatego cyberbezpieczeństwo powinno być uznane za podstawowe dobro publiczne, tak też rozumiane i promowane. W tym kontekście zachęcam również studentów do rozważenia znaczenia wagi etyki oraz aspektu szans i zagrożeń związanych z rozwojem sztucznej inteligencji - elementu niezbędnego w tworzeniu ekosystemu cyberbezpieczeństwa.

Adam Koniuszewski

Inwestor, wykładowca, Executive in Residence w Geneva Center for Security Policy (GSCP), Koordynator polskiego hubu ds. bezpieczeństwa przy Ambasadzie Szwajcarii w Polsce, Członek Światowej Akademii Nauki i Sztuki, założyciel fundacji The Bridge.



5 ZDROWIE



Anna Kowalczyk

Warszawski Uniwersytet Medyczny, Wydział Lekarski

REKOMENDACJE DOMENA MEDYCYN

Materiał źródłowy zgromadzony w ramach analizy programów nauczania, dokonanej w kooperacji studentów z jedenastu polskich uczelni medycznych. Reprezentowane uczelnie: Uniwersytet Medyczny w Białymstoku, Wyższa Szkoła Medyczna w Białymstoku, Collegium Medicum Uniwersytetu M. Kopernika w Bydgoszczy, Gdański Uniwersytet Medyczny, Collegium Medicum Uniwersytetu Jagiellońskiego, Uniwersytet Medyczny w Łodzi, Uniwersytet Opolski, Uniwersytet Warmińsko-Mazurski, Uniwersytet Medyczny w Warszawie, Uniwersytet Medyczny we Wrocławiu, Collegium Medicum Uniwersytetu Zielonogórskiego.

Aktualny stan nauczania na temat cyberbezpieczeństwa

Proces postępującej cyfryzacji w dziedzinie ochrony zdrowia, generuje dla funkcjonowania systemu zarówno wiele zalet, jak i wyzwań. Współdzielone systemy i bazy danych podmiotów leczniczych czy obsługa danych przez zagraniczne serwery wiążą się z licznymi, potencjalnymi zagrożeniami związanymi z cyberbezpieczeństwem.

Wykorzystując cyfrową rewolucję w celu poprawy jakości usług i efektywności zarządzania kosztami, sektor opieki zdrowotnej doświadcza równolegle rosnącej liczby problemów związanych z cyberbezpieczeństwem. Ze względu na wrażliwy charakter danych, jakimi dysponują podmioty sektora, naruszenia ich bezpieczeństwa mogą mieć poważne konsekwencje zarówno dla pacjentów, pracowników, jak i danej organizacji sektora.

Problemy te obejmują zarówno ataki związane ze złośliwym oprogramowaniem, które zagrażają integralności systemów i prywatności pacjentów, jak też ataki wykorzystujące rozproszoną odmowę usługi (DDoS- distributed denial-of-service attack), które zakłócają zdolność placówek do świadczenia opieki nad pacjentami.

Przyspieszenie procesu cyfryzacji wywołane zostało pandemią wirusa SARS-CoV. By nie doprowadzić do blokady sektora, rozpoczęto powszechne udzielanie porad medycznych telefonicznie i internetowo. Jeszcze przed pandemią wprowadzono obowiązkowe e-recepty (styczeń 2020 r.) oraz e-zwolnienia (grudzień 2018 r.). Wykorzystanie telemedycyny okazało się niezbędne do udzielania najszybszej, spersonalizowanej pomocy pacjentom, jednak fundamentem prawidłowego funkcjonowania takiego systemu jest staranna ochrona pozyskiwanych danych, regulowana przez rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne rozporządzenie o ochronie danych, tzw. RODO).

Dostępne opracowania jednoznacznie wskazują na ogromne trudności branży w adresowaniu wyzwań związanych z cyberbezpieczeństwem¹. Podczas gdy inne sektory infrastruktury krytycznej również są celami cyberataków, charakter branży opieki zdrowotnej podnosi wagę potencjalnych konsekwencji, które wykraczają poza straty finansowe lub naruszenie prywatności². Według Becker's Hospital Review naruszenia ochrony danych generują dla branży ochrony zdrowia koszty około 5,6 miliarda dolarów rocznie, a zgodnie z Report Breach Barometer:

¹ Clemens Scott Kruse i in., „Cybersecurity in healthcare: A systematic review of modern threats and trends”, *Technology and Health Care* 25, nr 1 (21 lutego 2017): 1–10, <https://doi.org/10.3233/THC-161263>.

² „CI Security”, <https://www.cisecurity.org>, dostęp: 02.08.2020

REKOMENDACJE DOMENA MEDYCYN

Year in Review w 2016 r. dochodziło do co najmniej jednego naruszenia ochrony danych zdrowotnych dziennie, które łącznie miały wpływ na ponad 27 milionów zapisów danych pacjentów³.

W innych branżach koszt cyberbezpieczeństwa może zostać przeniesiony na konsumenta. W ochronie zdrowia, gdzie marże są przeważnie niskie, a wykonywane usługi finansowane ze środków publicznych, świadczeniodawcy ponoszą koszty związane z zapewnieniem bezpieczeństwa danych⁴.

W związku z tym należyta ochrona informacji i związane z nią działania są przeważnie ignorowane przy planowaniu kosztów ogólnych działalności.

Jedne z najnowszych badań opublikowanych w JAMA Internal Medicine podają, że duża część zagrożeń bezpieczeństwa danych wrażliwych związana jest z nieprawidłowym postępowaniem personelu mającego kontakt z danymi - włączeniem ich w wiadomościach e-mailowych, wynoszeniem dokumentacji poza miejsce opieki czy przesyłaniem dokumentacji na prywatne urządzenia mobilne⁵. W związku z tym, najłatwiejszym i zarazem niskokosztowym rozwiązaniem, znacząco poprawiającym cyberbezpieczeństwo w placówkach ochrony zdrowia, jest edukacja personelu i osób na niższych etapach rozwoju kariery, w tym studentów kierunków medycznych i menedżerskich związanych z ochroną zdrowia. W celu określenia stanowiska studentów kierunków medycznych w tematyce wprowadzenia elementów cyberbezpieczeństwa w tok studiów oraz ustalenia stanu ich wiedzy w temacie, w ramach przygotowań do opracowania raportu (ankieta) uzyskano 190 odpowiedzi od studentów z 11 uczelni wyższych oferujących studia na kierunkach medycznych działających na terenie Polski. Według zdecydowanej większości osób (87,4%, n=166) temat cyberbezpieczeństwa powinien zostać poruszony w trakcie trwania edukacji na uczelni.

Wskazuje to na znaczne zainteresowanie tematem, który nie jest realizowany przez program studiów, gdyż tematyka ta została zwykle omówiona w trakcie zajęć jedynie u niewielkiego procenta badanych (18,4%, n=35). 90% respondentów (n=171) wskazuje, że widzą potencjalną możliwość włączenia tematyki cyberbezpieczeństwa do już istniejących przedmiotów, takich jak Bioinformatyka czy Prawo Medyczne.

Dane te nie oddają całkowitego zapotrzebowania studentów kierunków medycznych na rozszerzenie ich wiedzy o konkretne obszary związane z cyberbezpieczeństwem, stanowią jednak cenną wskazówkę o istotnej przydatności tych informacji w edukacji zawodowej. Cyfryzacji sektora medycznego powinna bezpośrednio towarzyszyć edukacja techniczna gwarantująca studentom zrozumienie i wagę postępu technologicznego w kontekście podejmowanego w przyszłości zawodu. Kadry medyczne winny mieć kontakt z podstawowymi zasadami cyberbezpieczeństwa i bezpiecznej obsługi infrastruktury informatycznej podmiotów świadczących usługi z zakresu ochrony zdrowia oraz otrzymywać wiedzę z zakresu wymienionych wyżej aspektów funkcjonowania współczesnej medycyny, możliwie najwcześniej na ścieżce rozwoju kariery.

³ „Breach Barometer Report: Year in Review” (Protenus, 2016).

⁴ Sean Murphy, „Is Cybersecurity Possible in Healthcare?”, *National Cybersecurity Institute Journal* 1, nr 3 (2015): 49

⁵ J. Jiang i G. Bai, „Evaluation of Causes of Protected Health Information Breaches.”, 2019, 179,265.

REKOMENDACJE DOMENA MEDYCyna

Główne kierunki koniecznych zmian

1 — Wprowadzenie problematyki cyberbezpieczeństwa w medycynie na podstawie studiów przypadków

Ze względu na wysokie zainteresowanie studentów poruszaną tematyką oraz fakt, że spotykają się z nią w praktyce zawodowej, wprowadzenie podstaw problematyki cyberbezpieczeństwa w medycynie mogłoby odbywać się na przykładzie studiów przypadków, opisujących rzeczywiste ataki, które wystąpiły na świecie w ostatnich latach, np. WannaCry. Spowoduje to uatrakcyjnienie procesu dydaktyki oraz umożliwi przystępne pokazanie problematyki i możliwych działań prewencyjnych, które należałoby w podobnych sytuacjach podjąć.

2 — Wprowadzenie praktyk podnoszących bezpieczeństwo danych pacjenta

Praca w sektorze ochrony zdrowia wiąże się z szerokim dostępem do danych wrażliwych. Z tego względu niezbędne jest, by już w pierwszych latach nauki studenci poznali tematykę ochrony danych w przyszłym miejscu pracy, np. zgodnie z krokami proponowanymi przez University of Illinois at Chicago czy HealthIT.

3 — Wprowadzenie praktyk podnoszących bezpieczeństwo danych własnych personelu

W czasie zajęć, bez względu na formę ich prowadzenia, poruszane powinny być tematy związane z rozpoznawaniem przez użytkowników sieci podstawowych cyberataków, takich jak phishing, scam, ataki typu ransomware czy malware. Należytem byłoby zapoznanie słuchaczy z narzędziami przydatnymi do tworzenia i bezpiecznego przechowywania hasel oraz podstaw odpowiedniego zabezpieczania kont osobistych.

4 — Zapoznanie studentów z przykładowymi programami wykorzystywanymi do prowadzenia historii pacjenta w szpitalach, przychodniach, zespołach ratownictwa medycznego typu P, S i HEMS

Mnogość programów wykorzystywanych przez placówki medyczne w Polsce uniemożliwia dokładne przygotowanie do pracy z konkretnymi programami, jednak podstawowe zapoznanie z programami wykorzystywanymi przez podmioty lecznicze danych uczelni medycznych pozwoli na bezpieczny kontakt z nimi już w trakcie studiów, wypracowanie prawidłowych nawyków związanych z ich obsługą, a następnie na prawidłowe ich wykorzystywanie.

Zespół typu P – podstawowy zespół, w karetce pracują co najmniej dwie osoby uprawnione do wykonywania medycznych czynności ratunkowych (np. ratownicy medyczni, bez lekarza)

Zespół typu S – specjalistyczny zespół, w karetce pracuje minimum trzyosobowa obsada wraz z lekarzem systemu

Zespół HEMS = LPR – Lotnicze Pogotowie Ratunkowe

5 — Wprowadzenie zajęć o tematyce cyberbezpieczeństwa do programu szkolenia wojskowego studentów kierunku wojskowo-lekarskiego nadzorowanego przez MON

Z uwagi na specyfikę pracy w placówkach wojskowej ochrony zdrowia, stopień narażenia na cyberataki może być w nich zdecydowanie wyższy, np. w warunki wojny hybrydowej. Dodatkowo instytucje przewidziane do reagowania są inne niż w przypadku publicznego sektora ochrony zdrowia – CSIRT MON, Żandarmeria Wojskowa, SKW. Wiąże się to z ograniczonym dostępem do odpowiednich narzędzi umożliwiających samodzielną naukę studentów czy pracowników tych podmiotów, co może utrudniać ich prawidłową reakcję w sytuacji cyberataku.

REKOMENDACJE DOMENA MEDYCyna

Opisane poniżej wyzwania wraz z propozycjami ich zaadresowania
oznaczone są piktogramami



Wyzwanie



Stan Pożądaný



Rekomendacje



Nauczanie w ramach zajęć Bioinformatyki niedostosowane do poziomu wiedzy studentów, przedstawianie przestarzałych praktyk w czasie zajęć.



Studenci określają poziom swojej wiedzy, a zajęcia mają na celu uzupełnienie braków. Wykładowcy przedstawiają zastosowanie nauczanych umiejętności w praktyce, co wzbudzi większe zainteresowanie studentów przedmiotem.



Rozpoczęcie zajęć od sprawdzenia poziomu umiejętności studentów, następnie wprowadzenie podziału zajęć według różnego poziomu zaawansowania.



Zbyt niski poziom umiejętności informatycznych wśród studentów kierunków medycznych, skutkujący w przyszłości brakiem zrozumienia elementów niezbędnych do zachowania bezpieczeństwa danych.



