Załącznik nr 1

z dnia 15/10/2022 do uchwały nr 65/2022 Rady Dydaktycznej dla kierunków

Bezpieczeństwo wewnętrzne, Europeistyka – integracja europejska,

Organizowanie rynku pracy, Politologia, Polityka społeczna, Stosunki międzynarodowe,

Studia euroazjatyckie

OPIS KONCEPCJI KSZTAŁCENIA

NA KIERUNKU: CYBERBEZPIECZEŃSTWO

PODSTAWOWE DANE O PROJEKTOWANYM KIERUNKU STUDIÓW

1. POZIOM KSZTAŁCENIA:

………………………………………………studia drugiego stopnia……………………………….………..…..…

(studia pierwszego stopnia, studia drugiego stopnia, jednolite studia magisterskie)

2. PROFIL KSZTAŁCENIA:

……………………………………..……...profil ogólnoakademicki ………….….…………..……………………...

(ogólnoakademicki, praktyczny)

3. FORMA STUDIÓW:

…………………………………………….……studia stacjonarne……………………..………………….………...

(studia stacjonarne, studia niestacjonarne wieczorowe, studia niestacjonarne zaoczne)

4. WNIOSKODAWCA

Rada Dydaktyczna dla kierunków Bezpieczeństwo wewnętrzne, Europeistyka – integracja europejska, Organizowanie rynku pracy, Politologia, Polityka społeczna, Stosunki międzynarodowe, Studia euroazjatyckie

……………………………………………………………..………………..……………………

(rada dydaktyczna lub grupa co najmniej 15 nauczycieli akademickich zatrudnionych na Uniwersytecie jako podstawowym miejscu pracy)

5. PLANOWANY TERMIN URUCHOMIENIA STUDIÓW:

………………………………………………I semestr, rok 2023/2024………….………..………………………….

(proszę wskazać semestr i rok akademicki)

6. PLANOWANA MINIMALNA LICZBA STUDENTÓW NA PIERWSZYM ROKU STUDIÓW:………………………………………….…...18 osób……………………………………………………..

7. PLANOWANA MAKSYMALNA LICZBA STUDENTÓW NA PIERWSZYM ROKU

STUDIÓW : …………………………………………..…30 osób ……………………………………………………

8. PROPONOWANA JEDNOSTKA DYDAKTYCZNA, KTÓRA MA ORGANIZOWAĆ KSZTAŁCENIE NA PROJEKTOWANYM KIERUNKU STUDIÓW:

Wydział Nauk Politycznych i Studiów Międzynarodowych (WNPiSM)……….……………………………..

(proszę podać nazwę istniejącej lub projektowanej jednostki dydaktycznej)

9. CZY PROJEKTOWANY KIERUNEK STUDIÓW PRZYGOTOWUJE DO WYKONYWANIA ZAWODU NAUCZYCIELA I UZYSKANIA UPRAWNIEŃ ZAWODOWYCH?

…………nie………………………………………………………………………………………………………………

KONCEPCJA KSZTAŁCENIA

1. Dyscypliny, do których projektowany kierunek studiów zostanie przyporządkowany.

nauki o bezpieczeństwie – 60%

nauki o polityce i administracji – 20%

informatyka – 20%

2. Kluczowe dla koncepcji kształcenia na projektowanym kierunku studiów osiągnięcia naukowe UW w dyscyplinach, do których kierunek ten zostanie przyporządkowany.

WNPiSM jest jednostką UW prowadzącą badania naukowe w dyscyplinach: „nauki o bezpieczeństwie” oraz „nauki o polityce i administracji”. Wydział skupia około 190 pracowników naukowych, którzy są zaangażowani w ponad 20 grantów badawczych . Wydział jest jedną z największych jednostek dydaktyczno-badawczych w Europie Środkowej i ma podpisanych 250 umów z ośrodkami uniwersyteckimi poza granicami kraju .

W bazie wiedzy WNPiSM znajduje się wykaz 456 publikacji z nauk o bezpieczeństwie oraz 2257 z dyscypliny – „nauki o polityce i administracji” pracowników naukowych WNPiSM .

Wydział prowadzi badania w zakresie bezpieczeństwa wewnętrznego i międzynarodowego, w tym badania w zakresie: systemów bezpieczeństwa wewnętrznego, stanów nadzwyczajnych, zagrożenia hybrydowego i cyberbezpieczeństwa oraz procesów, zjawisk, relacji i wydarzeń międzynarodowego środowiska bezpieczeństwa. Zgodnie z Uchwałą Nr 21/2022 Komisji Ewaluacji Nauki dyscyplina „nauki o bezpieczeństwie” uzyskała kategorię naukową A+, która wskazuje na bardzo wysoki poziom badań w tej dyscyplinie, natomiast dyscyplina „nauki o polityce i administracji” kategorię naukową B+.

W 2020 r. Rada naukowa dyscypliny Nauki o Polityce i Administracji oraz Nauki o Bezpieczeństwie nadała 32 stopnie naukowe - 12 doktoratów i 20 habilitacji. Na WNPiSM w 2020 r. uzyskano jedną profesurę . Natomiast w 2021 roku nadała 13 doktoratów.

