Czy sylabusy programowe na uczelniach nadążają za galopującą rewolucją cyfrową?

To temat przedstawionego przez fundację The Bridge, ogólnopolskiego raportu opinii środowiska studenckiego „Nowe otwarcie w edukacji o cyberbezpieczeństwie". Prezentacja odbyła się na Giełdzie Papierów Wartościowych w Warszawie, podczas inauguracji projektu wojewódzkich Cyber Labów.

Studenci, reprezentujący 35 uczelni, dokonali przeglądu programów nauczania, na kierunkach: biznesowych, IT, medycznych, prawniczych i wojskowych, pod kątem ekspozycji tematyki cyberbezpieczeństwa jako kluczowego wyzwania 21 wieku.

Omawiane kierunki studiów wpisane są w fundamenty cyfrowej transformacji na, co najmniej, najbliższe 10 lat. Analiza tych specjalności pod kątem szans i zagrożeń powstałych z korelacji postępu technologicznego i cyberbezpieczeństwa daje możliwości na wzmocnienie, i głębsze wykorzystanie kapitału intelektualnego studentów. Proces cyfryzacji gospodarki i społeczeństw generuje gruntowne zmiany dla systemu edukacji. Efekty tych przemian zależne będą od sposobu zarządzania transformacją cyfrową. Musimy sobie odpowiedzieć na pytanie czy programy na tych kierunkach umożliwiają studentom nabycie oczekiwanych przez rynek kompetencji i umiejętności? - Margo Koniuszewski, prezes fundacji The Bridge.

Poniżej syntetyczne ujęcie opinii studentów poszczególnych domen, szerzej, zaprezentowane w raporcie:

REKOMENDACJE STUDENTÓW KIERUNKÓW BIZNESOWYCH

Proponowane w raporcie rekomendacje, mają na celu wyposażyć studentów w kompetencje, pozwalające na funkcjonowanie w gospodarce cyfrowej. Budowanie świadomości o cyberzagrożeniach wpłynie pozytywnie na funkcjonowanie firm, a promocja dobrych praktyk przyczyni się do obniżenia ryzyka związanego z, nękającymi wszystkich, cyberatkami. Rozwój, opartego na technologii 5G, przemysłu 4.0 to impuls dla systemu edukacji do wprowadzenia koniecznych modyfikacji. Do obszarów wartych podkreślenia należą: ujęcie tematu cyberkryzysów w symulacjach biznesowych, w trakcie których studenci zarządzają wirtualnym przedsiębiorstwem, czy też wkomponowanie w przedmioty związane z zarządzaniem ryzykiem w firmie kontekstu cyber-ryzyka.

REKOMENDACJE STUDENTÓW KIERUNKÓW IT

Jednym z największych wyzwań w edukacji o cyberbezpieczeństwie, na technicznych kierunkach studiów, jest ograniczona liczba przedmiotów dotyczących bezpieczeństwa cyfrowego. Poruszane przez wykładowców obszary, z reguły, adresują jedynie podstawy dziedziny. W kontekście dynamicznego procesu cyfryzacji, nauczanie o cyberbezpieczeństwie powinno odbywać się na wszystkich kierunkach informatycznych, a nie tylko tych, związanych bezpośrednio z cyberbezpieczeństwem. W raporcie, zwrócono uwagę na kwestie przekazywania nieaktualnej wiedzy. Na zajęciach prezentowane są przestarzałe technologie i rozwiązania niemające już praktycznego zastosowania w sektorze IT. Istotnym problemem w nauczaniu o cyberbezpieczeństwie, przed którym stoi wiele uczelni, jest nieprzywiązywanie należytej uwagi do praktycznych umiejętności studentów. Opuszczający mury uczelni, dyplomowani specjaliści, bardzo często nie mieli styczności z symulacjami cyberataków na systemy informatyczne. Wzorowym i najbardziej efektywnym podejściem, byłoby wyrobienie u słuchaczy umiejętności myślenia „jak cyberprzestępca". Chodzi o to, by zawsze być o krok do przodu i działać według schematu proaktywnego, próbującego wyprzedzić zagrożenia.