Kształcenie w ramach zajęć Bioinformatyki skupione na nauczaniu praktycznych umiejętności informatycznych, niezbędnych w praktyce leczniczej z powodu szybko postępującej cyfryzacji w medycynie.



Większy nacisk na treści informatyki stosowanej w medycynie w ramach zajęć przedklinicznych. Umożliwienie poszerzania wiedzy studentów z pogranicza medycyny i informatyki oraz najnowszych rozwiązań inżynierii biomedycznej.



Studenci nie otrzymują podstawowej wiedzy nt. zachowania bezpieczeństwa danych pacjentów oraz bezpiecznych zachowań w sieci, w tym zabezpieczania danych własnych na urządzeniach mobilnych.



W czasie pierwszych lat studiów w ramach zajęć przedklinicznych na kierunkach medycznych student powinien osiągnąć wiedzę nt. podstaw zachowania bezpieczeństwa danych wrażliwych otrzymanych od pacjenta. Niezbędna jest wiedza nt. praktyk mogących zwiększać bezpieczeństwo danych i zachowań mogących narażać je na dostęp osób nieupoważnionych.



Wszyscy studenci w ramach zajęć przedklinicznych powinni wziąć udział w szkoleniu z podstawowych zasad cyberbezpieczeństwa, które może mieć charakter zbliżony do szkoleń BHP niezbędnych do rozpoczęcia praktyk szpitalnych.



W ramach zajęć studenci nie mają możliwości zapoznania się z systemami informatycznymi niezbędnymi w pracy w warunkach szpitala, przychodni, zespołach ratownictwa medycznego typu P, S i HEMS.



Śluchacze powinni zapoznać się z systemami wykorzystywanymi w placówkach leczniczych uczelni wyższej. Stwarzałoby to możliwość wypracowania prawidłowych nawyków związanych z ich obsługą oraz ich prawidłowe wykorzystywanie w przyszłości.



Wprowadzenie w ramach zajęć przedklinicznych nauki obsługi programów informatycznych wykorzystywanych w systemie ochrony zdrowia.

REKOMENDACJE DOMENA MEDYCYN

-  *Studenci rozpoczynający zajęcia kliniczne nie są przygotowani w zakresie podstawowych zasad cyberbezpieczeństwa oraz RODO.*
 -  *Na kilka dni przed rozpoczęciem pierwszych zajęć klinicznych studenci, w ramach zajęć obowiązkowych, powinni uczestniczyć, w dniu szkolenia związanego z BHP, w szkoleniu nt. RODO, tajemnicy zawodowej oraz cyberbezpieczeństwa. Umożliwi to wyrównanie poziomu wiedzy na te tematy wśród studentów i przedstawienie jednolitych zasad panujących w placówkach leczniczo-szkoleniowych, promując jednocześnie prawidłowe zachowania.*
 -  *Wprowadzenie zajęć przygotowujących do przedmiotów klinicznych, obejmujących szkolenia z BHP, RODO, tajemnicy zawodowej i cyberbezpieczeństwa. Zajęcia te mogłyby mieć formę jednodniowych warsztatów lub obowiązkowych szkoleń online. Przykładem może być kurs Cybersecurity in Healthcare Hospitals & Care Centres stworzony przez Erasmus University Rotterdam na platformie Coursera.*
-
-  *W ramach zajęć fakultatywnych w temacie prowadzenia własnej działalności leczniczej studenci nie są informowani o aspekcie prawidłowego zabezpieczenia systemów przechowujących dane pacjentów i pracowników.*
 -  *Wprowadzenie do problematyki zajęć nt. utworzenia własnego podmiotu leczniczego zagadnień dotyczących cyberbezpieczeństwa, właściwego wyposażenia podmiotu leczniczego w sprzęt komputerowy oraz przedstawienia prawidłowych zachowań podnoszących bezpieczeństwo danych wykorzystywanych przez podmiot. Studenci po ukończeniu studiów aktywnie wykorzystują uzyskaną wiedzę w celu ochrony danych wrażliwych.*
 -  *Implementacja w ramach zajęć dotyczących prowadzenia własnej praktyki leczniczej tematyki cyberbezpieczeństwa. Promocja odpowiednich zachowań zwiększających bezpieczeństwo systemów wykorzystujących dane pacjentów.*
-
-  *Ze względu na ograniczoną liczbę godzin na zajęciach nie istnieje możliwość dokładnego omówienia zagadnień, powiązanych z cyberbezpieczeństwem.*
 -  *Studenci mają dostęp do szkoleń online przygotowanych przez uczelnię lub przez nią wykupionych, poruszających problematykę cyberbezpieczeństwa w medycynie, mogą uczestniczyć w zajęciach fakultatywnych oraz w spotkaniach organizowanych przez organizacje studenckie i koła naukowe.*
 -  *Władze uczelni aktywizują i wspierają organizację wydarzeń o tematyce cyberbezpieczeństwa. W sytuacji uczelni wyższych oferujących jedynie kierunki medyczne wartościowe może być nawiązanie współpracy z innymi uczelniami wyższymi, które w swej ofercie posiadają kierunki informatyczne, a w ramach tej współpracy wymiana doświadczeń – jedna z uczelni przygotowuje warsztaty z cyberbezpieczeństwa, druga natomiast prowadzi warsztaty dla studentów i studentek z zakresu profilaktyki najczęstszych chorób czy pierwszej pomocy.*

WSPÓŁAUTORZY RAPORTU „DOMENA MEDYCYN

Mateusz Guziak — Wydział Lekarski, Gdański Uniwersytet Medyczny

Miłosz Korczak — Collegium Medicum, Uniwersytet Zielonogórski

Nicholas Karolak — Collegium Medicum, Uniwersytet Mikołaja Kopernika w Toruniu

Julia Makuch — Wydział Lekarski, Uniwersytet Medyczny we Wrocławiu



dr n.med. **Dagmara Gawęł-Dąbrowska**

O potrzebie wykorzystania systemów informatycznych w sektorze ochrony zdrowia w Polsce mówi się szeroko od ponad 20 lat. W 2000 roku wydawało się, że informatyzacja sektora będzie przebiegała dynamicznie - przy Ministerstwie Zdrowia powstało Centrum Systemów Informatycznych (CSIOZ), którego zadaniem było i jest upowszechnianie wykorzystania narzędzi informatycznych w placówkach ochrony zdrowia. Od początku istnienia CSIOZ toczyła się dyskusja o potrzebie zbudowania ogólnodostępnego dla pacjentów systemu informatycznego, którego celem miała być komunikacja między pacjentem – personelem medycznym i płatnikiem – ubezpieczycielem. Od początku w dyskusji zwracano szczególną uwagę na bezpieczeństwo przechowywania i przesyłania danych, które w tym wypadku mają szczególnie wrażliwy charakter.

Niestety pomimo szerokiego entuzjazmu tak się nie stało. Przeszkodą był brak rozwiązań legislacyjnych, ale również, jak słusznie zauważają autorzy przedstawionego raportu, czynnik ludzki. Ustawa o systemie informacji w ochronie zdrowia z 2011 r. pozwoliła na rozwój baz danych oraz systemów informatycznych różnych instytucji gromadzących dane o pracownikach świadczących usługi lecznicze, a także o samych usługach – zrealizowanych, realizowanych i planowanych. Bezpieczeństwo danych związanych ze świadczeniem usług medycznych powierzono Ministerstwu Zdrowia, które ma odpowiadać za prawidłowe funkcjonowanie platformy internetowej łączącej w przyszłości wszystkie podmioty pracujące na rzecz świadczenia usług leczniczych. Takie rozwiązanie zwiększyło bezpieczeństwo przepływu wrażliwych danych medycznych, ale nie wyeliminowało zagrożeń związanych z cyberbezpieczeństwem.

Autorzy raportu zwracają uwagę na konieczność uwrażliwienia na problem przyszłych użytkowników systemu, w tym studentów kierunków medycznych. Kluczem do sukcesu ma być właściwa ich edukacja. Wydaje się istotnym, by edukacja była przeprowadzona przez informatyków, w formie praktycznej – warsztatowej. Zgadzam się z wyrażonymi w raporcie potrzebami, iż kadry medyczne winny zostać zapoznane z podstawowymi zasadami cyberbezpieczeństwa i bezpiecznej obsługi infrastruktury informatycznej podmiotów świadczących usługi z zakresu ochrony zdrowia.

W projekcie podjęto bardzo istotny problem braku zagadnień cyberbezpieczeństwa w edukacji studentów kierunków medycznych. Co ważne w analizie podjęto próbę przedstawienia przykładów rozwiązań, które mogłyby pomóc w tym procesie. Jest to cenna inicjatywa.

Wskazane byłoby zapoznanie słuchaczy z narzędziami przydatnymi do tworzenia i bezpiecznego przechowywania haseł oraz podstaw odpowiedniego zabezpieczania kont osobistych, a także zapoznanie z przykładowymi programami stosowanymi w obsłudze pacjenta – przykładowo P, S, HEMS po to by zrozumieć istotę ich funkcjonowania i nabrać pewnych nawyków.

Interoperacyjność w informatyzacji zdrowia oznaczająca zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów m. in. do współdzielenia informacji jest naszą przyszłością. Użytkownicy tych systemów, w tym przyszli lekarze, muszą posiadać podstawową wiedzę techniczną w zakresie cyberbezpieczeństwa.

Problem podjęty w raporcie jest tym istotniejszy, że zmieniająca się obecnie rzeczywistość pandemiczna wymusiła szybkie wprowadzenie rozwiązań teleinformatycznych w ochronie zdrowia i zmiany, do których przygotowujemy się mogą nastąpić znacznie wcześniej.

Wiedza na temat cyberbezpieczeństwa mogłaby być przekazywana nie tylko na zajęciach z prawa medycznego (jak wskazano w raporcie) ale również zdrowia publicznego.

Dagmara Gawęł-Dąbrowska

Starszy wykładowca w Katedrze i Zakładzie Medycyny Społecznej Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu, specjalista chorób wewnętrznych, reumatologii i zdrowia publicznego



**2 PRAWO
I REGULACJE**



Weronika Bańska

Przewodnicząca Europejskiego Stowarzyszenia Studentów Prawa ELSA

REKOMENDACJE DOMENA PRAWO

Materiał źródłowy zgromadzony w ramach analizy programów nauczania, dokonanej w kooperacji studentów z jedenastu wydziałów prawa. Reprezentowane uczelnie: Uniwersytet w Białymstoku, Uniwersytet Gdański, Uniwersytet Kardynała Stanisława Wyszyńskiego w Warszawie, Uniwersytet Łódzki, Uniwersytet Marii Curie-Skłodowskiej w Lublinie, Uniwersytet Mikołaja Kopernika w Toruniu, Uniwersytet Rzeszowski, Uniwersytet Warszawski, Uniwersytet Warmińsko-Mazurski, Uniwersytet Wrocławski.

Aktualny stan nauczania na temat cyberbezpieczeństwa

Analizując programy nauczania na studiach prawniczych, pod kątem ekspozycji tematyki dotyczącej cyberbezpieczeństwa, za celowe uznaliśmy również opisanie obecnego podejścia na wydziałach prawa do całokształtu dydaktyki w temacie nowych technologii.

Mimo istotnej, dynamicznie rosnącej, roli technologii informacyjnych i ich oddziaływania na praktycznie każdą sferę życia, dydaktyka w tym obszarze odgrywa marginalną rolę na omawianym kierunku studiów. Na większości ze wskazanych wcześniej wydziałów możliwość rozwijania przez studentów umiejętności informatycznych kończy się na prowadzonym, w niewielkim wymiarze godzinowym, przedmiocie Informatyka Prawnicza (różnie nazywanym), nie zawsze mającym charakter obligatoryjny – co oznacza, że studia prawnicze można ukończyć bez jakiegokolwiek poszerzenia swoich umiejętności w wykorzystywaniu technologii informacyjnych.

Niektóre uczelnie umożliwiają studentom udział w fakultatywnych zajęciach związanych z nowymi technologiami i prawem nowych technologii (np. dotyczących tzw. sztucznej inteligencji), ale jeśli taka gałąź kształcenia występuje w danym ośrodku, jest ona zdecydowanie jedną z najmniej rozbudowanych i obejmuje, poza nielicznymi wyjątkami, jeden lub dwa przedmioty. Oznacza to, że studenci, chcący specjalizować się w szerokim spektrum tematów korelacji prawa i nowych technologii, nie mają możliwości rozwijania potrzebnych im umiejętności na uczelni.

Kolejnym aspektem wartym uwagi jest podejście do przedmiotów formalnych i informatycznych. Tylko pozornym – w tym kontekście – może wydać się brak związku cyberbezpieczeństwa i prawa z naukami formalnymi. Dla lepszego zrozumienia struktury świata informatycznego, potrzebna jest pewna kultura formalna (matematyczna) i wiedza techniczna umożliwiająca zrozumienie mechanizmów działania określonych technologii.

