**OPIS KONCEPCJI KSZTAŁCENIA**

**NA KIERUNKU ………………. BEZPIECZEŃSTWO CYBERNETYCZNE……………………**

(proszę podać proponowaną nazwę kierunku studiów)

**PODSTAWOWE DANE O PROJEKTOWANYM KIERUNKU STUDIÓW**

1. POZIOM KSZTAŁCENIA:

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

1. PROFIL KSZTAŁCENIA:

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

(ogólnoakademicki, praktyczny)

1. FORMA STUDIÓW:

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

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

1. 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)

1. PLANOWANY TERMIN URUCHOMIENIA STUDIÓW:

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

(proszę wskazać semestr i rok akademicki)

1. PLANOWANA MINIMALNA LICZBA STUDENTÓW NA PIERWSZYM ROKU STUDIÓW:………………………………………….…...18 osób……………………………………………………..
2. PLANOWANA MAKSYMALNA LICZBA STUDENTÓW NA PIERWSZYM ROKU

STUDIÓW : …………………………………………..…30 osoby ……………………………………………………

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

Wydział Nauk Politycznych i Studiów Międzynarodowych……………………….……………………………..

(proszę podać nazwę istniejącej lub projektowanej jednostki dydaktycznej)

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

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

**KONCEPCJA KSZTAŁCENIA**

1. Koncepcja i cele kształcenia, ich związek ze strategią uczelni oraz prowadzoną
w uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których projektowany kierunek studiów zostanie przyporządkowany ***– profil ogólnoakademicki***.
2. **dyscypliny, do których projektowany kierunek studiów zostanie przyporządkowany**

Projektowany kierunek studiów będzie przyporządkowany do następujących dyscyplin:

nauki o bezpieczeństwie – 60%

nauki o polityce i administracji – 20%

informatyka – 20%

1. **kluczowe dla koncepcji kształcenia na projektowanym kierunku studiów osiągnięcia naukowe Uniwersytetu Warszawskiego w dyscyplinach, do których kierunek ten zostanie przyporządkowany**

Jednostką UW prowadzącą badania naukowe w dyscyplinach: nauki o bezpieczeństwie i nauki o polityce i administracji jest WNPiSM. Wydział skupia około 190 pracowników naukowych, którzy są zaangażowani w ponad 20 grantów badawczych[[1]](#footnote-1). Zgodnie z informacją na stronie internetowej, wydział jest jedną z największych jednostek dydaktyczno-badawczych w Europie Środkowej i ma podpisanych 250 umów z ośrodkami uniwersyteckimi poza granicami kraju[[2]](#footnote-2).

W bazie wiedzy WNPiSM znajduje się wykaz 456 publikacji z nauk o bezpieczeństwie oraz 2257 z dyscypliny - nauki o polityce i administracji[[3]](#footnote-3).

**W zakresie nauk o bezpieczeństwie i nauk o polityce i administracji** Uniwersytet Warszawski w Katedrze Bezpieczeństwa Wewnętrznego prowadzi badania dotyczące bezpieczeństwa imprez masowych, badań nad terroryzmem i radykalizacją, bezpieczeństwa militarnego, bezpieczeństwa energetycznego i polityki energetycznej, ochrony infrastruktury krytycznej, studiów nad wywiadem, systemów bezpieczeństwa wewnętrznego, zarządzania kryzysowego, stanów nadzwyczajnych, zagrożenia hybrydowego i cyberbezpieczeństwa, dezinformacją oraz pozyskiwaniem informacji, bezpieczeństwem informacji w biznesie, ochroną informacji niejawnych, danych osobowych i  tajemnic prawnie chronionych, cyberprzestępczości i cyberterroryzmu, kryminalistyki. Natomiast w zakresie nauk o polityce i administracji prowadzone są badania dotyczące polityki zagranicznej i bezpieczeństwa Niemiec, relacji UE-Rosja i UE-Izrael, polityki energetycznej i  klimatycznej, dyplomacji ekonomicznej, polityki energetycznej, polityki transportowej, Unii Europejskej, integracji europejskiej, zarządzania wielopoziomowego (multi-level governance), polityki regionalnej, samorządu terytorialnego, administracji publicznej. Dodatkowo Katedra Technologii Informacyjnych prowadzi badania w zakresie polityki i administracji bezpieczeństwa, bezpieczeństwa IT,a także rafinacji informacji, tworzenia aplikacji badawczych do kolekcjonowania danych na potrzeby rafinacji.