REKOMENDACJE STUDENTÓW KIERUNKÓW MEDYCZNYCH

Ta domena, ma szczególny charakter. Potencjalne konsekwencje związane z cyberzagrożeniami, wykraczają tu poza straty finansowe czy naruszenie prywatności. Mówimy o życiu człowieka. Cyfryzacji sektora medycznego powinna bezpośrednio towarzyszyć edukacja techniczna, gwarantująca studentom zrozumienie postępu technologicznego w kontekście podejmowanego zawodu. Wszyscy studenci w ramach zajęć przedklinicznych powinni wziąć udział w szkoleniu z podstawowych zasad cyberbezpieczeństwa. 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. Warto byłoby zapoznać słuchaczy z narzędziami przydatnymi do tworzenia i bezpiecznego przechowywania haseł oraz podstaw odpowiedniego zabezpieczania kont osobistych.

REKOMENDACJE STUDENTÓW KIERUNKÓW PRAWNICZYCH

Mimo dynamicznie rosnącej roli technologii informacyjnych i ich oddziaływania na praktycznie każdą sferę życia, dydaktyka, w tym obszarze, na studiach prawniczych odgrywa wciąż marginalną rolę. Prawnicy, niezależnie od specjalizacji, powinni zdawać sobie sprawę z wpływu technologii informacyjnych na ich praktykę. To warunek konieczny do podnoszenia świadomości o możliwościach i zagrożeniach tworzonych przez informatyzację środowiska pracy. To też warunek konieczny dla zrozumienia i poruszania się w materii cyberbezpieczeństwa. W analizowanych programach studiów, brak jest obligatoryjnych przedmiotów dotyczących cyberbezpieczeństwa, w tym przeciwdziałania, wykrywania i zwalczania przestępczości komputerowej. Tematyka, jeśli jest omawiania, traktowana jest pobieżnie. Zwiększenie wiedzy o przestępczości w sieci, np. na przedmiocie Prawo Karne byłoby aktualnym odniesieniem do rzeczywistych wyzwań współczesnego świata. Dzisiejsza struktura przestępczości różni się względem tej, która dominowała, gdy uchwalano funkcjonujący Kodeks Karny w 1997 roku. Obecnie coraz więcej przestępstw popełnianych jest z wykorzystaniem technologii.

Projekt stwarza studentom możliwość dyskusji z przedstawicielami uczelni, w temacie kształtowania polityki programowej, uwzględniającej proces proaktywnego zarządzania transformacją cyfrową.

Przedstawione rekomendacje stanowią przedmiot rozmów z samorządami studenckimi, w ramach kampanii uświadamiającej wagę procesu transformacji cyfrowej we wzmacnianiu konkurencyjności programów nauczania.

Dokument wpisany jest w dyskurs dotyczący modelowania edukacji o cyberbezpieczeństwie w ujęciu lokalnym i międzynarodowym. Swoje opinie na temat wagi edukacji o cybrebezpieczeństwie w 21 wieku przekazało ponad 30 polskich i zagranicznych ekspertów, naukowców i dyplomatów.

To 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.

Geneza projektu

Powstał z potencjału stworzonego przez turniej **CyberSecurity Challenge PL2020**, zrealizowanego z patronatem Ministerstwa Cyfryzacji. 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, dotykającego różnych obszarów funkcjonowana państwa. To innowacyjne ćwiczenie, zgromadziło 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 - agory dla młodych liderów/liderek zainteresowanych domeną cyberbezpieczeństwa w kontekście studiowanej domeny. Raport jest pierwszym projektem wypracowanym przez wojewódzkie Cyber Laby. Współtwórcy dokumentu wywodzą się z grona uczestników turnieju, kół naukowych zajmujących się cyberbezpieczeństwem i z rekomendacji wykładowców akademickich.

Raport w wersji polskiej LINK

Kontakt:

lubelskie.cyberlab@gmail.com

kamilchmura@onet.pl