Na większości uczelni wciąż zauważalne jest podejście, iż prawo może istnieć w próżni, a nauka tekstów ustaw jest w stanie zastąpić umiejętności precyzyjnego, prawidłowego rozumowania, posługiwania się konstrukcjami abstrakcyjnymi i zrozumienia rzeczywistości cyfrowej. Wniosek ten nasuwa się po analizie sylabusów programowych. Na studiach prawniczych de facto występuje jeden tylko, obowiązkowy dla wszystkich studentów, przedmiot mogący być nazwany formalnym – Logika dla Prawników (czy też Logika Prawnicza), jednosemestralny, w wymiarze nie większym niż 75 godzin.

REKOMENDACJE DOMENA PRAWO

Elementy matematyki mogą pojawiać się także na, obecnych w niektórych ośrodkach akademickich, Podstawach Ekonomii (Ekonomii dla Prawników). Mimo istnienia wspomnianych przedmiotów, nie znajdujemy na uczelniach silniejszego akcentu ukierunkowanego na kształtowanie ww. kultury formalnej i umiejętności abstrakcyjnego myślenia, których pewien poziom jest niezwykle przydatny (lub nawet niezbędny) w rozumieniu technicznych niuansów związanych z cyberbezpieczeństwem.

Po scharakteryzowaniu powyższych, systemowych problemów, przechodzimy do kwestii nauczania tematyki cyberbezpieczeństwa. W ramach analizowanych programów, w toku studiów nie występuje obligatoryjny przedmiot bezpośrednio związany z domeną. Z reguły zupełnie podstawowym problemom cyberbezpieczeństwa – np. oprogramowaniu antywirusowemu, bezpiecznemu przeglądaniu Internetu itp. – poświęcone jest kilka godzin w ramach przedmiotu Informatyka Prawnicza – i jest to jedyny kontakt, który studenci mają z cyberbezpieczeństwem, o ile oczywiście Informatyka Prawnicza jest na danej uczelni przedmiotem obowiązkowym.

Na niektórych uczelniach obserwuje się szerszy wybór przedmiotów fakultatywnych, wśród których funkcjonują te związane np. z cyberprzestępczością czy ochroną danych osobowych w Internecie. Typowy przedmiot „Cyberbezpieczeństwo” pojawił się jednak tylko na jednej z poddanych analizie uczelni na Uniwersytecie Kardynała Stanisława Wyszyńskiego w Warszawie, pozostałe nie oferowały kursów dotyczącego tego tematu.

Problematyką, która powinna być poruszana w toku studiów jest przekazywanie informacji o tzw. przestępstwach komputerowych, w szczególności o sposobach prewencji, wykrywania, zwalczania i dogmatyki. Z naszej analizy wynika, iż na studiach prawniczych temat ten nie funkcjonuje w ramach kursów obowiązkowych, lub też adresowany jest pobieżnie – mimo, że w zmieniającej się rzeczywistości, uwarunkowanej postępującym procesem cyfryzacji, udział tego typu przestępstw w strukturze przestępczości wykazuje dynamiczny trend wzrostowy. Gdy studenci mają już okazję spotkać się z tematem, wykładane treści dotyczą raczej zagadnień teoretycznych i dogmatycznych, z pominięciem praktycznych aspektów prewencji i zwalczania przestępczości w sieci.

Poczyniona analiza wskazuje na rozległe pole do zagospodarowania w kwestii edukacji o cyberbezpieczeństwie na studiach prawniczych. Temat poruszany jest pobieżnie, o ile jest poruszany, brak jest obligatoryjnych przedmiotów dedykowanych problematyce. Co nie mniej istotne, konstrukcja systemu kształcenia prawników w Polsce zakłada marginalną rolę przedmiotów formalnych i informatycznych. Sam ten fakt bardzo utrudnia rzetelną edukację o cyberbezpieczeństwie.

Główne kierunki koniecznych zmian

1 — Uwzględnienie znaczącej roli przedmiotów o charakterze ścisłym na studiach prawniczych

W toku studiów prawniczych prowadzonych jest niewiele zajęć z zakresu matematyki, logiki i ekonomii. To kwestia warta zaadresowania, ze względu na kompetencje zawodowe przyszłych prawników. Przedmioty te uczą logicznego, precyzyjnego myślenia, które odgrywa znaczenie w każdej pracy intelektualnej, w szczególności tam, gdzie występują powiązania z dziedzinami ścisłymi, a te niewątpliwie są obecne w nauce o cyberbezpieczeństwie. Przedmioty te kształtują umiejętności wnioskowania, adekwatnej formalizacji problemów prawniczych i społecznych, co bezsprzecznie niezbędne jest w wykonywaniu zawodu prawnika na wysokim poziomie.

Nauka rozważanych przedmiotów przygotowuje do zdobycia wiedzy z zakresu nowych technologii, dając możliwość lepszego pojmowania zasad i mechanizmów rządzących domeną IT w korelacji z domeną prawa. To z kolei pozwala na dokonywanie prawidłowej analizy z informatyzowanego świata. Umiejętności te stają się przydatne w sposób bardziej bezpośredni, gdy mowa o kwestiach cyberbezpieczeństwa, które traktować należy w ujęciu interdyscyplinarnym.

Znaczące braki w myśleniu formalnym i te związane z elementarną wiedzą matematyczną, mogą prowadzić do faktycznej niemożności, nawet ogólnego, zrozumienia istotnych aspektów związanych z domeną cyberbezpieczeństwa, np.: szyfrowanie danych czy zagadnienia algorytmów uczenia maszynowego. Z tego względu rekomendowanym jest odejście od myślenia o prawie jako kierunku zupełnie niezwiązanym z matematyką i zwiększenie udziału przedmiotów ścisłych w toku studiów. To perspektywa założenia długookresowego celu – dostarczania interdyscyplinarnej wiedzy, odpowiadającej wymaganiom współczesnego świata.

2 — Silna ekspozycja przedmiotów informatycznych na studiach prawniczych

Pożądanym jest, by prawnicy, niezależnie od specjalizacji, mogli biegle posługiwać się różnorodnymi technologiami informacyjnymi i zdawali sobie sprawę z możliwości ich wykorzystania w zawodzie. Przynajmniej ogólna znajomość i zrozumienie tych technologii są warunkiem koniecznym dla poruszania się w materii cyberbezpieczeństwa i posiadania umiejętności zastosowania poznanych zasad zabezpieczania się przed cyberprzestępcstwami.

Istotnym kierunkiem zmian, na rzecz edukacji dla cyberbezpieczeństwa, jest zwiększenie roli zajęć informatycznych na studiach prawniczych. Ich wdrożenie pozwoli na kształcenie osób o szerszym spektrum percepcji, zdolnych do optymalizacji swojej praktyki prawniczej, ale przede wszystkim – świadomych możliwości i zagrożeń tworzonych przez informatyzację środowiska pracy.

3 — Cyberbezpieczeństwo w ramach przedmiotów obligatoryjnych

Scharakteryzowany wcześniej system edukacji blokuje dziś efektywne nauczanie, istotnych dla prawników, zagadnień dotyczących cyberbezpieczeństwa. Zajęcia związane z Informatyką poruszają głównie najprostsze aspekty tj. korzystanie z programów tekstowych oraz programów przeznaczonych do tworzenia prezentacji. Często prezentowana jest wiedza już zdobyta przez słuchaczy, przyswojona na wcześniejszych etapach edukacji. Zbędnym jest powielanie zajęć z tego zakresu, jeśli nie rozszerzają one uprzednio zdobytych kompetencji.

Mając na uwadze powyższe warto rozważyć rekonstrukcję treści obligatoryjnych, przedmiotów w sposób, by poszerzały horyzonty studentów, kładąc nacisk na praktyczną wiedzę o cyberbezpieczeństwie w zawodzie prawnika. Zasadnym wydaje się wprowadzenie przedmiotów poświęconych stricte cyberbezpieczeństwu. Uzupełniłyby one obecny system nauczania, zwiększając jego efektywność.

Sugerowane do implementacji treści w ramach nowo powstałych przedmiotów obejmowałyby m.in.: wybrane aspekty cyberbezpieczeństwa (w tym patologie i zagrożenia w cyberprzestrzeni), problematykę wykorzystania technologii w postępowaniu sądowym, praktyczne ujęcie cyberbezpieczeństwa w zawodzie prawniczym, prawo karne komputerowe, ochronę cyberprzestrzeni i podstawy kryptologii. Każdy z przedmiotów powinien trwać jeden semestr. Okolicznością wymagającą podkreślenia jest fakt, że wykładowcy winni prezentować, oprócz teoretycznego, praktyczne ujęcie poruszanego zagadnienia.

Cyberbezpieczeństwo jest obszarem wielowymiarowym, z którym wiążą się nie tylko kwestie dotyczące funkcjonowania w sieci, wykrywania i zwalczania przestępstw w cyberprzestrzeni, ale przede wszystkim przeciwdziałanie ich powstawaniu na wielu płaszczyznach. Działalność operacyjna dzisiejszych instytucji: uczelni, służby zdrowia, sądów czy firm prawniczych w większości oparta jest na cyfrowych nośnikach danych. Kluczowym w procesie gromadzenia i dystrybucji jest ich zabezpieczenie przed niepożądaną ingerencją osób trzecich, w tym bezpieczeństwo wykorzystywanego sprzętu. Tego typu praktyczne ujęcie problematyki wyrabia u studentów nawyk przewencyjnego myślenia i działania.

Interdyscyplinarne ujęcie tematyki cyberbezpieczeństwa jest wyzwaniem dla procesu edukacji prawniczej. Generuje szczególny wymóg dla wykładowców – przekazywana wiedza w jednoznaczny sposób powinna wskazywać na korelacje i współpracę różnych dyscyplin naukowych, adresujących cyberwyzwania.

4 — Możliwość specjalizacji w cyberbezpieczeństwie przez zwiększenie puli przedmiotów fakultatywnych

Bez względu na obraną przez studentów specjalizację, bezdyskusyjną wydaje się potrzeba implementacji w treściach programowych przynajmniej podstawowych aspektów dotyczących cyberbezpieczeństwa.

REKOMENDACJE DOMENA PRAWO

Znaczącą wartość dla studentów, upatrujących swój rozwój w dziedzinach nowych technologii i bezpośrednio w cyberbezpieczeństwie, byłoby umożliwienie im wyboru takiej ścieżki rozwoju. Obecnie, na większości wydziałów, jest to niemożliwe ze względu na niedostatek przedmiotów obieralnych poświęconych tej tematyce. Stworzenie szerszych możliwości nauczania w tych obszarach warunkuje kształcenie przyszłych specjalistów w zakresie cyberbezpieczeństwa i zwiększenie świadomości na tematy obecnych, globalnych wyzwań.

5 — Edukacja na rzecz dalszego ujednolicania zagadnień dotyczących cyberbezpieczeństwa w ramach europejskiego systemu prawnego

Rozbieżność w regulacjach między państwami wspólnoty europejskiej stanowi wyzwanie w walce z cyberzagrożeniami i w bezpośredni sposób utrudnia stworzenie jednolitej strategii adresującej ten temat. Stosownym byłoby rozszerzanie aktów prawa unijnego oraz dostosowanie norm wewnętrznych do obecnych możliwości technologicznych. Kwestią wymagającą uwagi jest również poszerzanie i promowanie współpracy międzynarodowej między organami i organizacjami ścigającymi przestępców, jak Interpol lub Europol, w tym poszerzanie zakresu ich działalności co do przestępczości w cyberprzestrzeni, tak by jej zwalczanie stało się jednym z kluczowych, adresowanych obszarów. Istnieje wysokie prawdopodobieństwo, że działalność taka umożliwiłaby, w szczególności, sprawniejsze wykrywanie nowych trendów i szlaków komunikacyjnych w przestępczości oraz szybszą, i szerszą wymianę informacji.

By wspomniane kroki były możliwe, potrzebne jest odpowiednio wczesne kształcenie i uwrażliwianie słuchaczy na rolę prawa unijnego w tworzeniu zintegrowanego ekosystemu cyberbezpieczeństwa.

Właściwym kierunkiem zmian jest przemodelowanie przedmiotów w programach studiów, by w ramach już istniejących, dotyczących prawa unijnego, pojawiał się temat wspólnotowych uregulowań związanych z cyberbezpieczeństwem. Warto, by w edukacji prawniczej poruszano aspekt wartości płynącej ze spójności międzynarodowych uregulowań dotyczących bezpieczeństwa w cyberprzestrzeni.