**Wykaz realizowanych grantów badawczych znajduje się na stronach:**

<https://wnpism.uw.edu.pl/realizowane-granty/>

<https://wnpism.uw.edu.pl/o-wydziale/struktura-wydzialu/katedra-technologii-informacyjnych/>

**W dyscyplinie informatyka** Uniwersytet Warszawski prowadzi następujące badania kluczowe dla koncepcji kształcenia:

W zakresie baz danych dotyczące zarządzania bazami danych, języków opisu przepływu danych, big data processing, data science, języków zapytań, dedukcyjnych i semi-strukturalnych baz danych, baz danych wiedzy, relacyjnych i nierelacyjnych baz danych, języka SQL. W zakresie inżynierii oprogramowania dotyczące funkcyjnych i obiektowych języków programowania, programowanie w logice, systemów operacyjnych, systemów czasu rzeczywistego, metodologii rozwijania oprogramowania, formalnej dokumentacji i specyfikacji, weryfikacji oprogramowania, programowania w języku R. W zakresie kryptografii dotyczące naukowych aspektów kryptografii, ze szczególnym uwzględnieniem protokołów kryptograficznych, kryptografii odpornej na ataki fizyczne, oraz metod teorio-złożonościowych i teorio-liczbowych. W zakresie sztucznej inteligencji i systemów wieloagentowych dotyczące różnorodnych zagadnień sztucznej inteligencji, w szczególności uczenia maszynowego, eksploracji danych i sieci neuronowych a także przetwarzania języka naturalnego. Dodatkowo teoretycznych podstaw systemów wieloagentowych: różnych aspektów rozproszonego, kooperatywnego rozwiązywania problemów.

**Wykaz realizowanych grantów badawczych znajduje się na stronie:** <https://www.mimuw.edu.pl/granty>

1. **związek koncepcji i celów kształcenia na projektowanym kierunku studiów ze strategią Uniwersytetu Warszawskiego w obszarze studiów**

Kierunek studiów I stopnia Bezpieczeństwo cybernetyczne w pełni wpisuje się w misję UW, którego fundamentem działania jest jedność nauki i nauczania; zapewnienie dostępu do wiedzy i nabywania umiejętności wszystkim tym, którzy mają do tego prawo; kształtowanie elit Rzeczypospolitej, jak również synteza wartości uniwersalnych i lokalnych. Celem nadrzędnym tworzonego nowego kierunku studiów który wpisuje się w cele strategiczne w części odnoszącej się do kształcenia studentów jest zwiększenie potencjału rozwojowego uczelni poprzez rozszerzanie i wzbogacenie oferty edukacyjnej odpowiadająca potrzebom rynku pracy i innowacyjnej gospodarki oraz społeczeństwa obywatelskiego.

Projektowany kierunek jest przykładem interdyscyplinarnego podejścia do nowoczesnego kształcenia. Dominujące elementy programu kształcenia z zakresu obszaru bezpieczeństwa cybernetycznego zostaną uzupełnione elementami nauk społecznych. Takie połączenie pozwoli absolwentom wyjść naprzeciw złożonym problemom bezpieczeństwa cybernetycznego, a ich kształcenie do pełnienia funkcji specjalisty przyczyni się do wzmacniania bezpieczeństwa i potencjału gospodarczego kraju, co wpisuje się w cel strategiczny UW: wykształcenie absolwentów liczących się na rynku pracy. Cel strategiczny dotyczący organizacji badań naukowych i procesu nauczania zapewniający dużą mobilność studentów i kadry naukowej, a także aktywnej współpracy międzynarodowej w sferze badań naukowych i dydaktyki zapewniają osiągnięcia naukowe pracowników Katedry Technologii Informacyjnych (KTI) oraz Katedry Bezpieczeństwa Wewnętrznego (KBW) WNPiSM, a także współpraca z Centrum Rafinacji Informacji (spin-off UW), które jest liderem konsorcjum (CTI-UW) realizującego projekt IKONA *(Identyfikacja, KOlekcjonowanie i oceNA nieprzyjaznych operacji dezinformacyjnych w cyberprzestrzeni prowadzonych w oparciu o narzędzia teleinformatyczne).*

1. **główne założenia programu studiów (kluczowe zagadnienia, specyficzne dla kierunku metody dydaktyczne, zarys konstrukcji programu)**