W dyscyplinie informatyka UW prowadzi kluczowe dla koncepcji kształcenia badania w zakresie: baz danych (w tym zasobów Big Data), inżynierii oprogramowania, kryptografii, sztucznej inteligencji oraz technologii informacyjnych, w tym m.in. polityki i administracji bezpieczeństwa, bezpieczeństwa IT . Zgodnie z Uchwałą Nr 21/2022 Komisji Ewaluacji Nauki dyscyplina ta uzyskała kategorię naukową A, która wskazuje na wysoki poziom badań w tej dyscyplinie.

Wykaz realizowanych grantów badawczych UW obejmujących ww. zagadnienia dostępny jest na stronie Wydziału Matematyki, Informatyki i Mechaniki .

3. Związek koncepcji i celów kształcenia na projektowanym kierunku studiów ze strategią UW w obszarze studiów.

Planowany kierunek studiów II stopnia jest zgodny z generalnymi założeniami strategii UW, czyli czynnikami, które stanowią o sile i prestiżu uczelni.

Nauczyciele akademiccy przewidywani do kształcenia na nowo tworzonym kierunku tworzą silny zespół, który oprócz licznych osiągnięć naukowych i dydaktycznych posiada duże doświadczenie w realizacji projektów B+R.

Zarys programu studiów opracowany został po szczegółowej analizie takich samych lub podobnych kierunków studiów prowadzonych na innych uczelniach krajowych i zagranicznych. W ramach wymiany doświadczeń zaplanowano również wizytę studyjną na dwóch uniwersytetach: Masarykova Univerzita i Univerzita Obrany w Brnie . Celem wizyty jest zapoznanie się z aspektami funkcjonowania studiów z zakresu cyberbezpieczeństwa takimi jak: działalność naukowo-badawcza, realizowane projekty, współpraca z otoczeniem gospodarczym oraz opracowanie katalogu metod wykorzystywanych do nauczania przedmiotów. Wizyta służyła będzie integracji środowiska akademickiego przez nawiązanie wzajemnej współpracy dotyczącej wymiany doświadczeń naukowych, udziału we wspólnych konferencjach naukowych.

Zadaniem projektowanego kierunku jest kształcenie absolwentów liczących się na rynku pracy. Projektowany program jest odpowiedzią na zapotrzebowanie społeczne i gospodarcze. Gwałtowny w ostatnich latach wzrost popularności pracy zdalnej i hybrydowej spowodował wzrost zapotrzebowania firm i organizacji na specjalistów znających zasady polityki cyberbezpieczeństwa i sposoby jej kształtowania, mających wiedzę z zakresu stosowania mechanizmów, technologii i systemów zabezpieczeń przed cyberzagrożeniami. Praca zdalna obnażyła niedostateczny poziom bezpieczeństwa w wielu firmach i spowodowała konieczność edukowania rynku, uświadamiania o problemach związanych z zagrożeniami w obszarze IT i zwiększania poziomu świadomości wśród kadry managerskiej i specjalistów. Relatywnie niska świadomość rynkowa dotycząca konieczności stosowania rozwiązań z zakresu cyberbezpieczeństwa połączona ze wzrostem zapotrzebowania na pracę zdalną i rozwiązania chmurowe oraz szybki wzrost rynku IoT, wymusiły konieczność zwiększania świadomości o bezpieczeństwie danych. Przeciętny obywatel nie wie, w jaki sposób chronić swoje dane i prywatność w sieci, często nie jest świadom utraty danych, bądź tego, że stał się ofiarą ataku. Edukacja oraz zwiększanie świadomości zarówno o zagrożeniach jak i rozwiązaniach zabezpieczających jest sposobem ochrony przed cyberprzestępcami .

W trakcie projektowania programu studiów II stopnia, a także podczas realizacji toku studiów zostaną wykorzystane wzorce międzynarodowe oraz własne doświadczenia. Podstawą sposobu sformułowania efektów uczenia się oraz doboru metod nauczania będzie ich projektowanie zgodnie z Europejskimi Ramami Kwalifikacji (ERK), zapewniającymi porównywanie poziomów kwalifikacji w różnych systemach edukacyjnych. Taki system pracy pomoże między innymi w możliwościach realizacji nowych wizji prowadzenia procesu dydaktycznego bazującego na teorii i praktyce w zakresie cyberbezpieczeństwa. Pomoże także w modularyzacji oraz możliwości racjonalnego wykorzystania Europejskiego Systemu Transferu Punktów (ECTS). Przy określaniu zakładanego poziomu wiedzy i umiejętności przypisanych poszczególnym kwalifikacjom, zostaną wykorzystane sposoby podziałów programu studiów na kategorie odnoszące się do postanowień europejskich występujących w deskryptorach dublińskich (Dublin Descriptors). Deskryptory te bazują na pięciu aspektach kształcenia, są to: wiedza i rozumienie; wykorzystanie w praktyce wiedzy i rozumienia; ocena i formułowanie sądów; umiejętności komunikacji; umiejętności uczenia się. Modularyzacja (stworzenie modułów, w skład których wejdą różne treści i formy kształcenia), pomoże między innymi w pogłębieniu efektywności studiów. To z kolei pozwoli na akumulację i transfer osiągnięć studentów, pogłębienie ich wiedzy (określonych w kategoriach efektów kształcenia), ale także większą indywidualizację programów studiów.