6 — Prawo Karne z uwzględnieniem współczesnej struktury przestępczości

Obecna struktura przestępczości różni się diametralnie względem tej, która dominowała, gdy uchwalano funkcjonujący Kodeks Karny – w 1997 r. Znaczący procent przestępców działa w sieci. Fakt ten powinien zostać uwzględniony w nauce Prawa Karnego. Nielegalne próby przejęcia kontroli nad kontem na portalu społecznościowym czy internetowa kradzież tożsamości stanowią już pospolite czyny zabronione i warto uwzględnić je w ramach dydaktyki przedmiotów karnistycznych. Przysłuży się to też do pozyskania, istotnej dla studentów, wiedzy o prawnokarnych regulacjach powiązanych z cyberbezpieczeństwem i typach zabronionych, które swoim zakresem obejmują czyny popełniane z wykorzystaniem Internetu. Inną korzyścią związaną ze zwiększenia udziału wiedzy o przestępczości w sieci w programach nauczania będzie aktualne odnoszenie się do rzeczywistych problemów współczesnego świata.

REKOMENDACJE DOMENA PRAWO

Opisane poniżej wyzwania wraz z propozycjami ich zaadresowania
oznaczone są piktogramami



Wyzwanie



Stan Pożądany



Rekomendacje



Brak dostosowania poziomu nauczania informatycznego/technologicznego do indywidualnej wiedzy nabytej przez studentów we wcześniejszym toku nauczania.



Przekazywanie wiedzy dostosowanej do poziomu merytorycznego słuchaczy, wywrze korzystny wpływ na zainteresowanie studentów danym przedmiotem, w tym wykrywanie i przeciwdziałanie przestępczości w sieci.



Wprowadzenie na zajęciach informatycznych grup zajęciowych charakteryzujących się różnym poziomem zaawansowania, których dobór uzależniony będzie od preferencji studenta oraz jego aktualnego poziomu wiedzy.



Zbyt mała lub nawet znikoma ilość materiału z zakresu logiki, matematyki oraz ekonomii na kierunkach prawniczych, zbyt duża odmiennność w programach studiów na różnych uczelniach.



Szeroki zakres nauczania w zakresie logiki, matematyki oraz ekonomii na studiach prawniczych, ujednolicenie systemu nauczania w zakresie obecności tych przedmiotów w programie studiów.



Poszerzenie godzinowego oraz merytorycznego zakresu przedmiotów z zakresu logiki, matematyki oraz ekonomii. Uznanie wartości nauczania tych dziedzin w ramach studiów prawniczych.



Zbyt niski poziom umiejętności informatycznych studentów prawa skutkujący przyszłymi brakami w zrozumieniu mechanizmów cyberataków i niemożnością właściwego zabezpieczenia się przed nimi.



Kształcenie w zakresie praktycznych umiejętności informatycznych, potrzebnych w praktyce prawniczej do płynnego korzystania z zdobyczy technologii.



Zwiększenie nacisku na treści informatyki stosowanej w prawie, umożliwienie studentom poszerzania wiedzy z pogranicza prawa i informatyki w ramach więcej niż jednego przedmiotu w trakcie studiów.



Brak obligatoryjnych przedmiotów dotyczących bezpośrednio cyberbezpieczeństwa, w tym przeciwdziałania, wykrywania i zwalczania przestępczości komputerowej, tematyka omawiania jest pobieżnie.



Kwestie dotyczące cyberbezpieczeństwa szeroko omawiane na przedmiotach obligatoryjnych.



Wprowadzenie obligatoryjnych zajęć poświęconych stricte cyberbezpieczeństwu, w tym: zagrożeniom w cyberprzestrzeni i ich prewencji, problematyce wykorzystania technologii w postępowaniu sądowym, praktycznemu ujęciu cyberbezpieczeństwa w zawodzie prawniczym i podstaw kryptologii.

REKOMENDACJE DOMENA PRAWO



Bardzo mała liczba przedmiotów fakultatywnych, poruszających kwestie cyberbezpieczeństwa.



Liczba przedmiotów związanych z cyberbezpieczeństwem dostosowana do wymagań kształtowych przez współczesne realia, możliwość specjalizowania się w cyberbezpieczeństwie w ramach studiów prawniczych.



Uwzględnienie wśród zajęć fakultatywnych przedmiotów poruszających różne aspekty cyberbezpieczeństwa. Umożliwienie studentom zdobywania wiedzy specjalistycznej z pogranicza prawa i nowych technologii.



Brak praktycznego ujęcia tematu bezpieczeństwa w cyberprzestrzeni, przeteoretyzowanie przekazywanych treści.



Ukazanie zjawiska przeciwdziałania przestępczości w sieci w sposób praktyczny.



Prowadzenie zajęć przez specjalistów-praktyków.



Brak wystarczającej liczby specjalistów z dziedziny cyberbezpieczeństwa w kadrze naukowej wydziałów prawa.



Prowadzenie zajęć na wydziałach prawa także przez specjalistów z zakresu cyberbezpieczeństwa.



Zwrócenie uwagi na obecność przedmiotów stricte dotyczących cyberbezpieczeństwa w toku studiów na kierunku prawo. Organizowanie szkoleń oraz kursów, zwiększenie liczby konkursów i projektów dotyczących poszczególnych kwestii.



Ogólny brak specjalistów z dziedziny cyberbezpieczeństwa.



Kształcenie wystarczającej liczby specjalistów dla biznesu i sektora publicznego.



Zwrócenie uwagi studentów prawa na obecność przedmiotów stricte dotyczących cyberbezpieczeństwa oraz możliwości rozwoju w ramach przedmiotów fakultatywnych. Organizowanie szkoleń oraz kursów, zwiększenie liczby konkursów i projektów dotyczących zagadnień cyberbezpieczeństwa.

WSPÓŁAUTORZY RAPORTU „DOMENA PRAWO”

Natalia Boguszewska — Wydział Prawa i Administracji, Uniwersytet Łódzki
Zuzanna Choińska — Wydział Prawa i Administracji, Uniwersytet Warszawski
Klaudia Jędrzejowska — Wydział Prawa i Administracji, Uniwersytet Łódzki
Jan Lewit — Wydział Prawa i Administracji, Uniwersytet Kard. S. Wyszyńskiego w Warszawie
Janusz Linowski — Wydział Prawa i Administracji, Uniwersytet M. Skłodowskiej-Curie w Lublinie
Łukasz Lisowski — Wydział Prawa i Administracji, Uniwersytet Łódzki
Marcelina Łukowicz — Wydział Prawa i Administracji, Uniwersytet Łódzki
Mikołaj Niedźwiadek — Wydział Prawa i Administracji, Uniwersytet Łódzki
Piotr Orzechowski — Wydział Prawa i Administracji, Uniwersytet Kard. S. Wyszyńskiego w Warszawie
Zuzanna Piątek — Wydział Prawa i Administracji, Uniwersytet Łódzki
Andrzej Porębski — Wydział Prawa i Administracji, Uniwersytet Jagielloński w Krakowie
Kacper Stoś — Wydział Prawa i Administracji, Uniwersytet Łódzki
Filip Strzępek — Wydział Prawa i Administracji, Uniwersytet Łódzki
Agata Zalewska — Wydział Prawa i Administracji, Uniwersytet Warmińsko-Mazurski w Olsztynie



” dr Kamil Mamak

Truizmem jest twierdzenie, że technologie odgrywają bardzo ważną rolę w ludzkim życiu. Wydaje się, że na poziomie ogółu nie trzeba nikogo do tego przekonywać, bardziej kłopotliwe jest jednak przełożenie tej obserwacji na konkrety. Prezentowany raport to próba pokazania jak zyskująca na znaczeniu technologia wpływa na kształcenie przyszłych prawników. Z raportu wyłania się obraz studiów prawniczych, które w niewystarczającym zakresie uwzględniają jej społeczną rolę, szczególnie, w zakresie cyberbezpieczeństwa, które stanowiło główny punkt odniesienia studentów zajmujących się tymi kwestiami.

Problemy cyberbezpieczeństwa są nie tylko ważne z punktu widzenia klientów późniejszych absolwentów studiów prawniczych, ale także z perspektywy ich samych. Zarówno kancelarie prawnicze, jak i sędziowie czy prokuratorzy powinni być przygotowani na występujące z coraz większym natężeniem zagrożenia.

Przygotowany raport wykazuje się dojrzałością w podchodzeniu do problemu. Świadczy o tym przede wszystkim fakt, że autorzy zwracają szczególną uwagę na potrzebę wyposażenia studentów prawa w umiejętności samodzielnego zrozumienia zjawisk. Niektóre uczelnie na świecie wychodzą naprzeciw tym oczekiwaniom oferując w programie studiów prawniczych naukę kodowania, w raporcie wskazuje się zapotrzebowanie m.in. na naukę logiki czy matematyki.

Autorzy projektu zwracają też uwagę na niewystarczającą ilość specjalistów od technologii i cyberbezpieczeństwa w kadrze prawniczych wydziałów. Wydaje się, że obecność takich osób pozwoliłoby w szybszy sposób reagować na zmieniające się zagrożenia i dostosowywać nauczanie do aktualnego obrazu rzeczywistości.

Zwraca się też uwagę na niewystarczające uwzględnienie cyberprzestępczości w kursach skupionych na opisie popełnianych przestępstw. Obraz przestępczości się zmienia i jeżeli coraz więcej przestępstw popełnianych jest z wykorzystaniem technologii, to powinno to być uwzględnione w większym stopniu w tych przedmiotach, które się nimi zajmują.

Wydaje się, że osoby odpowiedzialne za przygotowanie programów studiów prawniczych powinny ze szczególną uwagą przyjrzeć się temu raportowi, gdyż zawiera wiele cennych informacji o tym w jakim kierunku można dokonywać zmian.

Kamil Mamak

Doktor prawa i filozofii. Asystent w Katedrze Prawa Karnego Uniwersytetu Jagiellońskiego. Członek zarządu w Krakowskim Instytucie Prawa Karnego. Naukowo zajmuje się wpływem nowych technologii na człowieka i prawo karne.



Tomasz Kowalewski, Karol Spychała

Akademia Wojsk Lądowych im. Gen. T. Kościuszki we Wrocławiu

CYBERBEZPIECZEŃSTWO W EDUKACJI PODCHORAŻYCH



Specyfika funkcjonowania uczelni wojskowych pozwala, w wąskim zakresie, na publiczną prezentację elementów związanych z procesem kształcenia studentów. Rekomendacje środowiska studenckiego, opinie dotyczące implementacji w programach nauczania tematyki związanej z cyberbezpieczeństwem, w tym przypadku nie mogą zostać przedstawione szerokiej opinii publicznej. Poniżej zaprezentowano ogólną konkluzję w temacie edukacji o ekosystemie cyberbezpieczeństwa w ujęciu kształcenia podchorążych, wynikającą z ich udziału w turnieju CyberSecurity Challenge PL2020.

W tegorocznej edycji uczestniczyli podchorążowie z Akademii Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni, Wydział Mechaniczno-Elektryczny i Akademii Wojsk Lądowych im. Tadeusza Kościuszki we Wrocławiu, Wydziały: Nauk o Bezpieczeństwie, Inżynierii Bezpieczeństwa i Zarządzania.

Zaaranżowana interakcja studentów uczelni wojskowych i cywilnych, w ramach kooperacji multidyscyplinarnych zespołów wojewódzkich, uznana została przez podchorążych za jeden z najważniejszych elementów edukacyjnych tej symulacji. Ćwiczenie pozwoliło im na dogłębne poznanie złożonego charakteru kryzysu jakim jest cyberatak. Jego wymiaru strategicznego, regulacyjnego, organizacyjnego i komunikacyjnego.

Ekspozycja, w projekcie, wątku wieloaspektowości oraz transgraniczności cyberzagrożeń wzmacnia u studentów uczelni wojskowych świadomość sytuacyjną. Równolegle pozyskują oni kompetencje niezbędne im w kontekście uznania cyberprzestrzeni jako domeny działań militarnych.

Nabyte w turnieju doświadczenie i jego kontynuacja w ramach działań wojewódzkich Cyber Labów poszerzają zakres wiedzy o funkcjonowaniu ekosystemu cyberbezpieczeństwa, kształtując nowe kompetencje u przyszłych żołnierzy zawodowych.

W tym miejscu dziękujemy za okazane projektowi zainteresowanie

gen. bryg. dr hab. inż. Dariuszowi Skorupce, prof. AWL

Rektorowi – Komendantowi Akademii Wojsk Lądowych im. T. Kościuszki

dr hab. inż. Kazimierzowi Worwie

Prorektorowi ds. Kształcenia na Wojskowej Akademii Technicznej

kmdr por. dr inż. Przemysławowi Rodwaldowi

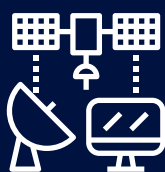
Kierownikowi Zakładu Systemów Komputerowych w Katedrze Informatyki Akademii Marynarki Wojennej im. Bohaterów Westerplatte



MODUŁY TEMATYCZNE



PRAWO



TECHNOLOGIE
INFORMACYJNE



BIZNES



ZDROWIE



OBRONNOŚĆ



PRZYSZŁOŚĆ

Udział w projekcie stwarza studentom możliwość aktywnej, eksperckiej dyskusji z przedstawicielami uczelni i z zewnętrznymi interesariuszami, w temacie kształtowania polityki programowej, uwzględniającej proces proaktywnego zarządzania transformacją cyfrową.