Opracowano zarys programu, który stanowi rozszerzenie oferty programowej WNPiSM, zawierającej kierunek związany z bezpieczeństwem wewnętrznym i porządkiem publicznym w polityce organów władzy, o kwestie związane z bezpieczeństwem cybernetycznym. Główne założenia programu skierowane są na rozpoznawanie potrzeb organizacji w zakresie bezpieczeństwa IT, kształtowanie polityki bezpieczeństwa cybernetycznego na poziomie państwowym oraz zarządzanie bezpieczeństwem informacyjnym UE. W systemie bezpieczeństwa cybernetycznego 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 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. Ważnym elementem programu są również zagadnienia związane z dezinformacją oraz manipulowaniem opinią publiczną, regulacjami prawnymi w cyberprzestrzeni.

Powyższe treści znajdujące się w proponowanym programie studiów będą zgodne również z wytycznymi programowymi w zakresie poszczególnych przedmiotów znajdującymi się w raporcie **Cybersecurity Curricula 2017** grupy roboczej, składającej się z największych międzynarodowych stowarzyszeń komputerowych która je opracowała dla programów kształcenia na poziomie ponadlicealnym w zakresie cyberbezpieczeństwa[[4]](#footnote-4). Opublikowany raport jest zgodny z wymogami **Bazy Uczelni Wyższych ENISA**, a przedstawiony w nim program kształcenia w obszarze cyberbezpieczeństwa może posłużyć jako dobra praktyka lub też inspiracja dla polskich uczelni wyższych, pracujących nad własnymi programami w zakresie bezpieczeństwa cybernetycznego.

Bezpieczeństwo cybernetyczne staje się kluczowym obszarem bezpieczeństwa. Zainteresowanie tą tematyką w latach 1995-2020 wzrastało wykładniczo i kilkakrotnie przekroczyło uwagę poświęcaną bezpieczeństwu wojskowemu i międzynarodowemu (wykres 1).

**Wykres 1: Wzrost zainteresowania cyberbezpieczeństwem w latach 1995-2020**



Jednocześnie rynek pracy odczuwa brak specjalistów w tym zakresie i dyskontuje to poziomem wynagrodzeń („Cybersecurity – raport o rynku pracy w Polsce”):

Szereg raportów firmy TestArmy lub Gartnera wskazuje na braki specjalistów w tej dziedzinie.[[5]](#footnote-5)

Założenia programu są zbudowane na trzech filarach:

* obszary wiedzy związane z bezpieczeństwem cybernetycznym,
* zagadnienia przekrojowe - prawa, ekonomii, polityki, zarządzania ryzykiem, czy etyki,
* wiedza z zakresu IT - inżynierii komputerowej, informatyki, technologii informacyjnych.

Obszary wiedzy związane z bezpieczeństwem cybernetycznym:

* + bezpieczeństwo danych,
	+ bezpieczeństwo oprogramowania,
	+ bezpieczeństwo komponentów,
	+ bezpieczeństwo komunikacji sieciowej,
	+ bezpieczeństwo systemów,
	+ bezpieczeństwo ludzi,
	+ bezpieczeństwo organizacji (w tym gospodarczych),
	+ bezpieczeństwo społeczne.

Źródłem przewagi konkurencyjnej na rynku edukacyjnym proponowanych studiów I stopnia będzie:

* + uwzględnienie bezpieczeństwa cybernetycznego w aspekcie międzynarodowym,
	+ dezinformacja – jako obszar bezpieczeństwa państwa,
	+ praktyczny charakter studiów zapewni współpraca z Centrum Rafinacji Informacji (spin-off UW), które jest liderem konsorcjum (CTI-UW) realizującego projekt **IKONA** (*Identyfikacja, KOlekcjonowanie i oceNA nieprzyjaznych operacji dezinformacyjnych w cyberprzestrzeni prowadzonych w oparciu o narzędzia teleinformatyczne)*,
	+ praktyczny kontakt z technologiami i procedurami w zakresie ochrony przed zagrożeniami informacyjnymi w przestrzeni wirtualnej,
	+ współpraca z praktykami z CRI i innych podmiotów, którzy będą prowadzić przedmioty praktyczne typu case study i pokazać realizowane przez nich projekty związane z bezpieczeństwem cybernetycznym, a także proponować staże zawodowe,
	+ kadra dydaktyczna (pracownicy katedry technologii informacyjnych, katedry bezpieczeństwa wewnętrznego) posiadająca bogate doświadczenie dydaktyczne i naukowe w przygotowywaniu programów dydaktycznych 5 (nagrodzony w konkursie POWER – Zarządzanie Big Data) oraz projektów naukowych związanych z bezpieczeństwem cybernetycznym.