Zdobyta przez studentów wiedza i umiejętności pozwolą także w przyszłości na wykorzystanie ich kompetencji na użytek społeczno-gospodarczy oraz generowanie nowych zapotrzebowań w informacyjnej sferze nauki, edukacji i biznesu. Począwszy od potrzeb małych społeczności i przedsiębiorstw (diagnozowanie trendów rozwoju w danej dziedzinie czy obszarze gospodarki, nauki, kultury, edukacji), skończywszy na wyzwaniach organizacyjnych i zarządczych stojących przed poszczególnymi sektorami gospodarki, ale także określeniu kierunków rozwoju nauki i technologii, a więc także potencjału sektora B+R+I. Jako ważną część procesu dydaktycznego przewiduje się kształtowanie umiejętności samodoskonalenia zawodowego.

Planowane studia będą cyklicznie weryfikowane na podstawie przeprowadzanych okresowych analiz i ocen dotyczących rynkowego zapotrzebowania na specjalistów z zakresu cyberbezpieczeństwa. Istotne w tym względzie będą także, zgłaszane w trakcie całego procesu edukacyjnego, potrzeby samych słuchaczy. W trakcie prowadzenia poszczególnych zajęć wykorzystane zostaną dotychczasowe doświadczenia pracowników naukowych UW oraz współpracujących z nimi specjalistów spoza uniwersytetu (instytucji państwowych oraz przedsiębiorstw).

4. Główne założenia programu studiów II stopnia.

Program studiów zakłada kształcenie absolwentów w oparciu o dwa poniższe filary:

I filar – wiedza z zakresu kształtowania i stosowania polityki cyberbezpieczeństwa na poziomie firm, organizacji, instytucji państwowych i europejskich

II filar – wybrane obszary IT istotne w tworzeniu polityki cyberbezpieczeństwa

I filar programowy obejmuje następujące zagadnienia:

 rozpoznawanie potrzeb oraz kształtowanie polityki i strategii cyberbezpieczeństwa na poziomie firm, organizacji, instytucji państwowych i europejskich,

 sposoby tworzenia zasad kontrolnych i ochronnych dla zasobów technologicznych i informacyjnych przedsiębiorstw,

 rozwiązania z zakresu cyberbezpieczeństwa funkcjonujące na szczeblu państwowym,

 zasady polityki UE mające na celu zwiększenie cyberodporności, walkę z cyberprzestępczością, wzmocnienie cyberdyplomacji i cyberobrony,

 prawo karne i ochrona cyberprzestrzeni,

 zarządzanie ryzykiem i ocena bezpieczeństwa systemów IT,

 ochrona prywatności w Internecie,

 społeczna percepcja zagrożeń,

 dezinformacja oraz narzędzia i techniki manipulowania opinią publiczną.

Powyższe zagadnienia obejmują tworzenie i kształtowanie polityki bezpieczeństwa w następujących obszarach:

 bezpieczeństwo systemów informatycznych,

 zabezpieczenia systemów operacyjnych,

 bezpieczeństwo komunikacji sieciowej i elektronicznej,

 technologie i zabezpieczenia internetowe,

 bezpieczeństwo pracy w chmurze,

 bezpieczeństwo IoT.

II filar to wybrane zagadnienia dotyczące obszarów IT, które wspierają operacje cyberbezpieczeństwa i których poznanie jest konieczne do realizacji zagadnień z I filaru, takie jak:

 sztuczna inteligencja,

 Big Data i analiza danych,

 technologie budowy serwisów i portali internetowych,

 podstawy programowania w cyberprzestrzeni,

 web 2.0 i media społecznościowe

Cyberbezpieczeństwo jest obszarem, którego znaczenie stale rośnie. Na świecie obserwuje się wzrost zainteresowania tematyką związaną z bezpieczeństwem IT. Trendy wzrostu popularności wyszukiwania słów: „cybersecurity”, „security IT”, „cyber attacks” w wyszukiwarce Google w ciągu ostatnich pięciu lat przedstawia Wykres 1. Wzrost znaczenia bezpieczeństwa informatycznego, powoduje wzrost zapotrzebowania na specjalistów security IT.

Wykres 1. Trendy popularności wyszukiwania: cybersecurity, security IT, cyber attacks

Źródło: GTrends, https://trends.google.pl, dostęp [2022-04-29]

Program studiów jest odpowiedzią na rosnące wciąż zapotrzebowanie na wykwalifikowanych pracowników zajmujących się bezpieczeństwem IT. Główne założenia programu skierowane są na rozpoznawanie potrzeb organizacji w zakresie bezpieczeństwa IT, kształtowanie polityki cyberbezpieczeństwa na poziomie państwowym oraz zarządzanie bezpieczeństwem informacyjnym UE.

W systemie cyberbezpieczeństwa najsłabszym ogniwem wciąż pozostaje człowiek, dlatego tak ważną kwestią jest cyberedukacja. Najbardziej zaawansowane technologie z zakresu bezpieczeństwa IT mogą okazać się nieskuteczne w przypadku braku wystarczającej wiedzy użytkowników w zakresie bezpiecznego korzystania z narzędzi informatycznych i rozwiązań sieciowych.