Rekomendacje płynące z raportu stanowią obecnie przedmiot rozmów z samorządami studenckimi. Prowadzone są w ramach kampanii uświadamiającej wagę procesu transformacji cyfrowej we wzmacnianiu konkurencyjności programów nauczania.

Art. 28§ 2 Ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U 2018 poz. 1066) w brzmieniu „ustalenie programu studiów wymaga zasięgnięcia opinii samorządu studenckiego”, oznacza że każdy program studiów w Polsce jest współtworzony przez studentów, reprezentowanych poprzez ich przedstawicieli. W praktyce, władze uczelni zwracają się do samorządów z prośbą o zaopiniowanie programów studiów. Opinie wydawane są na podstawie prac i konsultacji samorządów ze środowiskiem studenckim.

Ogólnopolska promocja wniosków płynących z raportu, odbywa się regionalnie poprzez sieć wojewódzkich Cyber Labów, w formule aranżowanych przez nie debat. Aktywności animują lokalni liderzy. To przestrzeń do tworzenia nowych partnerstw, wzmacniania współpracy między różnymi środowiskami i platforma dla innowacji w edukacji o cyberbezpieczeństwie.

EKSPERCI O WADZE INTERDYSCYPLINARNEJ EDUKACJI



REGIONAL
CYBER LABS

#RegionalCyberLabsPL20/21
@CyberPoland



Kluczowy element w procesie edukacji, obok edukacji formalnej, stanowi tzw. edukacja nieformalna w ramach grup rówieśniczych, realizowana głównie przy wsparciu organizacji pozarządowych. Optymalnym dla tworzenia efektu inteligentnych specjalizacji (sprzyjających włączeniu społecznemu) jest łączenie tych dwóch skorelowanych ze sobą wymiarów. Impulsem do uruchomienia tej kooperacji w obszarze edukacji o cyberbezpieczeństwie jest interdyscyplinarny turniej wiedzy o cyberwyzwaniach CyberSecurity Challenge PL2020. To inwestycja w cyberbezpieczeństwo oparta na solidnym know-how, wspierającym konkurencyjną gospodarkę cyfrową i interes publiczny.



THE BRIDGE
FOUNDATION



REGIONAL
CYBER LABS

EKSPERCI O WADZE INTERDYSCYPLINARNEJ EDUKACJI



PIOTR ALBRECHT

Dyrektor ds. Bezpieczeństwa
Giełda Papierów Wartościowych w Warszawie

Złożoność warunków funkcjonowania współczesnej gospodarki powoduje że cyberbezpieczeństwo musi łączyć aspekty technologiczne, prawne i organizacyjne, obejmując zarządzanie informacją, danymi, ryzykiem i zgodnością. Interdyscyplinarność cyberbezpieczeństwa siłą rzeczy przenikać musi do edukacji. Przy czym podkreślić należy, że ze względu na złożoność środowiska edukacja musi być procesem ciągłym. Zatem, jedynie ciągły proces edukacyjny obejmujący wiele aspektów związanych z cyberzagrożeniami może być skuteczny.



GRAHAM CARR

Prezydent, Wicekanclerz
Concordia University Montreal, Kanada

Jako gospodarze największego w Kanadzie uniwersyteckiego cyber labu, zauważyliśmy ze strony studentów i społeczeństwa, szybki wzrost zainteresowania tą strategiczną i błyskawicznie rozwijającą się dziedziną. Kluczowe znaczenie dla naszego połączonego w sieci świata ma wyedukowanie, w zakresie cyberbezpieczeństwa, kolejnego pokolenia. Pożądanym jest podejście łączące różne perspektywy, specjalistyczną wiedzę i zrównoważone zarządzanie.



FRANCESCO CHIARINI

Dyrektor ds. Projektów Międzynarodowych
ISSA Polska

Najlepsi specjaliści od cyberbezpieczeństwa potrzebują więcej niż tylko wiedzy w swojej dziedzinie. Ewolucja w IT wymaga współpracy wszystkich zajmujących się bezpieczeństwem informacji. Szersze zrozumienie implikacji prawnych bezpiecznego kodowania/konfiguracji, procedur reagowania, ustalania organizacyjnych procedur, jest dziś niezbędne. Cyberbezpieczeństwo powinno łączyć koncepcję bezpieczeństwa z procesami biznesowymi, kodowaniem i reagowaniem organizacji. Potrzebujemy nieustannej edukacji, by być na topie i nie możemy zapomnieć o prawdziwym merytorycznym partnerstwie z kolegami po fachu wewnątrz i na zewnątrz firmy.

EKSPERCI O WADZE INTERDYSCYPLINARNEJ EDUKACJI



JOLANTA PLIETH-CHOLEWIŃSKA

Departament Strategii, Współpracy Zagranicznej i Informacji Publicznej
Główny Urząd Geodezji i Kartografii

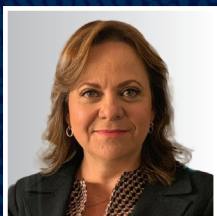
Jak niezwykle ważne jest cyberbezpieczeństwo przekonujemy się szczególnie teraz w czasie pandemii, gdy niemal wszystkie działania instytucji i firm przeniosły się w cyberprzestrzeń. Jednocześnie zwiększa się zagrożenie w tej sferze. Dla ochrony nie wystarczy już tylko dobre zabezpieczenie informatyczne. Potrzebne jest połączenie działań specjalistów wielu dziedzin, by skutecznie zapobiegać atakom i reagować na nie. Jedną z nich jest Public Relations - bez dobrze przygotowanej i poprowadzonej komunikacji, dzięki której rzetelnie informujemy i edukujemy, nie ma mowy o pełnym cyberbezpieczeństwie.



ALEKSANDER CZARNOWSKI

Prezes AVET Information and Network Security
Sędzia w turnieju CyberSecurity Challenge PL2020

Niewiele jest tak interdyscyplinarnych gałęzi jak cyberbezpieczeństwo. To też jeden z powodów dlaczego domena jest często niewłaściwie wykładana. Dla dobrego i pełnego ujęcia tematu potrzeba nie tylko wiedzy z zakresu IT, teorii bezpieczeństwa informacji, kryptografii, projektowania algorytmów, ale również nauk kojarzonych z kierunkami humanistycznymi, jak prawo i biznesowymi jak zarządzanie czy ekonomia. Do realizacji rozsądnych celów cyberbezpieczeństwa potrzeba dobrego zrozumienia biznesowych potrzeb organizacji. Musimy też rozumieć wewnętrzne języki organizacji: język IT, developerów, architektów, prawników, działu compliance i audytu, język biznesu wysokiej kadry kierowniczej i rady nadzorczej.



MARTHA DELGADO

Podsekretarz ds. Wielostronnych Stosunków i Praw Człowieka
Ministerstwo Spraw Zagranicznych, Rząd Meksyku

Miliardy użytkowników IT, intensyfikują codzienne wykorzystanie technologii. Edukacja ma kluczowe znaczenie dla zapewnienia równowagi między możliwościami rozwoju, ochroną praw podstawowych i promocją pokojowego i zgodnego z prawem korzystania z technologii informacyjnych. Edukacja zwiększa świadomość i daje możliwość wyboru. Użytkownicy IT mają prawo korzystać z dobrodziejstwa i potencjału technologii, ale równolegle powinni rozumieć potencjalne zagrożenia. Trzeba nadążać za innowacjami, gdyż zawsze można się czegoś nauczyć, a jeśli wiedza jest potęgą w świecie rzeczywistym, to jest również siłą w świecie wirtualnym. Wiedza o cyberbezpieczeństwie stanie się integralnym elementem edukacji, biorąc pod uwagę potrzebę naszej alfabetyzacji cyfrowej w codziennym funkcjonowaniu. Wiedza zawsze będzie najlepszą obroną przed wyzwaniami, które są przed nami.

EKSPERCI O WADZE INTERDYSCYPLINARNEJ EDUKACJI



BRUCE DORRIS, J.D., CFE, CPA

Prezes

CEO Stowarzyszenia Certified Fraud Examiners

W kontekście pandemii COVID-19 edukacja o cyberbezpieczeństwie jest ważniejsza niż kiedykolwiek wcześniej. Organizacje obserwują bowiem znaczący wzrost ryzyka cyberprzestępczości. Informacje to waluta cyfrowej ery, uzyskanie dostępu do zastrzeżonych danych jest cenniejsze niż kradzież gotówki. Przedsiębiorstwa, we wszystkich branżach, potrzebują kompetentnych osób w zakresie cyberbezpieczeństwa, by rozwijać zaawansowane programy chroniące ich aktywa informacyjne. Dokładnie na tej samej zasadzie, jak robiły to w przeszłości chroniąc aktywa finansowe. Dobrze wyszkoleni eksperci ds. cyberbezpieczeństwa są niezbędnym zasobem dla każdej firmy.



DR HAB. WOJCIECH FILIPKOWSKI

Prof. UwB

Pracownia Kryminalistyki, Katedra Prawa Karnego i Kryminologii

Wydział Prawa, Uniwersytet w Białymstoku

Badanie zjawiska cyberbezpieczeństwa, a w szczególności cyberprzestępczości, w sposób tradycyjny, to jest z punktu widzenia pojedynczych dziedzin wiedzy, daje zaledwie jednostronne spojrzenie. Takie podejście jest obciążone wadą niekompletności. Osoby, które w sektorze prywatnym lub publicznym będą zajmować się przeciwdziałaniem i zwalczaniem wielowymiarowych zagrożeń w cyberprzestrzeni muszą być wyposażone w kompetencje umożliwiające im interdyscyplinarne podejście do poszukiwania adekwatnych rozwiązań. Dlatego, moim zdaniem, warto wykorzystać potencjał kryminologii i kryminalistyki w procesie ich edukacji.



PŁK DR HAB. INŻ. MARIUSZ FRĄCZEK, PROF. AWL

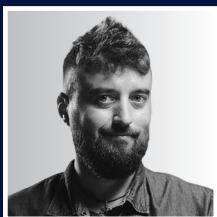
Zakład Bezpieczeństwa w Cyberprzestrzeni

Instytut Inżynierii Bezpieczeństwa, Wydział Nauk o Bezpieczeństwie

Akademia Wojsk Lądowych im. gen. T. Kościuszki

Kształcenie w obszarze bezpieczeństwa w cyberprzestrzeni jest jednym z priorytetów edukacji kadry oraz kandydatów na żołnierzy zawodowych, który wynika bezpośrednio z potrzeb Sił Zbrojnych Rzeczypospolitej Polskiej. Przygotowujemy specjalistów do nowych wyzwań oraz realizacji zadań nie tylko podczas działań kinetycznych, w trakcie sytuacji kryzysowych, ale także w piątej domenie funkcjonowania człowieka. Kładziemy wysoki nacisk na umiejętności praktyczne.

EKSPERCI O WADZE INTERDYSCYPLINARNEJ EDUKACJI



PIOTR GNYP

Dyrektor ds. Rozwoju Biznesu
Walkabout Games
Sędzia w turnieju CSC PL2020

Nasze życie w dużej mierze przeniosło się do przestrzeni wirtualnej. Higiena pracy w tym środowisku powinna być równie ważna co higiena osobista, a do wiedzy o tym, co zrobić w przypadku pożaru, wypadku czy powodzi powinno dość szkolenie z działania w trakcie i po cyberataku. No i oczywiście z tego co zrobić, by do niego nie dopuścić.



DR MACIEJ HULICKI

Kierownik kierunków „Człowiek w cyberprzestrzeni” i „Bezpieczeństwo w gospodarce cyfrowej”
Wydział Prawa i Administracji
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

Złożoność problemów występujących w środowisku cyfrowym wymaga stosowania kompleksowych rozwiązań i koordynacji działań. Jako, że cyberbezpieczeństwo łączy w sobie zagadnienia z różnych domen, edukacja w tym zakresie wymaga interdyscyplinarnego podejścia, które uwzględni wiedzę i doświadczenie wielu dziedzin. Umożliwia to całościowe zrozumienie istoty tego zjawiska i poznanie różnorodnych rozwiązań, które można wykorzystać do walki z zagrożeniami związanymi z cyfryzacją. To zaś może przyczynić się do uzyskania efektu synergii, a tym samym zwiększy efektywność podejmowanych działań.