Wnioskodawcy projektując proponowany kierunek studiów będą korzystać z doświadczeń w instytucji międzynarodowych (od instytucji zajmujących się bezpieczeństwem cybernetycznym do bezpieczeństwa placówek zagranicznych).

**Projekt planowanych studiów będzie miał również zaplecze technologiczne i biznesowe w postaci CRI spółce typu spin-off, które jest pierwszym podmiotem gospodarczym działającym na Uniwersytecie Warszawskim na wydziale społecznym i jedynym zajmującym się komercjalizacją wiedzy z zakresu rafinacji dużych zasobów danych (głównie nieustrukturyzowanych).**

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, metoda grywalizacji, 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. Wsparciem metod nauczania tradycyjnego będzie również wykorzystanie nowoczesnych technologii (https://kampus-student2.ckc.uw.edu.pl/ platforma Kampus UW) i oprogramowania informatycznego do poszczególnych przedmiotów.

1. **kompetencje wymagane od kandydatów na studia (w przypadku studiów II stopnia należy wskazać kierunki studiów lub dyscypliny, do których przyporządkowano kierunki studiów będące źródłem rekrutacji na projektowany kierunek studiów)**

Oferta studiów I stopnia skierowana będzie do wszystkich uczniów, którzy ukończyli szkołę ponadpodstawową zdali egzamin maturalny i otrzymali świadectwo dojrzałości.

Podstawą przyjęcia na studia są wyniki lub ocena z języka obcego nowożytnego oraz wyniki lub ocena z dwóch przedmiotów, spośród przewidzianych w warunkach rekrutacji na określony kierunek studiów, które po stosownym przeliczeniu pozwolą osiągnąć kandydatowi najwyższą liczbę punktów.

**Przedmioty stanowiące podstawę rekrutacji na studia:**

* Geografia
* Historia
* Wiedza o społeczeństwie
* Matematyka
* Informatyka
1. **sylwetka absolwenta – kompetencje (w zakresie wiedzy, umiejętności i postaw społecznych), miejsce na rynku pracy oraz możliwości dalszego uczenia się absolwenta projektowanego kierunku studiów**

**Absolwenci kierunku będą posiadać wiedzę w następujących obszarach:**

* praktycznego zastosowania technologii związanych z  bezpieczeństwem cybernetycznym i wymogów ochrony danych w celu zabezpieczania działalności podmiotów gospodarczych i instytucji publicznych,
* związanych z bezpieczeństwem cybernetycznym takich jak między innymi: bezpieczeństwo aplikacji internetowych, systemów komputerowych i sieci, oprogramowania,
* na temat zasad działania podstawowych narzędzi, technik kryptograficznych i kryptoanalizy,
* z zakresu IT - inżynierii komputerowej, informatyki, technologii informacyjnych,
* interdyscyplinarną w zakresie innych zagadnień przekrojowych - ekonomii, polityki, zarządzania ryzykiem, czy etyki,
* na temat regulacji prawnych związanych z bezpieczeństwem cybernetycznym i zapewnianiem ochrony danych,
* w zakresie funkcjonowania krajowego systemu bezpieczeństwa cybernetycznego i rozwiązań międzynarodowych w tym zakresie.

**Absolwenci kierunku będą posiadać umiejętności w następujących obszarach:**

* tworzenia, projektowania systemów bezpieczeństwa cybernetycznego dla podmiotów publicznych i  prywatnych z użyciem najnowocześniejszych narzędzi informatycznych,
* analizy i zabezpieczania systemów informatycznych pod kątem podatności na ataki,
* skutecznego oceniania zabezpieczenia systemów informatycznych w zakresie zgodności z  aktualnymi aktami prawnymi oraz normami międzynarodowymi,
* wdrażania systemu zarządzania bezpieczeństwem informacji (w tym szczególnie umiejętności szacowania ryzyka),
* używania zaawansowanych technik kryptograficznych w tym algorytmów uwierzytelniających, autoryzacyjnych i szyfrujących,
* pracowania indywidualnie i w zespole, planowania pracy, a także komunikowania się przy użyciu technik właściwych dla branży IT w szczególności w sektorze bezpieczeństwa cybernetycznego.