Program ukierunkowany jest na rozwój kompetencji w zakresie podnoszenia poziomu świadomości występowania cyberzagrożeń i możliwości zapobiegania ich gospodarczym, społecznym, psychologicznym i politycznym konsekwencjom. Umożliwia zdobycie wiedzy z zakresu szerokiego spektrum rozwiązań technologicznych security IT, niezbędnej do definiowania zagrożeń w cyberprzestrzeni i stosowania środków zapobiegawczych.

Studenci nauczą się diagnozować i analizować zagrożenia związane z cyberbezpieczeństwem, a także stosować narzędzia służące do ich ograniczania i eliminacji. Kształtowanie umiejętności zawodowych będzie miało na celu sprostanie stale zmieniającym się wymaganiom dzisiejszego cyfrowego świata.

Zagadnienia programowe będą realizowane przy użyciu tradycyjnych metod dydaktycznych, takich jak: wykłady problemowe, konwersatoria, ćwiczenia. Zastosowane zostaną również metody oparte na dyskusji, angażujące studentów w wymianę poglądów, wymagające wewnętrznej aktywności oraz zachęcające do zajęcia własnego stanowiska (metoda sytuacyjna, giełda pomysłów, SWOT czy dyskusja panelowa, okrągłego stołu lub seminaryjna). Istotnym narzędziem będzie również zespołowe, pod kierunkiem prowadzącego zajęcia, analizowanie i rozwiązywanie konkretnych oraz rzeczywistych problemów, z którymi studenci mogą się spotkać w przyszłej działalności projektowej lub pracy zawodowej. Ważną częścią procesu dydaktycznego będzie również kształtowanie umiejętności samodoskonalenia zawodowego.

5. Kompetencje wymagane od kandydatów na studia.

Oferta studiów II stopnia skierowana będzie do wszystkich studentów, którzy posiadają minimum tytuł zawodowy licencjata. O przyjęcie na studia będą mogły ubiegać się osoby, które uzyskały dyplom licencjata, magistra, inżyniera lub równoważny na dowolnym kierunku studiów.

Planowany proces kwalifikacji obejmuje dwa etapy:

 punkty ze ocenę na dyplomie (z wagą 30%),

 punkty za egzamin pisemny – test wielokrotnego wyboru (z wagą 70%).

Zagadnienia egzaminacyjne wraz z wykazem literatury zostaną udostępnione kandydatom przed egzaminem. Obejmowały będą wiedzę informatyczną zdobytą przez kandydatów w szkole podstawowej i średniej oraz na studiach I stopnia w zakresie ogólnie pojmowanej technologii informacyjnej, która zawarta jest w wielu programach różnego typu studiów przyporządkowanych do różnych dyscyplin.

Kandydatów z dyplomem zagranicznym będą obowiązywały takie same zasady, jak kandydatów z dyplomem uzyskanym w Polsce. Dodatkowo, kandydaci z dyplomem uzyskanym za granicą, którzy nie będą posiadali honorowanego przez UW dokumentu poświadczającego znajomość języka polskiego, w trakcie egzaminu będą podlegali sprawdzeniu znajomości języka polskiego na poziomie B2.

6. Sylwetka absolwenta.

Absolwenci będą wyróżniać się wiedzą w zakresie planowania i wdrażania prewencyjnych środków cyberbezpieczeństwa w celu ochrony przed cyberatakami. Będą znać zasady i regulacje kształtowania polityki i strategii cyberbezpieczeństwa na poziomie firmy, kraju i EU. Będą posiadać umiejętności identyfikowania obszarów występowania cyberzagrożeń i doboru metod przeciwdziałania ich występowaniu.

Ważną kwestią będzie rozpoznawanie potrzeb organizacji w zakresie bezpieczeństwa IT, formułowanie, aktualizowanie i stosowanie rozwiązań organizacyjnych i technologicznych służących podnoszeniu poziomu zabezpieczeń.

W aspekcie społecznym, ważnym elementem będzie propagowanie zrozumienia występowania i oceny zagrożeń cyberbezpieczeństwa oraz kształtowanie i uświadamianie potrzeby ograniczania ryzyka ich występowania.

Absolwenci studiów będą posiadać wiedzę w zakresie:

 funkcjonowania systemu cyberbezpieczeństwa na poziomie firmy i kraju oraz rozwiązań międzynarodowych w tym zakresie,

 oceny bezpieczeństwa systemów IT,

 podstaw prawnych ochrony informacji i systemów informatycznych,

 znaczenia sztucznej inteligencji w ograniczaniu ryzyka występowania cyberzagrożeń i ich zapobieganiu,

 bezpieczeństwa sieci komputerowych i komunikacji elektronicznej,

 wyzwań związanych z zapewnieniem bezpieczeństwa pracy systemów chmurowych,

 zagrożeń związanych z wdrażaniem nowych usług sieciowych, np. IoT.

Podczas trwania studiów studenci będą mogli kształtować następujące umiejętności w zakresie:

 analizowania sytuacji stwarzających ryzyko występowania cyberzagrożeń,

 diagnozowania zagrożeń w cyberprzestrzeni, na jakie są narażone są obecnie organizacje, państwa i ich obywatele,

 zarządzania ryzykiem i wdrażania strategii zapobiegawczych w celu zapewnienia bezpieczeństwa przedsiębiorstw,

 wykorzystywania narzędzi do przeciwdziałania zagrożeniom i destrukcyjnemu oddziaływaniu na informację i systemy informatyczne,

 ochrony systemów informatycznych zgodnie z aktualnymi aktami prawnymi oraz normami międzynarodowymi,

 współpracy w grupie i wspólnego rozwiązywania problemów,

 samodzielnego zdobywania wiedzy i kierowania rozwojem swoich umiejętności.