PROF. DR HAB. KRZYSZTOF JAJUGA

Kierownik Katedry Inwestycji Finansowych i Zarządzania Ryzykiem
Uniwersytet Ekonomiczny we Wrocławiu
Prezes CFA Society Poland

Sukcesy w biznesie są dziś osiągnięte dzięki kreowaniu nowych idei oraz współpracy interdyscyplinarnych zespołów, wykorzystujących efekt synergii jego członków. Efektem takiej współpracy jest raport o interdyscyplinarnej edukacji w zakresie cyberbezpieczeństwa. Zmiany technologiczne, oprócz bezdyskusyjnych korzyści, prowadzą też do wzrostu ryzyka, zaś edukacja jest warunkiem koniecznym skutecznego zarządzania tym ryzykiem. Waga edukacji interdyscyplinarnej wynika również z tego, że współczesny absolwent szkoły wyższej będzie w swoim życiu zmieniał zawód co najmniej kilkakrotnie, ułatwi mu to interdyscyplinarna wiedza.

EKSPERCI O WADZE INTERDYSCYPLINARNEJ EDUKACJI



PROF. MICH KABAY, CISSP-ISSMP

Wydział Cyberbezpieczeństwa

Norwich University - The Military College of Vermont

Proces postępującej integracji technologii informatycznych z właściwie każdą już dziedziną życia, doprowadził do wzrostu znaczenia bezpieczeństwa informacji (z ang. information assurance- IA). E-mail, chat, VoIP i media społecznościowe stwarzają okazję do nadużyć od naruszenia prywatności, poprzez zastraszanie, kradzież danych po odmowę dostępu. Z kolei rozwój IoT dotyczy również systemów krytycznych kontrolowanych przez niewłaściwie zaprojektowane i wdrożone oprogramowanie w kontrolerach procesów przemysłowych i urządzeniach medycznych w których błędy i ataki mogą mieć katastrofalne skutki. IA chroni wszystkich.

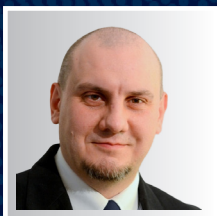


MARCIN KOBYLŃSKI, MBA, CISM, CRISC

Przewodniczący Komisji Rewizyjnej ISSA Polska

Sędzia w turnieju CSC PL2020

Zestaw kompetencji podstawowych „cyberbezpiecznika” powinien zawierać znajomość: technologii informatycznych, matematyki wyższej, programowania/testowania oprogramowania, języków obcych, podstaw ekonomii, prawa, psychologii/socjologii, zagadnień związanych z biometrią. Interdyscyplinarność była, jest i pozostanie niezbędna dla każdej osoby zajmującej się zawodowo cyberbezpieczeństwem. Znamiennym przykładem jest jeden z nestorów polskiego cyberbezpieczeństwa ppłk. Jan Kowalewski. Wstąpił się m.in. złamaniem szyfrów sowieckich w 1919/1920 r. Ukończył liceum handlowe, chemię na Uniwersytecie w Liège, znał biegle kilka języków obcych. Nie posiadał wykształcenia matematycznego, ale znał realia służby w carskich wojskach łączności. Cechował go otwarty, logiczny i dociekliwy umysł oraz dobra pamięć.



HUBERT ŁABĘCKI

Przewodniczący Grupy ds. Ciągłości Działania przy Związku Banków Polskich

Przesunięcie większości aktywności współczesnego społeczeństwa w obszarze globalnej sieci internetowej i wirtualnej rzeczywistości, powoduje, że zmienia się charakter i specyfika zagrożeń, z którymi musimy się zmierzyć. Obecnie dostęp do informacji jest jednym z kluczowych aktywów – im szerzej rozumiemy powiązania pomiędzy różnymi elementami otaczającego nas środowiska i infrastruktury tym szybciej i skuteczniej będziemy mogli zapobiegać, chronić i reagować na materializację istniejących i przyszłych zagrożeń. Dlatego tak ważne dla tworzenia świadomego społeczeństwa jest budowanie interdyscyplinarnej wiedzy z zakresu szeroko rozumianego bezpieczeństwa, w tym cyberbezpieczeństwa.

EKSPERCI O WADZE INTERDYSCYPLINARNEJ EDUKACJI



DANIEL MCMAHON, FCPA, FCA

Rektor

Uniwersytet Quebecu w Trois-Rivières, Kanada

Bezpieczeństwo cyfrowe dla środowiska akademickiego wiąże się kilkoma ważnymi kwestiami: zagwarantowaniem integralności naszej infrastruktury IT, ochroną danych poufnych członków społeczności, ochroną danych badawczych przy jednoczesnym pogodzeniu etyki i badań otwartych oraz szkoleniem studentów i pracowników. Rozwój w erze cyfrowej wymaga ostrożności i czujności, ale także prewencji, i edukacji. Nasi absolwenci to liderzy jutra, mamy zatem obowiązek pomóc im, by byli świadomi i wyposażeni w narzędzia do stawienia czoła obecnym, i przyszłym wyzwaniom, w tym bezpieczeństwu cyberprzestrzeni.

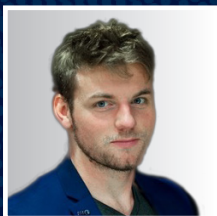


GENEVIÈVE MOTTARD, CPA, CA

Prezes, Dyrektor Zarządzająca

Order of Chartered Professional Accountants, prowincja Quebec

Zarządzanie ryzykiem leży w sercu naszej profesji. Wraz z cyfryzacją firm, w erze big data, cyberzagrożenia to koszmar dla firm. W dynamicznie zmieniającym się otoczeniu biznesu, cyberbezpieczeństwo ma kluczowe znaczenie dla zapewnienia dobrego zarządzania ryzykiem i podejmowania decyzji opartych na właściwej informacji. Kolejna generacja specjalistów w naszej profesji musi rozumieć czym jest cyberbezpieczeństwo.



BARTOSZ POSTULKA

Akademia Górniczo-Hutnicza im. S. Staszica w Krakowie

AGH Space Systems

Demokratyzacja przestrzeni kosmicznej otworzyła nowy horyzont dla badań i innowacji. Nowe możliwości ukazują jednak nowe słabe punkty w zakresie kosmicznego cyberbezpieczeństwa. Satelity komercyjne komunikują się z Ziemią bezprzewodowo, często za pomocą standardowych protokołów TCP czy UDP jako warstwy transportowej. Interdyscyplinarne podejście do edukacji umożliwia zrozumienie zagadnienia cyberbezpieczeństwa jako stałego elementu systemów telekomunikacyjnych zarówno naziemnych jak i orbitalnych. Dobrym przykładem tego typu działań są hackathony jako miejsce do nauki i rozwoju studentów.

EKSPERCI O WADZE INTERDYSCYPLINARNEJ EDUKACJI



DR HAB. INŻ. PIOTR PRYZSTAŁKA

Z-ca Kierownika Katedry Podstaw Konstrukcji Maszyn
Wydział Mechaniczny Technologiczny

Edukacja w zakresie cyberbezpieczeństwa systemów automatyki powinna być podejściem praktycznym z wykorzystaniem nowoczesnych narzędzi wspomagających proces dydaktyczny. W tym aspekcie szczególnie ważną rolę odegrają symulatory procesów przemysłowych uwzględniające scenariusze cyberataków. Ze względu na brak komercyjnych symulatorów o takiej funkcjonalności członkowie Koła Naukowego AI-METH zaprojektowali i zbudowali stanowisko laboratoryjne do symulacji cyberataków na przemysłowe systemy sterowania. Otwiera to nowe możliwości dydaktyczne i badawcze dając podwaliny pod kolejne inicjatywy np. związane z rozwojem systemów detekcji i izolacji cyberataków



KMDR POR. DR INŻ. PRZEMYSŁAW RODWALD

Kierownik Zakładu Systemów Komputerowych
Katedra Informatyki
Akademia Marynarki Wojennej

W Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej podkreślono potrzebę rozwijania interdyscyplinarnych specjalizacji związanych z cyberbezpieczeństwem na uczelniach wyższych. To właśnie interdyscyplinarność, rozumiana jako połączenie zagadnień teleinformatycznych, technologicznych, prawnych, ekonomicznych, organizacyjnych oraz militarnych, jest kluczem do zapewnienia bezpieczeństwa w cyberprzestrzeni. Kluczem, ale też nie lada wyzwaniem stojącym przed współczesnym systemem edukacji.



TOMASZ SADOWSKI

Naczelnik Departamentu Bezpieczeństwa, Narodowy Bank Polski
Sędzia w turnieju CSC PL2020

CyberSecurity Challenge PL2020, pozwolił jego uczestnikom doświadczyć jak trudnym i złożonym jest proces zarządzania kryzysowego. Uczestnictwo w tym nowatorskim projekcie, studentów z wielu specjalizacji, przyczyniło się do spojrzenia na omawiane problemy z różnych perspektyw. Cyberbezpieczeństwo to bez wątpienia globalne wyzwanie więc budowanie odpowiedzialnej świadomości o cyberzagrożeniach staje się w obecnych czasach kluczowe.

EKSPERCI O WADZE INTERDYSCYPLINARNEJ EDUKACJI



DR RÉMI QUIRION, OC, CQ, FRSC

Główny Naukowiec Quebecu, Kanada
Rząd Quebecu

Alfabetyzm cyfrowy jest dziś koniecznością. Podczas pandemii COVID-19 doświadczyliśmy tego wyraźniej niż kiedykolwiek wcześniej. W tym kontekście rozwój nauk powiązanych z cyberbezpieczeństwem i edukacja w tym zakresie powinny być silnie promowane na uniwersytetach, ale także wśród szeroko pojętego społeczeństwa.



MAŁGORZATA WEBER

Rzecznik Prasowy Agencji Mienia Wojskowego
Sędzia w turnieju CSC PL2020

Najtrudniejszym wyzwaniem w cyberbezpieczeństwie jest nieustannie zmieniający się charakter zagrożeń. Dlatego dziś tak ważne jest ich ciągłe monitorowanie. Ale równie istotna jest interdyscyplinarna edukacja, która pozwoli zbudować świadomość społeczną w tym zakresie i aktywnie przeciwdziałać zagrożeniom. Dzisiejsi studenci wkrótce zasilą szeregi pracowników różnych firm czy instytucji i dlatego już na studiach powinni zostać przygotowani do nowej rzeczywistości oraz wyposażeni we wszechstronną wiedzę i narzędzia, które pozwolą im sprostać cyber-wyzwaniom. Doświadczenie w turnieju CSC PL2020 na pewno im w tym pomoże.



DR HAB. INŻ. KAZIMIERZ WORWA

Prorektor ds. Kształcenia
Wojskowa Akademia Techniczna

Skuteczne zapewnienie bezpieczeństwa w cyberprzestrzeni, powszechnie rozumianej jako przestrzeni przetwarzania i wymiany informacji, tworzonej przez systemy teleinformatyczne z całokształtem powiązań pomiędzy nimi oraz relacji z ich użytkownikami, jest bardzo złożonym i wieloaspektowym problemem, obejmującym m.in. zagadnienia o charakterze organizacyjnym, prawnym, ekonomicznym czy wojskowym. Determinuje to konieczność interdyscyplinarnego podejścia do edukacji w zakresie cyberbezpieczeństwa, przy czym bardzo ważne, m.in. ze społecznego punktu widzenia, jest zapewnienie powszechnego i ciągłego charakteru tej edukacji.

EKSPERCI O WADZE INTERDYSCYPLINARNEJ EDUKACJI



MGR INŻ. ANNA ROMAŃSKA-ZAPAŁA

Katedra Automatyki i Technik Informatycznych
Wydział Inżynierii Elektrycznej i Komputerowej
Politechnika Krakowska im. T. Kościuszki

Cyberbezpieczeństwo to podstawa prawidłowego funkcjonowania każdego systemu. Nowe technologie i innowacyjne rozwiązania wtargnęły we wszystkie dziedziny życia. Kluczem do sukcesu w przyszłości jest wypracowanie potrzeby współpracy w interdyscyplinarnych zespołach, gdzie wykorzystując wiedzę specjalistów z różnych dziedzin będą tworzone kompletne oraz optymalne produkty i usługi z zapewnieniem cyberbezpieczeństwa. Najłatwiej to osiągnąć poprzez odpowiednie modelowanie programu studiów, warunków do współdziałania w ramach kół naukowych, realizację projektów badawczo-wdrożeniowych, czy celową współpracę z przemysłem.



ALBERTO ZUCCONI

Sekretarz Generalny
World University Consortium

Potrzeba edukacji w zakresie cyberbezpieczeństwa jest bezdyskusyjna. Zapewnia nam ona skuteczne narzędzie do ochrony i promowania praw indywidualnych i zbiorowych, wspierając równoległe procesy niezbędne do osiągnięcia zrównoważonego rozwoju i dobrobytu.