**Absolwenci kierunku będą posiadać kompetencje społeczne w następujących obszarach:**

* rozumienia potrzeby krytycznej oceny posiadanej wiedzy oraz ciągłego dokształcania w  szczególności w branży IT związanej z bezpieczeństwem cybernetycznym,
* współpracy i działania w grupie współpracowników,
* myślenia i działania w sposób przedsiębiorczy,
* przestrzegania zasady etyki zawodowej w branży związanej z bezpieczeństwem cybernetycznym funkcjonowania w podmiotach sektora prywatnego i publicznego związanych z zapewnieniem bezpieczeństwa cybernetycznego,
* świadomości jak wdrożenie rozwiązań związanych z bezpieczeństwem cybernetycznym wpływa na społeczne i polityczne funkcjonowanie otoczenia gospodarczego.

**PERSPEKTYWY ZAWODOWE**

Absolwenci tego kierunku będą przygotowani do pracy w obszarze zarządzania bezpieczeństwem cybernetycznym oraz dziedzin pokrewnych zarówno w organizacjach sektora publicznego w tym w rządowej i  samorządowej administracji publicznej, jak i prywatnego, a także w instytucjach Unii Europejskiej zajmujących się aspektami bezpieczeństwa państwa jako audytorzy, analitycy, doradcy, specjaliści i  menedżerowie a także testerzy czy administratorzy sieci komputerowych posiadający fachową i  ekspercką wiedzę. Dodatkowo mogą pracować na uczelniach, w instytutach badawczych, biurach projektowych i innych instytucjach zaangażowanych w projektowanie systemów informatycznych.

1. **uzasadnienie wyboru poziomu kształcenia, profilu studiów, proponowanych limitów przyjęć (minimalna i maksymalna liczba) na I rok studiów**

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 I stopnia 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.

Studenci studiów I stopnia będą mieli możliwość realizacji własnych projektów i prowadzenia badań w zakresie bezpieczeństwa cybernetycznego przy wykorzystaniu potencjału informatycznego i doświadczenia projektowego pracowników KTI oraz Centrum Rafinacji Informacji (CRI) - spin-off UW, z którym ściśle współpracuje KTI[[6]](#footnote-6). Wśród założycieli CRI są pracownicy KTI.

Zakładane limity studentów na studiach I 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.

 **Uzasadnienie utworzenia nowego kierunku studiów odnoszące się do dotychczasowej oferty studiów Uniwersytetu Warszawskiego oraz doświadczeń innych uczelni krajowych i zagranicznych.**

Analizę oferty edukacyjnej Uniwersytetu Warszawskiego wykonano na podstawie danych zawartych w  systemie RAD-on[[7]](#footnote-7). Uczelnia w swojej ofercie nie posiada kierunku, którego treści programowe byłyby poświęcone w całości bezpieczeństwu cybernetycznemu. Wybrane zagadnienia z zakresu bezpieczeństwa cybernetycznego 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.[[8]](#footnote-8) 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 bezpieczeństwa cybernetycznego dla wszystkich studentów, również dla tych, którzy nie mają możliwości wyboru płatnych studiów.

 Zgodnie z informacjami zawartymi w systemie RAD-on, studia na kierunku cyberbezpieczeństwo oferuje sześć uczelni w Polsce (Tabela 1). Trzy z nich proponują studia pierwszego i drugiego stopnia, dwie tylko studia pierwszego stopnia a jedna tylko studia drugiego stopnia. 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.

Na potrzeby opracowania nowego programu studiów dokonano przeglądu dostępnych a 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 ich ofertach programowych zostały skonfrontowane z proponowanym programem studiów nowego kierunku.

