DZIAŁALNOŚĆ W ZAKRESIE CYBERBEZPIECZEŃSTWA. ASPEKTY PRAWNE, ORGANIZACYJNE I TECHNICZNE

Kształcenie informatyków w zakresie cyberbezpieczeństwa.

Nowe wyzwania związane z pandemią

Jerzy Cytowski, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

Edukacja w erze cyfrowej

Epidemia koronawirusa spowodowała, że systemy edukacji musiały nagle i szybko przestawić się na zdalne formy nauczania. Komisja Europejska opracowuje nowy plan działania w dziedzinie edukacji cyfrowej, który utoruje drogę do prawdziwie integracyjnej i wysokiej jakości edukacji online w Europie

Postępy w zastosowaniu technologii w edukacji są powolne we wszystkich państwach członkowskich Unii Europejskiej. Utrzymują się rozbieżności, jeśli chodzi o dostępność infrastruktury cyfrowej i sprzętu oraz umiejętności cyfrowe.

18 czerwca 2020 r. rozpoczęły się otwarte konsultacje publiczne w sprawie nowego planu.

Potrwają one do 4 września 2020 r.

Plan dotyczący wysokiej jakości cyfrowego kształcenia i szkolenia, sprzyjającego włączeniu społecznemu

Priorytet 1: Lepsze wykorzystanie technologii cyfrowej w nauczaniu i uczeniu się

- Działanie 1 – Podłączanie szkół do sieci
- Działanie 2 – Narzędzie samooceny SELFIE i program mentoringu dla szkół
- Działanie 3 – Kwalifikacje podpisane cyfrowo

Priorytet 2: Rozwijanie kompetencji i umiejętności cyfrowych

- Działanie 4 – Platforma (hub) dla szkolnictwa wyższego
- Działanie 5 – Umiejętności w ramach otwartej nauki
- Działanie 6 – Europejski Tydzień Kodowania w szkołach
- Działanie 7 – Cyberbezpieczeństwo w edukacji
- Działanie 8 – Szkolenia w zakresie umiejętności cyfrowych i przedsiębiorczości dla dziewcząt

Priorytet 3: Poprawa kształcenia dzięki lepszej analizie danych i prognozowaniu

- Działanie 9 – Badania na temat technologii ICT w edukacji
- Działanie 10 – Sztuczna inteligencja i analityka
- Działanie 11 – Prognoza strategiczna

Początek pandemii koronawirusa w Polsce na początku marca zmusił szkoły i uczelnie w kraju, gotowe lub nie, do przyjęcia modelu uczenia się w pełni online.

Gdy budynki były zamykane, aby spowolnić rozprzestrzenianie się choroby, administratorzy musieli stawić czoła szeregowi pytań:

Jak szybko wprowadzić uczenie zdalne, jak robić to skutecznie?

Co z uczniami i studentami, którzy nie mają dostępu do Internetu w domu?

Jak należy zorganizować zadania, aby odciążyć rodziny, gdzie dorośli często pracują teraz w domu?

W jaki sposób zapewnić uczniom, studentom i wrażliwym informacjom bezpieczeństwo w całkowicie zdalnym środowisku nauczania?

Jakie ryzyko może być większe w przypadku zdalnego uczenia się?
Być może największym problemem w tak dramatycznym i szybkim przejściu na całkowicie nowy model uczenia się jest potencjalne zastosowanie technologii, która nie została w pełni zweryfikowana i w przypadku której nauczyciele i uczniowie nie byli w pełni przygotowani do jej zastosowania.

Często wykorzystywane były aplikacje konsumenckie i narzędzia, które nie były zaprojektowane do celów edukacyjnych, może to komplikować obawy o bezpieczeństwo.

Głównym kryterium kwalifikacji technologii jest możliwość darmowego korzystania
Bezpłatne narzędzia i usługi online to potencjalnie

- nękanie nieodpowiednimi reklamami i śledzeniem użytkowników,
- niewystarczająca kontrola prywatności,
- złośliwe oprogramowanie.

Uczniowie, studenci lub nauczyciele mogą używać osobistych urządzeń domowych, które najczęściej są niezabezpieczone, stwarzając ryzyko wprowadzenia intruzów do sieci i systemów edukacyjnych.