AMBASADOROWIE O POTRZEBIE EDUKACJI O CYBERBEZPIECZEŃSTWIE



H.E. JÜRG LAUBER

Przewodniczący Otwartej Grupy Roboczej ds. Cyberbezpieczeństwa (OEWG)
Stały Przedstawiciel Szwajcarii przy ONZ

W erze cyfryzacji rozwój technologii postępuje szybciej niż nasze zrozumienie dla konsekwencji tego procesu. W połączonej przez technologie informacyjne świecie, edukacja w zakresie cyberbezpieczeństwa jest coraz bardziej istotna dla wszystkich kierunków studiów. Wojewódzkie Cyber Laby to ważna inicjatywa na rzecz budowania niezbędnej nam świadomości. Bezpieczeństwo cybernetyczne może być tylko tak silne, jak jego najstarsze ogniwo. Życzę młodym Ambasadorom tworzącym ten projekt powodzenia w działaniach.



H.E. LLOYD BRODRICK

Ambasador Australii w Polsce

W połączonej i zdominowanej przez nowe technologie rzeczywistości zapewnienie stabilności, i bezpieczeństwa naszej infrastruktury cyfrowej ma fundamentalne znaczenie. By stawić czoła międzynarodowym wyzwaniom w zakresie cyberbezpieczeństwa, Rząd Australii coraz więcej inwestuje w zdolności w zakresie cyberbezpieczeństwa, zacieśniając równolegle współpracę z podobnie myślącymi partnerami z administracji publicznej, organizacji pozarządowych i biznesu. Sprostanie tym wyzwaniom, wymaga wykształcenia nowej generacji ekspertów w naukach technicznych i regulacjach oraz traktowania wysokiej jakości edukacji w zakresie cyberbezpieczeństwa jako podstawowego dobra publicznego.



H.E. JUHA OTTMAN

Ambasador Republiki Finlandii w Polsce

Znaczenie świata cyfrowego dla polityki zagranicznej, bezpieczeństwa i obronności wzrasta, i będzie rość gwałtownie na całym świecie. Proces ten wymaga przygotowania nie tylko od rządów, ale całego społeczeństwa. Bezpieczeństwo cybernetyczne powinno zajmować wysokie miejsce w świadomości każdego użytkownika technologii cyfrowych, a kluczem do tego jest edukacja. Dla nas, Finów, celem edukacji jest przygotowanie młodzieży do wyzwań XXI wieku i do wyrobienia nawyku uczenia się przez całe życie. W 2019 roku światowy indeks Educating for the Future ocenił Finlandię jako światowego lidera w nauczaniu umiejętności na przyszłość. Uważamy, że cyberbezpieczeństwo za jedno z kluczowych wyzwań przyszłości.

AMBASADOROWIE O POTRZEBIE EDUKACJI O CYBERBEZPIECZEŃSTWIE



H.E. CLEMENTINE SHAKEMBO KAMANGA

Ambasador Demokratycznej Republiki Konga

Chcielibyśmy uniknąć cyfrowego chaosu w Afryce. W DRK dostęp do Internetu jest luksusem dla znacznej części społeczeństwa. Używany w administracji i instytucjach państwowych, nie jest powszechny w środowisku akademickim. Nadużycia i cyberprzestępczość stanowią przeszkodę w korzystaniu z sieci w szkołach. Internet powinien zapewniać bezpieczną przestrzeń dla edukacji. Zapraszam społeczność międzynarodową do współpracy z nami, by pomóc afrykańskim uczniom w zapewnieniu dostępu do Internetu, budowaniu ich umiejętności i rozwijaniu ich potencjału.



H.E. ALEXANDER BEN ZVI

Ambasador Izraela w Polsce

Ekosystem cyberbezpieczeństwa Izraela oparty jest na współpracy sektora publicznego, prywatnego i środowiska akademickiego. Pomaga to zagwarantować bezpieczeństwo izraelskiej cyberprzestrzeni, zapewniając ochronę krytycznej infrastruktury wojskowej i cywilnej. Cyberedukacja jest istotnym elementem tego ekosystemu. Uświadamianie i kształcenie o cyberwyzwaniach od najmłodszych lat, połączone z równoległym szkoleniem kolejnych generacji cybereksperatów ma kluczowe znaczenie dla bezpieczeństwa kraju i jego obywateli.



H.E. EDGARS BONDARS

Ambasador Litwy w Polsce

W erze cyfryzacji cyberprzestrzeń jest ważną platformą codziennych interakcji, w tym społecznych i osobistych. By środowisko to było bezpieczne i niezawodne, użytkownicy technologii informacyjno-komunikacyjnych (ICT) muszą znać zasady cyberhigieny. Zasadnicze znaczenie dla poprawy naszej wiedzy oraz zrozumienia zagrożeń i możliwości w cyberprzestrzeni mają oprócz polityki publicznej, współpraca między organizacjami pozarządowymi i biznesem.

AMBASADOROWIE O POTRZEBIE EDUKACJI O CYBERBEZPIECZEŃSTWIE



H.E. PAUL SCHMIT

Ambasador Wielkiego Księstwa Luksemburga w Polsce

Dla kraju budującego swoją siłę gospodarczą w oparciu o ICT i cyfryzację, cyberbezpieczeństwo ma zasadnicze znaczenie. Kluczowym jest zbudowanie zaufania obywateli i biznesu do IT. Dla Luksemburga bezpieczeństwo cybernetyczne to zadanie wymagające współpracy, angażujące rządy, firmy i osoby prywatne. W społeczeństwie cyfrowym rozwój umiejętności w zakresie cyberbezpieczeństwa jest nową podstawą, którą należy uwzględnić w edukacji. Bezpieczeństwo cybernetyczne wzmacnia naszą pozycję. Jeśli nie jesteśmy świadomi cyberzagrożeń i dobrych praktyk, chroniących nas przed nimi, atakujący celują w nasze ludzkie słabości, łatwo je namierzając. Podnoszenie świadomości i szkolenia w formie studiów przypadków są ogromnym wsparciem dla rozwoju naszej cyberodporności.



H.E. BOŽENA FORŠTNARIČ BOROJE

Ambasador Słowenii w Polsce

W 21 wieku wyzwania związane z bezpieczeństwem odchodzą od tradycyjnego – fizycznego pojmowania domeny. Obecne zagrożenia dla naszego bezpieczeństwa funkcjonują w sferze dominującej nasze codzienne życie - w Internecie. Pandemia COVID-19 utrwaliła nowy sposób wykonywania codziennych czynności. Coraz więcej czasu spędzamy w wirtualnym świecie, wykorzystując go do nauki, pracy i relacji towarzyskich. Ponieważ życie online stanowi tak ogromną część życia ludzi, należy zwrócić większą uwagę na edukację o możliwych zagrożeniach, sposobach ich rozpoznawania oraz ochronę nas i naszych dzieci. Zwiększenie odporności na cyberzagrożenia musi stać się wspólnym celem.



H.E. JÜRG BURRI

Ambasador Szwajcarii w Polsce

Szwajcaria popiera inicjatywy takie jak „Regional Cyber Labs”, a Ambasada Szwajcarii w Polsce jest dumna, że może im patronować. Polska znana jest z talentów w branży IT i jest też doskonałym dostawcą usług IT, w tym rozwiązań z zakresu cyberbezpieczeństwa. Jako kraj kładziemy duży nacisk na badania, silną ochronę prawną, najwyższe bezpieczeństwo, zarządzanie centrami danych i centrami bezpieczeństwa operacyjnego. Promujemy również dobre praktyki w funkcjonowaniu Internetu: Szwajcaria jest hubem dla kluczowych międzynarodowych instytucji, Internet Governance Forum, Międzynarodowego Związku Telekomunikacyjnego (ITU), Fundacji ICT4Peace, Genewskiego Centrum Polityki Bezpieczeństwa czy Światowego Forum Ekonomicznego. Wszystkie one aktywnie działają w cyberbezpieczeństwie i są wspierane przez Szwajcarię!

AMBASADOROWIE O POTRZEBIE EDUKACJI O CYBERBEZPIECZEŃSTWIE



H.E. STEFAN GULLGREN

Ambasador Królestwa Szwecji w Polsce

Edukacja w zakresie cyberbezpieczeństwa jest kluczowym elementem krajowej strategii bezpieczeństwa cybernetycznego Szwecji. Wraz z rozwojem i zwiększającym się wykorzystaniem technologii 5G, przepływ informacji w naszych społeczeństwach będzie szybko wzrastał. Otworzy to ogromne możliwości, równolegle pociągając za sobą pewne zagrożenia. Należy i można je złagodzić różnymi środkami, w tym przez podnoszenie świadomości o cyberbezpieczeństwie. Te działania powinny obejmować edukację młodzieży i studentów. Dlatego też gorąco popieramy inicjatywę fundacji The Bridge i jej integralny element turniej Cybersecurity Challenge PL2020. Bezpieczeństwo cybernetyczne jest obszarem o dużym potencjale współpracy między Szwecją a Polską. Będziemy silniejsi, działając wspólnie.



H.E. GEORGETTE MOSBACHER

Ambasador Stanów Zjednoczonych w Polsce

W miarę jak technologia cyfrowa w coraz większym stopniu wkracza w nasze życie, ujawniają się nowe słabe punkty w naszych sieciach i – szerzej – cyberprzestrzeni. Wszyscy musimy więc zwiększyć naszą wiedzę na temat bezpieczeństwa cybernetycznego i lepiej chronić nasze sieci. Stany Zjednoczone stale inwestują i poszerzają programy, które budują potencjał merytoryczny naszych przyszłych specjalistów w dziedzinie bezpieczeństwa cybernetycznego, już od szkoły podstawowej poprzez edukację pomaturalną. Współpracujemy z wieloma krajami na całym świecie – w tym z Polską – aby promować najlepsze praktyki w zakresie bezpieczeństwa cybernetycznego poprzez upowszechnianie wspólnej wizji otwartego, interoperacyjnego, niezawodnego i bezpiecznego Internetu, który sprzyja inwestycjom i otwiera nowe rynki gospodarcze.



H.E. MARTIN ROGER

Ambasador Republiki Estonii w Polsce

W wyniku pandemii COVID-19 musieliśmy szybko i skutecznie przystosować się do codziennego i efektywnego użycia technologii, by zagwarantować ciągłość procesu edukacji. Musimy zadbać o to, aby uczniowie i studenci mogli bezpiecznie działać w cyfrowym świecie, by byli świadomi zagrożeń, potrafili zachować niezbędną cyberhigienę i posiadali umiejętności radzenia sobie z zagrożeniami cybernetycznymi.



Postępująca transformacja cyfrowa, a wraz z nią rosnąca zależność domen oddziałują na wszystkich użytkowników sieci. Z punktu widzenia naszego dobrostanu, zarówno w ujęciu mikro, jak i makro kluczową kwestię, w procesie powszechnej cyfryzacji, stanowi bezpieczeństwo informacji.

Edukacja promująca prawidłowe zachowania i dobre praktyki powinna być wprowadzana możliwie jak najwcześniej, ze wskazaniem na zajęcia z informatyki w szkołach podstawowych. Natomiast kontynuacja ukierunkowanego podejścia do cyberbezpieczeństwa winna odbywać się w szkołach średnich i wyższych.

Koncentrując przedmiot omawianego raportu na poziomie uczelni wyższych poddajemy, pod rozwałę szerokiego gremium, propozycje wdrożenia zmian programowych, które umożliwią studentom nabycie, oczekiwanych przez pracodawców kompetencji, i wpłyną równolegle na podniesienie ogólnego poziomu cyberbezpieczeństwa, w ujęciu jednostki i instytucjonalnym.

Z lektury raportu wyłtywa jeden, wspólny dla wszystkich domen, wniosek. Problematyce cyberbezpieczeństwa, na znaczącej większości kierunków, nie poświęca się należytej uwagi, a dydaktyka, nie współgra z dynamicznymi zmianami i oczekiwaniami rynku.

Zwalczanie cyberprzestępczości jest wyzwaniem interdyscyplinarnym, wymagającym współpracy między wieloma domenami. Niezbędnym, w naszym przekonaniu, jest wprowadzenie nauczania o bezpieczeństwie w sieci we wszystkich omawianych obszarach.

Przedstawione w raporcie rekomendacje mają na celu stworzenie pola do dialogu i działań.

Z opinii zebranych od studentów uczelni wyższych z całej Polski, wyselekcjonowane zostały najistotniejsze aspekty, na które według nas, powinno zwrócić się, w najbliższych latach, szczególną uwagę.