Na uwagę zasługuje również fakt, że znaczna część kierunków studiów z Tabeli 1 została uruchomiona w ostatnich pięciu latach – z wyjątkiem kierunku na studiach pierwszego stopnia Wojskowej Akademii Technicznej. Świadczy to o rosnącej w ostatnich latach potrzebie kształcenia specjalistów z zakresu cyberbezpieczeństwa.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp** | **Nazwa kierunku studiów** | **Instytucja prowadząca** | **Poziom** | **Dyscypliny** | **Data uruchomienia** |
| 1 | Bezpieczeństwo informacyjne i cyberbezpieczeństwo | Akademia Sztuki Wojennej | pierwszego stopnia | nauki o bezpieczeństwie (100%) | 2021-10-01 |
| 2 | Cyberbezpieczeństwo | Akademia Górniczo-Hutnicza  | pierwszego stopnia | informatyka techniczna i telekomunikacja (100%) | 2019-10-01 |
| 3 | Cyberbezpieczeństwo | Politechnika Warszawska | pierwszego stopnia | informatyka techniczna i telekomunikacja (100%) | 2019-10-01 |
| 4 | Cyberbezpieczeństwo | Politechnika Wrocławska | pierwszego stopnia | informatyka techniczna i telekomunikacja (100%) | 2017-10-01 |
| 5 | Kryptologia i cyberbezpieczeństwo | Wojskowa Akademia Techniczna | pierwszego stopnia | informatyka techniczna i telekomunikacja (100%) | 2014-10-01 |

Analizę uczelni zagranicznych oferujących studia pierwszego 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.[[9]](#footnote-9) W zasobach platformy, na stronie [[10]](#footnote-10) w dyscyplinie Cyber Security, zamieszczone są 390 oferty studiów, 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 bezpieczeństwem cybernetycznym, cyberbezpieczeństwo i zapewnienie informacji, cyberbezpieczeństwo i kryminalistyka cyfrowa i inne..

Analiza dostępnych na platformie ofert programowych pozwoliła na sformułowanie głównych obszarów tematycznych w zakresie bezpieczeństwa cybernetycznego, które mogą być podstawą do tworzenia siatki przedmiotów realizowanych w trakcie studiów 1 stopnia

* Tworzenie oprogramowania
* Systemy komputerowe i operacyjne
* Bazy danych
* Cyfrowa kryminalistyka
* Testowanie bezpieczeństwa
* Bezpieczne tworzenie oprogramowania
* Bezpieczne przetwarzania w chmurze
* Zarządzanie ryzykiem cybernetycznym, zarządzanie bezpieczeństwem, aspekty prawne związane z bezpieczeństwem cybernetycznym
* Kryptografia, kryminalistyka
* Bezpieczeństwo urządzeń mobilnych i sieci bezprzewodowych
* Bezpieczeństwo społeczne

**Przeprowadzona analiza była punktem wyjścia do sformułowania nowego programu studiów.**

**Uzasadnienie utworzenia nowego kierunku studiów odnoszące się do potrzeb otoczenia społeczno-gospodarczego i studentów udokumentowane wynikami badań lub efektami przeprowadzonego rozeznania.**

W celu zbadania stopnia zainteresowania uczniów nowo tworzonym kierunkiem studiów I stopnia, przeprowadzono ankietę wśród uczniów szkół ponadpodstawowych. W badaniu wzięło udział 240 osób[[11]](#footnote-11), w tym 125 kobiet i 115 mężczyzn. Większość badanych osób (41,3%) to osoby mieszkające w miastach powyżej 500 tys. mieszkańców. Większość badanych osób (56,4%) to uczniowie liceum ogólnokształcącego natomiast (43,6%) osób to uczniowie technikum.

Wyniki ankiety jednoznacznie wskazują, że uczniowie postrzegają zawód specjalisty ds. cyberbezpieczeństwa jako atrakcyjny i przyszłościowy (72,1% badanych). Na pytanie, czy zdecydowaliby się na wybór kierunku Cyberbezpieczństwo, gdyby ten znalazłby się w ofercie studiów, aż 46,9% respondentów odpowiedziało twierdząco (Wykres 2).

**Wykres 2. Zainteresowanie uczniów nowym kierunkiem studiów I stopnia**



*Źródło: Badanie własne.*

W zawodzie specjalisty ds. bezpieczeństwa chciałoby pracować 43,6% badanych (Wykres 3)

**Wykres 3. Zainteresowanie uczniów pracą w zawodzie specjalisty ds. bezpieczeństwa**



*Źródło: Badanie własne*

Pytania w ankiecie dotyczyły również wyboru rodzaju studiów z zakresu cyberbezpieczeństwa. Znaczna część badanych - 66,8% wybrałaby studia dzienne.

Przeprowadzona ankieta dowiodła, że projektowany kierunek studiów I stopnia doskonale wpisuje się w oczekiwania uczniów Na podstawie uzyskanych wyników można założyć, że będzie chętnie wybieranym kierunkiem studiów.