Kompetencje społeczne absolwentów będą dotyczyły następujących obszarów:

 propagowania i rozpowszechniania wiedzy dotyczącej możliwości występowania zagrożeń w cyberprzestrzeni,

 uświadamiania potrzeby ograniczania ryzyka zagrożeń,

 kształtowania odpowiedzialnych postaw dotyczących korzystania z cyberprzestrzeni,

 uznania znaczenia wiedzy w krytycznym odnoszeniu się do problemów bezpieczeństwa IT i w ich rozwiązywaniu w życiu społecznym i gospodarczym,

 konieczności uczenia się przez całe życie i ponoszenia swoich kwalifikacji wobec zmieniającego się otoczenia.

7. Uzasadnienie wyboru poziomu kształcenia, profilu studiów, proponowanych limitów przyjęć.

Jako profil dla nowego kierunku studiów wybrano profil ogólnoakademicki.

Zgodnie z art. 64 ustawy Prawo o szkolnictwie wyższym i nauce z dnia 20 lipca 2018, profil ogólnoakademicki studiów wymaga, aby ponad połowa punktów ECTS była przypisana zajęciom związanym z prowadzoną w uczelni działalnością naukową.

W projektowanym programie studiów ponad połowa punktów ECTS zostanie przyznana za przedmioty związane z zagadnieniami będącymi tematami badań naukowych pracowników Katedry Technologii Informacyjnych (KTI) oraz Katedry Bezpieczeństwa Wewnętrznego (KBW) WNPiSM.

Ważnym elementem programu będzie kształtowanie zdolności oraz umiejętności stosowania metodologii badawczych dających podstawy do prowadzenia własnych badań. Cel ten będzie realizowany w ramach obowiązkowych zajęć projektowych oraz w procesie dyplomowania. Studenci będą mieli możliwość korzystania z infrastruktury badawczej znajdującej się w zasobach KTI.

Wynikająca z ww. ustawy struktura zatrudnienia - co najmniej 75% godzin zajęć prowadzona będzie przez nauczycieli akademickich zatrudnionych na UW jako podstawowym miejscu pracy, umożliwi słuchaczom korzystanie z licznych doświadczeń wykładowców w zakresie prowadzenia działalności naukowej.

Studenci będą mieli możliwość realizacji własnych projektów i prowadzenia badań w zakresie cyberbezpieczeństwa przy wykorzystaniu potencjału informatycznego i doświadczenia projektowego pracowników KTI oraz Centrum Rafinacji Informacji (CRI) - spin-off UW, z którym ściśle współpracuje KTI . Wśród założycieli CRI są pracownicy KTI. Będą również mieli możliwość uczestnictwa w projektach B+R realizowanych w KTI.

W projektowanym programie studiów, większość treści programowych ukierunkowana jest na zdobycie wiedzy związanej z kształtowaniem polityki cyberbezpieczeństwa i występowaniem zagrożeń w cyberprzestrzeni. Uwzględniając szerokie spektrum obszarów występowania cyberzagrożeń, program ukierunkowany jest na poznanie mechanizmów i narzędzi służących do zmieszania ryzyka ich występowania.

Zakładane limity studentów na studiach II stopnia:

minimalna liczba studentów na pierwszym roku - 18 osób

maksymalna liczba studentów na pierwszym roku - 30 osób

Ww. limity zostały uzgodnione z władzami WNPiSM. Zostały dostosowane do planowanej infrastruktury IT służącej realizacji zajęć i projektów prowadzonych przez studentów.

8. Uzasadnienie utworzenia nowego kierunku studiów odnoszące się do dotychczasowej oferty studiów UW oraz doświadczeń innych uczelni krajowych i zagranicznych.

a) oferta edukacyjna UW kierunku studiów realizującego przedstawioną koncepcję kształcenia

Analizę oferty edukacyjnej UW wykonano na podstawie danych zawartych w systemie RAD-on . Uczelnia w swojej ofercie nie posiada kierunku, którego treści programowe byłyby poświęcone w całości cyberbezpieczeństwu. Wybrane zagadnienia z zakresu cyberbezpieczeństwa realizowane są jedynie w ramach pojedynczych przedmiotów wybranych kierunków takich jak np. Cyberbezpieczeństwo na Wydziale Prawa i Administracji lub Bezpieczeństwo zasobów cyfrowych, Bezpieczeństwo cybernetyczne i Warsztaty cyberbezpieczeństwa dla humanistów na WNPiSM.

W ofercie uczelni znajduje się płatny kurs Cybersecurity realizowany w ramach współpracy Wydziału Matematyki Informatyki i Mechaniki z wiodącym izraelskim instytutem szkoleniowym HackerU. W zależności od wyboru oferty programowej, kurs trwa maksymalnie 6 miesięcy i kończy się uzyskaniem certyfikatu ukończenia. Utworzenie i prowadzenie płatnego kursu z zakresu cyberbezpieczeństwa świadczy o dużym zapotrzebowaniu na specjalistów z tej dziedziny i chęci kształcenia się w tym zakresie.