*Studenci – współautorzy raportu
„Nowe otwarcie w edukacji o cyberbezpieczeństwie”*

PARTNERZY – ORGANIZACJE STUDENCKIE



REGIONAL
CYBER LABS

#EkosystemCyberbezpieczeństwa



THE BRIDGE
FOUNDATION



REGIONAL
CYBER LABS

CYBERWYZWANIE NIE ZNAJĄ GRANIC



REGIONAL
CYBER LABS

#RegionalCyberLabsPL20/21
@CyberPoland



ZAPRASZAMY DO WSPÓŁPRACY



THE BRIDGE
FOUNDATION



REGIONAL
CYBER LABS

- „3-2-1 Backup Rule: The Rule of Thumb to Solve Your Data Loss Problems”. Udośćępniono 29 lipiec 2020. <https://securityboulevard.com/2020/05/3-2-1-backup-rule-the-rule-of-thumb-to-solve-your-data-loss-problems/>.
- „7 Zasad przetwarzania danych osobowych”. Udośćępniono 29 lipiec 2020. <https://praksyma.pl/7-zasad-przetwarzania-danych-osobowych/>.
- 300RESEARCH. „Efekt zamrożenia. Szansa na radykalną cyfryzację gospodarki”, b.d. https://impactcee.com/reaction/2020/wp-content/uploads/2020/06/raport_cyfryzacja_final.pdf.
- „2018 NortonLifeLock Cyber Safety Insights Report”. NortonLifeLock, 2018. <https://www.nortonlifelock.com/us/en/newsroom/press-kits/2018-norton-lifelock-cyber-safety-insights-report/>.
- Amazon. „Dynamo: Amazon’s Highly Available Key-value Store”, b.d. <https://www.allthingsdistributed.com/files/amazon-dynamo-sosp2007.pdf>.
- AON Polska. „Zarządzanie ryzykiem i Ubezpieczeniami w Firmach w Polsce- Edycja VI”, b.d. https://aoncomauthoring.blob.core.windows.net/aoncom2017media/aon.com/media/poland/publikacje/raport%202019-2020/raport-grms-polska-2019-20.pdf?utm_source=Aoncom.
- Bandi, Ajay, Abdelaziz Fella, i Harish Bondalapati. „Embedding Security Concepts in Introductory Programming Courses”. School of Computer Science and Information Systems Northwest Missouri State University Maryville, b.d. <https://www.nwmissouri.edu/csis/msacs/PDF/Fall%202019/p78-bandi.pdf>.
- „Breach Barometer Report: Year in Review”. Protenus, 2016.
- C. Seacord, Robert. Secure Coding in C and C++ (2nd. ed.). Addison-Wesley Professional, 2013.
- CERT NZ. „Guide - Default credentials”. Udośćępniono 29 lipiec 2020. <https://www.cert.govt.nz/it-specialists/guides/default-credentials/>.
- „CI Security”, 02.08. <https://www.cisecurity.org>.
- „CVE - Common Vulnerabilities and Exposures”. Udośćępniono 29 lipiec 2020. <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=default+password>.
- Czech, Marta. Umowa powierzenia danych osobowych jako instrument ich ochrony (b.d.). https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/8735/1/M_Czech_Umowa_powierzenia_przetwarzania_danych_osobowych.pdf.
- „Czym są „dane wrażliwe” i czy PESEL jest „daną wrażliwą”?” Udośćępniono 29 lipiec 2020. <https://niebezpiecznik.pl/post/czym-sa-dane-wrażliwe-i-czy-pesel-jest-dana-wrażliwa/>.
- DARKreading. „User-Friendly Cybersecurity: Is a Better UX the Key to a Better Defense?” Udośćępniono 29 lipiec 2020. https://www.darkreading.com/edge/theedge/user-friendly-cybersecurity-is-a-better-ux-the-key-to-a-better-defense-/b/d-id/1337699?_mc=rss%5Fx%5Fdr%5Fedt%5Faud%5Fdr%5Fx%5F%2Drss%2Dsimple&page_number=1.
- „De Zan, Tommaso & franco, fabio. (2020). Cybersecurity skills development in the EU: The certification of cybersecurity degrees and ENISA’s Higher Education Database.” Udośćępniono 29 lipiec 2020. https://www.researchgate.net/publication/340416935_Cybersecurity_skills_development_in_the_EU_The_certification_of_cybersecurity_degrees_and_ENISA’s_Higher_Education_Database.
- Deloitte. „«Nowa normalność» dla sektora usług finansowych w Polsce, Europie i Azji”. b.d. https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Brochures/pl_FSI_Webinar_odcinek_nr_2_30.04_final.pdf.
- „Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa w sieci i systemów informatycznych na terytorium Unii”. Parlament Europejski, 6 lipiec 2016. https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/dyrektywa_NIS-1-Dyrektywa-NIS-3.pdf.
- EITCA. „Certyfikat EITC/IS/EEIS”. Udośćępniono 29 lipiec 2020. <https://pl.eitca.org/certyfikacja/eitciseis-gospodarka-elektroniczna-bezpiecze%C5%84stwo-informacji/?v=9b7d173b068d>.
- „EITCA”. Udośćępniono 29 lipiec 2020. <https://eitca.pl/is>.
- „Equifax used ‘admin’ as username and password internally”. Udośćępniono 29 lipiec 2020. <https://securityboulevard.com/2019/10/equifax-used-admin-as-username-and-password-internally/>.
- Google / Harris Poll. „Online Security Survey”, b.d. https://services.google.com/fh/files/blogs/google_security_infographic.pdf.
- havebeenpwned. „havebeenpwned”. Udośćępniono 29 lipiec 2020. <https://havebeenpwned.com/>.
- J. Jiang, i G. Bai. „Evaluation of Causes of Protected Health Information Breaches.”, 2019, 179,265.
- „Jak chronić swoje dane osobowe?” Udośćępniono 29 lipiec 2020. <https://uodo.gov.pl/pl/138/1221>.
- KPMG. „Barometr cyberbezpieczeństwa. W kierunku rozwiązań chmurowych”, b.d. <https://home.kpmg/content/dam/kpmg/pl/pdf/2020/06/pl-raport-kpmg-barometr-cyberbezpieczenstwa-2020-w-kierunku-rozwiazan-chmurowych.pdf>.
- „Krajobraz bezpieczeństwa polskiego internetu, Raport roczny 2019 z działalności CERT Polska”, 2019. https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf.
- Kruse, Clemens Scott, Benjamin Frederick, Taylor Jacobson, i D. Kyle Monticone. „Cybersecurity in healthcare: A systematic review of modern threats and trends”. Technology and Health Care 25, nr 1 (21 luty 2017): 1–10. <https://doi.org/10.3233/THC-161263>.
- Krutz, Daniel & Richards, Thomas. „Cyber security education: why don’t we do anything about it?” ACM Inroads, 8(4):5-5, 10.1145/3132217 (2017).
- lastline. „Practice what you Preach? 45% of Infosec professionals reuse passwords across multiple accounts, Lastline research says”. Udośćępniono 29 lipiec 2020. https://www.lastline.com/press/press_release_infosec2018_practice_what_you_preach/.
- „Maastricht University”. Udośćępniono 29 lipiec 2020. <https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-93-lessons-learned>.

BIBLIOGRAFIA

- Ministerstwo Rozwoju. „Raport Nowy Surowiec - otwarte zasoby danych dla polskiej gospodarki”, b.d. <https://www.gov.pl/web/rozwoj/raport-nowy-surowiec-otwarte-zasoby-danych-dla-polskiej-gospodarki>.
- „Navigating GDPR Compliance on AWS”, b.d. https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf.
- Niebezpiecznik. „Jakie hasła mają Polacy? Wyciek hasła 144 000 użytkowników Autocentrum.pl”. Udostępniono 29 lipiec 2020. <https://niebezpiecznik.pl/post/wyciek-hasel-144-000-uzytkownikow-autocentrum-pl>.
- OWASP WebGoat. „Learn the hack - Stop the attack”. Udostępniono 29 lipiec 2020. <https://owasp.org/www-project-webgoat/>.
- Kaspersky Lab. „Public WiFi Security”. Udostępniono 29 lipiec 2020. <https://usa.kaspersky.com/resource-center/preemptive-safety/public-wifi>.
- „Raport NASK - Cyber Policy AD”, b.d. 2019 https://cyberpolicy.nask.pl/wp-content/uploads/2020/05/Raport_CyberbezpieczenstwoAD2019_online.pdf.
- „Raport OECD - Measuring the Digital Transformation. A Roadmap for the Future”, b.d. <https://www.oecd-ilibrary.org/docserver/9789264311992-en.pdf?expires=1591890852&id=id&accname=guest&checksum=C9D41D565730C8FE77EF72FA3A78C46D>.
- „Raport OECD - The Future of Work. OECD Employment Outlook 2019”, b.d. <https://www.oecd-ilibrary.org/docserver/9ee00155-en.pdf?expires=1591891492&id=id&accname=guest&checksum=C5553CC9EBF0BF8D8C1514BA3113069C>.
- „Raport OECD - Trends Shaping Education 2019”, b.d. https://www.oecd-ilibrary.org/deliver/trends_edu-2019-en.pdf?itemId=/content/publication/trends_edu-2019-en&mimeType=pdf.
- „Raport ONZ - The Age of Digital Interdependence Report of the UN Secretary-General's High-level Panel on Digital Cooperation”, b.d. <https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-for-web.pdf>.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Pub. L. No. 2016/679 (2016). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- Kaspersky Lab. „Research on unsecured Wi-Fi networks across the world”. Udostępniono 29 lipiec 2020. <https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/>.
- „Share of households with internet access in the European Union (EU28) from 2007 to 2019”. Udostępniono 29 lipiec 2020. <https://www.statista.com/statistics/377585/household-internet-access-in-eu28/>.
- Stallings, W. Kryptografia i bezpieczeństwo sieci komputerowych. Gliwice: Helion, 2012.
- „Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej”, 31 lipiec 2020. https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf.
- OWASP, Web Security Testing Guide. „Testing for Default Credentials”. Udostępniono 29 lipiec 2020. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/02-Testing_for_Default_Credentials.
- „The Radicati Group, INC, Email Statistics Report, 2018-2022”. Udostępniono 29 lipiec 2020. https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report_2018-2022_Executive_Summary.pdf.
- Traynor, Patrick, Kevin Butler, William Enck, Patrick McDaniel, i Kevin Borders. „malnets: large-scale malicious networks via compromised wireless access points”. Special Issue: Special Issue on Security in Mobile Wireless Networks 3, nr 2-3 (2010): 102-113.
- Uchwała nr 125 Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 (2019). <http://www.dziennikustaw.gov.pl/M2019000103701.pdf>.
- Ustawa o ochronie danych osobowych (Dz. U. 2016 r. poz. 922), Pub. L. No. 922 (1997). https://archiwum.giodo.gov.pl/144/id_art/386/j/pl.
- Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, Pub. L. No. 1560 (2018). <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf>.
- Verizon. „2020 Data Breach Investigations Report”. Udostępniono 29 lipiec 2020. <https://enterprise.verizon.com/resources/reports/dbir/>.
- „W 2019 CERT Polska odnotował więcej cyberuderzeń”. Udostępniono 29 lipiec 2020. <https://www.telko.in/cert-polska-w-2019-r-odnotowal-wiecej-cyberuderzen>.
- „What personal data is considered sensitive?” Udostępniono 29 lipiec 2020. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en.
- Yubico. „2020 State of Password and Authentication Security Behaviors report”. Udostępniono 29 lipiec 2020. <https://www.yubico.com/blog/yubico-releases-2020-state-of-password-and-authentication-security-behaviors-report/>.
- The European Digital Strategy, <https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy>
- Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające program Cyfrowa, Europa na lata 2021–2027 <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2018:434:FIN>
- Raport NATO, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20190315_sgar2018-en.pdf

NOWE OTWARCIE W EDUKACJI O CYBERBEZPIECZEŃSTWIE	— 2
SŁOWO WSTĘPNE	— 3
ZASIĘG LOKALNY I MIĘDZYNARODOWY	— 4
METODYKA	— 5
KOORDYNATORZY DOMEN	— 6
REKOMENDACJE STUDENTÓW	— 7
DOMENA IT	— 9
KOMENTARZ EKSPERTA	— 17
DOMENA BIZNES	— 20
KOMENTARZ EKSPERTA	— 28
DOMENA MEDYCYNĄ	— 30
KOMENTARZ EKSPERTA	— 35
DOMENA PRAWO	— 38
KOMENTARZ EKSPERTA	— 46
DOMENA OBRONNOŚĆ	— 47
IMPULS DO ZMIAN	— 49
EKSPERCI O WADZE INTERDYSCYPLINARNEJ EDUKACJI	— 50
OPINIE AMBASADORÓW AKREDYTOWANYCH W POLSCE	— 60
PARTNERZY – ORGANIZACJE STUDENCKIE	— 65
CYBERWYZWANIA NIE ZNAJĄ GRANIC	— 66
BIBLIOGRAFIA	— 67

Fundacja The Bridge – organizacja non-profit, posiadająca specjalny status konsultacyjny przy Radzie Społeczno-Gospodarczej ONZ. Działa w Szwajcarii, Kanadzie i Polsce. Wspiera i realizuje programy edukacyjne obejmujące obszary wyzwań społeczno-gospodarczych i bezpieczeństwa.

#CSCPL2020 | **@CyberPoland**

Kontakt:

office@thebridge-foundation.org

+41 76 585 78 46

+48 601 214 041



THE BRIDGE
FOUNDATION