W celu przeprowadzenia rozeznania potrzeb/oczekiwań otoczenia społeczno-gospodarczego zwrócono się do Komitetu Interesariuszy WNPiSM oraz firm i instytucji o udzielenie rekomendacji w sprawie utworzenia nowego kierunku studiów I stopnia w zakresie cyberbezpieczeństwa.

Ponieważ termin złożenia wniosku do Uniwersyteckiej Rady ds. Kształcenia upływa 31 maja – trwa proces pozyskiwania rekomendacji.

Załącznik 1 – Komitet Interesariuszy WNPiSM

Załącznik 2 – Urząd Komunikacji Elektronicznej

Załącznik 3 – Polskie Badania Internetu

Załącznik 4 – Heilderberg Polska

Załącznik 5 – Dagma Bezpieczeństwo IT – w przygotowaniu

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

Nauczyciele akademiccy Uniwersytetu Warszawskiego przewidywani do kształcenia na projektowanym kierunku studiów:

|  |
| --- |
| **prof. dr hab. Stanisław Sulowski** |
| profesor zwyczajny (2018). Dziekan Wydziału Nauk Politycznych i Studiów Międzynarodowych w latach 2016-2020. Politolog, absolwent Instytutu Nauk Politycznych UW (1975). Profesor Uniwersytetu Warszawskiego, do 2016 r. dyrektor Instytutu Nauk Politycznych Uniwersytetu Warszawskiego. Od 2010 roku kieruje Ośrodkiem Analiz Politologicznych UW. Redaktor naczelny kwartalnika Studia Politologiczne, redaktor serii wydawniczej w Peter Lang Verlag: Studies in Politics, Security and Society. Członek Komitetu Nauk Politycznych Polskiej Akademii Nauk. Konsul RP w Niemczech w latach 1991-1995. Członek Rady Programowej Center Francais de Berlin w Berlinie. Współzałożyciel Red Hispano Polca de Investigación Científica. |
| **Zainteresowania badawcze** |
| Administracja publiczna, ustrój polityczno-administracyjny Niemiec, teoria państwa, polityka zagraniczna, nauki o bezpieczeństwie. |

|  |
| --- |
| **dr hab. inż. Wiesław Cetera, prof. Ucz.** |
| Absolwent Wydziału Cybernetyki WAT, doktor nauk ekonomicznych w zakresie zarządzania (WZ UW), doktor habilitowany w zakresie nauk o mediach i komunikacji, pracownik naukowo-dydaktyczny Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. Założyciel i redaktor naczelny jednego z pierwszych czasopism informatycznych. Dziennikarz, menedżer przedsiębiorstw w sektorze poligraficznym. |
| **Zainteresowania badawcze** |
| Wykorzystanie dużych zasobów danych w analityce społecznej. |

|  |
| --- |
| **dr hab. Grzegorz Gudzbeler, prof. ucz** |
| Doktor habilitowany nauk o bezpieczeństwie, adiunkt. W latach 2013-2017 Dyrektor Instytutu Koordynacji Badań i Rozwoju Wyższej Szkoły Policji w Szczytnie. W latach 2013-2016 członek Rady Naukowo-Technicznej przy MSW. W latach 2014-2015 członek zespołu eksperckiego programu strategicznego „Satelitarny system optoelektronicznej obserwacji Ziemi” Narodowego Centrum Badań i Rozwoju i Polskiej Agencji Kosmicznej. Uczestnik 66 projektów naukowych, badawczo-rozwojowych i zadań projektowych o charakterze krajowym i międzynarodowym w charakterze wykonawcy, kierownika, koordynatora. Użytkownik końcowy wielu projektów europejskich oraz członek komitetów sterujących konsorcjów naukowo-przemysłowych. Autor ponad 40 publikacji i komunikatów naukowych w obszarze bezpieczeństwa, symulacji komputerowej, cyberprzestępczości i wsparcia technicznego działań o charakterze kryzysowym wydawanych m.in. w USA, Chinach, Hongkongu, Australii. Uczestnik jedenastu staży zagranicznych m.in. w Instituto Superior de Ciencias Policiaia e Seguranca Interna w Lisbonie. Były zastępca redaktora naczelnego Internal Security Journal (ISSN:20805268). Członek Międzynarodowego Stowarzyszenia Inżynierów – IAENG oraz NDIA (National Defence Industrial Association). |
| **Zainteresowania badawcze** |
| Zarządzanie kryzysowe, logistyka zarządzania kryzysowego, technologie bezpieczeństwa, ochrona informacji niejawnych, cyberprzestępczość i cyberterroryzm, bezpieczeństwo imprez masowych. |