Projektowany kierunek studiów stanowiłby unikalną ofertę uczelni, doskonale uzupełniającą ofertę programową i stwarzającą możliwość zdobycia wiedzy z zakresu cyberbezpieczeństwa dla wszystkich studentów, również dla tych, którzy nie mają możliwości wyboru płatnych studiów.

b) przykłady takich samych lub podobnych kierunków studiów prowadzonych na innych uczelniach krajowych i zagranicznych

Zgodnie z informacjami zawartymi w systemie RAD-on, studia II stopnia na kierunku cyberbezpieczeństwo oferują cztery polskie uczelnie (Tabela 1). Jedna z uczelni prowadzi zajęcia w języku angielskim, pozostałe w języku polskim. Profil kształcenia wszystkich oferowanych studiów to profil ogólnouniwersytecki.

Cyberbezpieczeństwo występuje również jako specjalność na innych uczelniach krajowych.

W celu opracowania nowego programu studiów dokonano przeglądu dostępnych na stronach uczelni zakresów nauczania i profili kandydatów dla kierunków zawartych w Tabeli 1. Szczególną uwagę zwrócono na kierunki, które zostały przyporządkowane do dyscyplin: nauki o bezpieczeństwie, nauki po polityce i administracji oraz informatyki. Treści zawarte w ofertach programowych zostały skonfrontowane z proponowanym programem studiów nowego kierunku.

Na uwagę zasługuje fakt, że znaczna część kierunków studiów z Tabeli 1 została uruchomiona w ostatnich czterech latach. Świadczy to o rosnącej potrzebie kształcenia specjalistów z zakresu cyberbezpieczeństwa.

Tabela 1. Wykaz uczelni wyższych w Polsce prowadzących studia II stopnia na kierunku związanym z cyberbezpieczeństwem

Lp Nazwa kierunku studiów Instytucja prowadząca Poziom Dyscypliny Data uruchomienia

1 Bezpieczeństwo informacyjne i cyberbezpieczeństwo Akademia Sztuki Wojennej II stopnia nauki o bezpieczeństwie (100%) 2021-10-01

2 Cyberbezpieczeństwo Politechnika Wrocławska II stopnia informatyka techniczna i telekomunikacja (100%) 2020-11-05

3 Kryptologia i cyberbezpieczeństwo Wojskowa Akademia Techniczna II stopnia informatyka techniczna i telekomunikacja (100%) 2018-03-01

4 It cyber security Uniwersytet Marii Curie-Skłodowskiej w Lublinie II stopnia nauki o polityce i administracji (55%), informatyka (45%) 2020-10-01

Źródło: https://radon.nauka.gov.pl, dostęp [2022-04-14]

Analizę uczelni zagranicznych oferujących studia II stopnia w zakresie cyberbezpieczeństwa przeprowadzono w oparciu o dane zawarte na międzynarodowej platformie Studyportals, skupiającej ponad 3750 instytucji edukacyjnych w 110 krajach. Platforma jest wspierana przez Komisję Europejską i inne krajowe instytucje szkolnictwa wyższego . W zasobach platformy, w dyscyplinie Cyber Security, zamieszczone są 553 oferty studiów II stopnia obejmujące zarówno studia ukierunkowane na zdobycie kompleksowej wiedzy z zakresu bezpieczeństwa, jak również studia skupiające się na konkretnych aspektach z zakresu cyberbezpieczeństwa lub łączące cyberbezpieczeństwo z innymi zagadnieniami np. zarządzanie cyberbezpieczeństwem, sieci komputerowe i cyberbezpieczeństwo.

Analiza dostępnych na platformie ofert programowych studiów II stopnia pozwoliła na sformułowanie głównych obszarów w zakresie cyberbezpieczeństwa:

 informacje w cyberprzestrzeni i bezpieczeństwo cyberprzestrzeni,

 bezpieczeństwo sieci komputerowych i pracy w chmurze,

 zarządzanie danymi i bazami danych, w tym zbiorami Big Data,

 komunikacja mobilna i programowanie,

 prawo i ochrona w cyberprzestrzeni,

 ochrona prywatności w Internecie,

 społeczeństwo informacyjne i socjologia cyberprzestrzeni,

 technologie i zabezpieczenia internetowe,

 podstawy internetu rzeczy – IoT,

 inżynieria oprogramowania,

 bezpieczeństwo systemów informatycznych,

 bezpieczeństwo komunikacji elektronicznej,

 metody badawcze i planowanie projektów,

 administracja systemów informatycznych,

 uczenie maszynowe i sztuczna inteligencja,

 kryptografia.

Szczegółowej analizie poddano programy nauczania uczelni, które zgodnie z informacją zawartą na stronach portalu, zostały uznane w 2021 r. za jedne z najlepszych szkół cyberbezpieczeństwa na świecie:

 Georgia Institute of Technology , USA,

 King's College Londyn , Wielka Brytania,

 Uniwersytet w Leiden , Holandia,

 ETH Zurych , Szwajcaria,

 Uniwersytet w Aalborgu , Dania,

 Uniwersytet Nowej Południowej Walii , Australia,

 Uniwersytet Jiao Tong w Szanghaju , Chiny .

Przeprowadzona analiza była punktem wyjścia do sformułowania nowego programu studiów II stopnia.