Kształcenie informatyków, zapotrzebowanie, programy, potrzeby

ZAPOTRZEBOWANIE

Programy uczelni powinny uwzględnić zapotrzebowanie na usługi specjalistów. Najsilniej sygnalizowane są potrzeby zatrudnienia specjalistów cyberbezpieczeństwa w obszarze usług finansowych. Jednak ostatnie miesiące zwiększyły zapotrzebowanie na zatrudnienie specjalistów cyberbezpieczeństwa w innych instytucjach publicznych, również edukacyjnych.

Coraz częściej sygnalizowane jest zapotrzebowanie na zatrudnianie zespołów ekspertów z wielu dziedzin, pracujących wspólnie nad konceptualizacją, projektowaniem, produkcją, programowaniem, konfigurowaniem, ochroną i wdrażaniem każdego elementu technologii informatycznej.

PROGRAMY

Większość uczelni w Polsce kształci studentów kierunków informatycznych łącząc inżynierię oprogramowania i inżynierię systemów. Niektóre uczelnie dzielą te dziedziny na dwa różne programy.

W obydwu przypadkach nauczanie na większości uczelni skupia się na informatyce tworzenia aplikacji i sieciach komputerowych. W przeszłości bezpieczeństwo prawie nie było brane pod uwagę.

W ciągu ostatnich pięciu lat, większość uczelni włączyło kilka wykładów z zakresu bezpieczeństwa do swoich programów.

Niektóre polskie uczelnie, głównie techniczne (AGH, Politechniki, WAT), wprowadziły studia z zakresu cyberbezpieczeństwa (pierwszego i drugiego stopnia).

Wiele uczelni stara się aktualizować programy akademickie ze względu na aktualne wymagania i standardy.

PROGRAMY

Na Uniwersytecie Kardynała Stefana Wyszyńskiego prowadzone są interdyscyplinarne studia

Człowiek w cyberprzestrzeni

Ich absolwent ma podstawową wiedzę, umiejętności oraz unikatowe kompetencje interdyscyplinarne w dwóch obszarach - naukach społecznych i naukach ścisłych, a w szczególności w zakresie prawa, informatyki, socjologii oraz biznesu.

Na polskich uczelniach stosunkowo nieliczna jest oferta praktycznych podyplomowych studiów z zakresu cyberbezpieczeństawa – interdyscyplinarnych, kształcących współdziałanie zespołów informatyków, prawników i specjalistów z zakresu finansów i bądź administracji.

CERTYFIKATY

Uczelnie oferują wsparcie dla studentów w zakresie zdobywania certyfikatów

Cisco (najwięcej certyfikatów z cyberbezpieczeństwa), Microsoft, IBM i inne

Opinie środowiska akademickiego na temat certyfikatów zawodowych nie zawsze są entuzjastyczne, niektórzy twierdzą, że takie wsparcie nie jest zgodne z duchem akademickości (choć nie szkodzi). Dominująca jednak jest opinia, że certyfikacja sprzyja uczeniu się profesorów i studentów.

Komunikat Europejskiego Instytutu Certyfikacji Informatycznej w Brukseli w odpowiedzi na pandemię COVID-19

Rozszerzenie subsydiowanego przez EITCI programu dostępu do Europejskiej Certyfikacji Informatycznej w redukcji od 80% do 95% opłat dla certyfikatów Akademii EITCA w celu zwiększenia upowszechniania poświadczeń kompetencji cyfrowych wspomagających efektywność pracy zdalnej. coronavirus.eitci.org.

POTRZEBY

W związku z szybkim rozwojem technologii i popularnością wśród dzieci mediów społecznościowych, bardzo ważne stało się wprowadzenie edukacji w zakresie cyberbezpieczeństwa na każdym poziomie. Oprócz ataków na zasoby, dzieci narażone są na nękanie, wykorzystywanie i inne przestępstwa.

W krajach czołówki w walce o cyberbezpieczeństwo - USA, Kanadzie, Wielkiej Brytanii, Australii edukacja w zakresie cyberbezpieczeństwa obecna jest na każdym etapie nauczania.

Dodatkowo w USA edukacja w zakresie cyberbezpieczeństwa ma silne powiązania z wojskiem i agencjami ochrony.

Istnieje więc konieczność tworzenia programów kształcenia nauczycieli informatyki na wszystkich szczeblach edukacji w zakresie cyberbezpieczeństwa. W polskim systemie edukacyjnym oznacza to potrzebę kształcenia wszystkich nauczycieli przedmiotów ścisłych w zakresie nauczania o cyberbezpieczeństwie.

Dziękuję za uwagę