9. Uzasadnienie utworzenia nowego kierunku studiów odnoszące się do potrzeb otoczenia społeczno-gospodarczego i studentów.

a) opinia studentów na temat potrzeby uruchomienia projektowanego kierunku studiów II stopnia i koncepcji kształcenia na tym kierunku

W celu zbadania stopnia zainteresowania studentów nowo tworzonym kierunkiem studiów II stopnia, przeprowadzono ankietę wśród studentów studiów I stopnia . Prośby o wypełnienie ankiety zostały wysłane do wszystkich studentów studiów I stopnia WNPiSM UW (za pośrednictwem Biura promocji i komunikacji) oraz zostały skierowane do wybranych studentów studiów I stopnia UW przy wykorzystaniu służbowych i osobistych kontaktów pracowników UW zaangażowanych w przygotowanie niniejszego projektu.

W badaniu wzięło udział 335 osób, w tym 207 kobiet i 128 mężczyzn. Większość badanych osób (70%) to osoby mieszkające w miastach powyżej 500 tys. mieszkańców. Wszystkie badane osoby są studentami UW, a znaczna większość – 217 osób studiuje na WNPiSM, na którym planowane jest otwarcie nowego kierunku.

Wyniki ankiety jednoznacznie wskazują, że studenci postrzegają zawód specjalisty ds. cyberbezpieczeństwa jako atrakcyjny i przyszłościowy, aż 43,88% badanych osób chciałoby pracować w tym zawodzie (Wykres 2).

Wykres 2. Zainteresowanie studentów zawodem specjalisty ds. cyberbezpieczeństwa

Źródło: Badanie własne.

Średnie wynagrodzenie w branży cybersecurity to około 15 000 zł miesięcznie . 96,12% respondentów uznało je za atrakcyjne (Wykres 3).

Wykres 3. Atrakcyjność wynagrodzenia w branży cybersecurity

Źródło: Badanie własne.

Kluczowe pytanie ankiety miało na celu zbadanie zainteresowania i ewentualnego wyboru nowo utworzonego kierunku przez studentów. Aż 47,16% respondentów zdecydowałoby się na wybór kierunku Cyberbezpieczeństwo, gdyby ten znalazłby się w ofercie studiów II stopnia (Wykres 4). Na uwagę zasługuje również fakt, że 217 badanych osób to studenci studiów I stopnia WNPiSM, na którym nowy kierunek ma zostać utworzony.

Wykres 4. Wybór nowego kierunku Cyberbezpieczeństwo na studiach II stopnia

Źródło: Badanie własne.

Jedną z kluczowych kwestii przy projektowaniu nowego kierunku jest opracowanie programu studiów, który byłby atrakcyjny dla studentów i zapewniałby stałe zainteresowanie ofertą programową.

Zdaniem studentów, najważniejsze jest bezpieczeństwo danych, a następnie bezpieczeństwo ludzi i bezpieczeństwo społeczne (Wykres 5). W opinii ankietowanych (236 osób), program studiów powinien uwzględniać zagadnienia związane z nowymi technologiami - sztuczną inteligencją, uczeniem maszynowym, zagadnienia Big Data itp.

Wykres 5. Preferowane przez studentów treści programu nauczania

Źródło: Badanie własne.

Ostatnim elementem badania było ustalenie preferowanych przez studentów kanałów promocji kierunku, mające na celu dotarcie z informacją do jak największej liczby potencjalnych studentów nowego kierunku, w przypadku, gdy kierunek ten zostałby utworzony. Zdaniem studentów, najbardzej skutecznym kanałem promocji są media społecznościowe, następnie serwisy internetowe dla kandydatów na studia oraz strony internetowe uczelni (Wykres 7). Ważnym elementem promocji kierunku są również dni otwarte na uczelni. Pozostałe kanały promocji, w tym zwłaszcza media tradycyjne, zostały uznane przez stdentów jako mało skuteczne.

Wykres 7. Preferowane przez studentów kanały promocji nowego kierunku

Źródło: Badanie własne.

b) sposób przeprowadzenia badań lub rozeznania potrzeb/oczekiwań otoczenia społeczno-gospodarczego

W ramach przeprowadzenia rozeznania potrzeb/oczekiwań otoczenia społeczno-gospodarczego pozyskano rekomendacje następujących instytucji:

 Komendy Głównej Policji,

 Departamentu Spraw Obronnych, Zarządzania Kryzysowego i Bezpieczeństwa Ministerstwa Klimatu i Środowiska,

 NASK’u - Państwowego Instytutu Badawczego.

stanowiące załączniki do niniejszego opisu koncepcji kształcenia.

10. Informacja o infrastrukturze i potencjale kadrowym zapewniającym prawidłową realizację koncepcji i celów kształcenia.

a) osiągnięcia naukowe i doświadczenie zawodowe nauczycieli akademickich

Nauczyciele akademiccy UW przewidywani do kształcenia na projektowanym kierunku studiów:

 prof. dr hab. Stanisław Sulowski – WNPiSM UW

 prof. dr hab. Andrzej Misiuk – WNPiSM UW

 dr hab. inż. Wiesław Cetera, prof. Ucz. – WNPiSM UW

 dr hab. Grzegorz Gudzbeler, prof. UW – WNPiSM UW

 dr hab. Daniel Mider – WNPiSM UW

 dr hab. Bartosz Pieliński – WNPiSM UW

 dr Janusz Jabłonowski – MIM UW

 dr Szymon Nowakowski – MIM UW

 dr Kamil Mroczka – WNPiSM UW

 dr inż. Dariusz Jaruga – WNPiSM UW

 dr Piotr Potejko – WNPiSM UW

 dr inż. Bartłomiej Moszoro – WNPiSM UW

 dr Paweł Kuczma – WNPiSM UW

 dr Agnieszka Heba – WNPiSM UW

 dr Wioletta Matosek – WNPiSM UW

Do współpracy zaproszono również poniższych specjalistów:

 dr Paweł Majdan – MON, Departament Cyberbezpieczeństwa

 dr Paweł Ciszek - Wojska Obrony Cyberprzestrzeni

Wykaz osiągnięć naukowych i doświadczenia zawodowego nauczycieli akademickich UW przewidywanych do kształcenia na projektowanym kierunku studiów znajduje się w Załączniku – szczegółowe osiągnięcie naukowe i dydaktyczne kadry.

Wśród nauczycieli znajdują się pracownicy KTI oraz KBW WNPiSM prowadzący badania naukowe w dyscyplinach, do których został przyporządkowany projektowany kierunek.

b) Infrastruktura niezbędna do realizacji przedstawionej koncepcji kształcenia oraz wskazać jednostkę/jednostki, która/e ją zapewni/ą

Zajęcia w ramach nowego kierunku studiów będą prowadzone w budynkach należących do WNPiSM. Wydział posiada pracownię komputerową wyposażoną w 21 komputerów z systemem Windows 10 oraz pakietem Office 2016 i oprogramowaniem statystycznym SPSS. W pracowni jest możliwość bezprzewodowej transmisji obrazu dzięki, której te same treści mogą być prezentowane na wszystkich komputerach oraz na 65 ’calowym monitorze jednocześnie.

Wydział posiada sieć lokalną. We wszystkich budynkach uniwersyteckich dostępna jest bezpłatna sieć wifi Edurom. Sale wykładowe wyposażone są w komputery stacjonarne z dostępem do Internetu i infrastrukturę umożliwiającą podłączenie komputerów przenośnych. Obsługa studentów odbywa się poprzez system USOS administrowany centralnie. Wydział posiada licencję programu SPSS wykorzystywanego do badań statystycznych.

Infrastruktura informatyczna KTI WNPiSM, to obecnie park maszynowy składający się z:

 serwera, CPU: 16-Core Processor, Passmark 25471, MEM: 128GB, HDD: Dysk 0: 250G (SSD), Dysk 1: 1T (SSD M.2), Dysk 2: 2T (SSD M.2), Dysk 3: 8T (RAID 1 SATA), Dysk 4: 8T, Dysk 5: 8T, Dysk 6: 1T (SSD M.2), Dysk 7: 250G (SSD);Funkcja – serwery wirtualne

 serwera CPU: Intel(R) Core(TM) i5-7400 CPU @ 3.00GHz, Passmark: 7336 (4 core) RAM: 16GB, HDD: HDD1:7,3T, HDD2:298,1G, HDD3:7,3T; - serwera wirtualnego do dydaktyki;

a także z oprogramowania:

 baz danych relacyjnych i nierelacyjnych (dokumentowe, klucz-wartość, grafowe, rodziny kolumn),

 serwera brokera wiadomości,

 środowiska do tworzenia oprogramowania,

 oprogramowania do zarządzania Comarch ERP Optima (pracownicy KTI od lat współpracują z firmą w zakresie doskonalenia procesu dydaktycznego obejmującego narzędzia IT do zarządzania przedsiębiorstwem).

Dodatkową infrastrukturę IT na projektowanym kierunku zapewni współpraca z CRI, zajmującym się komercjalizacją wiedzy z zakresu rafinacji dużych zasobów danych (głównie nieustrukturyzowanych), które jest liderem konsorcjum (CTI-UW) realizującego projekt IKONA („Identyfikacja, KOlekcjonowanie i oceNA nieprzyjaznych operacji dezinformacyjnych w cyberprzestrzeni prowadzonych w oparciu o narzędzia teleinformatyczne”).

W ramach pierwszej fazy projektu IKONA planowany jest zakup 25-ciu komputerów do kwerend danych oraz trzech węzłów obliczeniowych AI. Zakupiona aparatura będzie mogła być wykorzystana do prowadzenia zajęć laboratoryjnych na nowo utworzonym kierunku studiów. Parametry komputerów będą umożliwiały przeprowadzanie takich operacji jak: obliczenia AI, klastrowanie AI – tworzenie modelu, wirtualizacja, np. budowa klastra obliczeniowego (własna chmura). Dodatkowo na potrzeby dydaktyki zostanie wykorzystany posiadany serwer wirtualny z systemem operacyjnym Linux, który zawierał będzie dedykowane do zajęć oprogramowanie. Każdy student będzie posiadał indywidualne konto na tym serwerze na czas trwania studiów.

Realizacja drugiego etapu projektu wymagała będzie zakupu sześciu serwerów - węzłów obliczeniowych oraz trzech serwerów do środowiska serwerów wirtualnych. Serwery te będą mogły być wykorzystywane przez studentów nowego kierunku do prowadzenia badań w ramach realizowanych projektów oraz do pisania prac dyplomowych.