|  |
| --- |
| **dr inż. Dariusz Jaruga** |
| Doktor nauk społecznych w dyscyplinie nauki o komunikacji społecznej i mediach (2019); Absolwent Wydziału Mechatroniki Politechniki Warszawskiej. Od 2022 Pracownik naukowo-dydaktyczny Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. Pracownik naukowo-dydaktyczny Wydziału Dziennikarstwa, Informacji i Bibliologii Uniwersytetu Warszawskiego (2015-2021); Współpracownik dydaktyczny na Wydziale Dziennikarstwa i Nauk Politycznych (2002 – 2015). Pełnomocnik Dziekana Wydziału Dziennikarstwa, Informacji i Bibliologii ds. ochrony danych osobowych (w latach 2016 – 2021). Jest współtwórcą studiów Zarządzanie Big Data na UW. Brał udział w dwóch projektach NCBIR z zakresu B+R+I i trendów technologicznych. Aktualnie członek zespołu w projekcie: „Identyfikacja, kolekcjonowanie i ocena nieprzyjaznych operacji dezinformacyjnych w cyberprzestrzeni, prowadzonych w oparciu o narzędzia teleinformatyczne (IKONA)”. Doświadczenie zawodowe zdobywał także w Polskiej Agencji Prasowej i Szkole Głównej Handlowej w Warszawie. |
| **Zainteresowania badawcze** |
| Rafinacja informacji, tworzenie aplikacji badawczych do kolekcjonowania danych na potrzeby rafinacji, przetwarzanie danych big data jako wartościowego źródła informacji wtórnej, systemy operacyjne, usługi sieciowe, relacyjne i nierelacyjne bazy danych, nowe media, programowanie, bezpieczeństwo IT. |

|  |
| --- |
| **dr Piotr Potejko** |
| Piotr Potejko posiada ponad 25-letnie doświadczenie w dziedzinie bezpieczeństwa. Były oficer ABW w stopniu pułkownika. Jego wcześniejsza kariera zawodowa związana była przede wszystkich z tworzeniem strategii bezpieczeństwa, ochroną informacji niejawnych, czy szkoleniem funkcjonariuszy służb specjalnych na całym świecie. Pełnił m.in. funkcję Dyrektora Departamentu Ochrony Informacji Niejawnych ABW, gdzie odpowiadał za ochronę informacji krajowych, jak i zagranicznych UE/NATO w administracji i biznesie, a także Dyrektora Centralnego Ośrodka Szkolenia ABW, sprawując nadzór nad organizacją systemu szkoleń dla cywilnych służb specjalnych wywiadu i kontrwywiadu RP. Jako członek Komitetu Sterującego Narodowego Centrum Badań i Rozwoju wspierał działania organów administracji państwowej w zakresie realizacji strategicznych i międzynarodowych kwestii bezpieczeństwa oraz międzynarodowych projektów związanych z badaniami na rzecz bezpieczeństwa i obronności w polskiej gospodarce. Jest specjalistą w zakresie organizacji i wdrażania systemów bezpieczeństwa, zarządzania zidentyfikowanymi sytuacjami kryzysowymi i terrorystycznymi. W trakcie pracy zawodowej specjalizuje się dodatkowo w zarządzaniu jakością w administracji oraz wdrażaniem bezpieczeństwa przemysłowego. Zajmuje się praktycznym przygotowaniem specjalistów w zakresie bezpieczeństwa w administracji i biznesie, utrzymania porządku publicznego oraz prowadzeniem wykładów o tematyce cyberbezpieczeństwa, służb specjalnych, dezinformacji oraz pozyskiwania informacji. Uczestnik prac komisji sejmowej nad nowelizacją Ustawy o ochronie informacji niejawnych. Uczestnik prac Sejmowej Komisji Spraw Zagranicznych w sprawie umów międzynarodowych w zakresie bezpieczeństwa informacji. Przedstawiciel Prezesa Rady Ministrów w zakresie procedowania i parafowania umów międzypaństwowych oraz przedstawiciel strony polskiej w posiedzeniach Komitetu Bezpieczeństwa NATO i Unii Europejskiej w Brukseli. Kontroler i ekspert w zakresie bezpieczeństwa informacji w polskich przedstawicielstwach dyplomatycznych. Pomysłodawca i realizujący pięć międzynarodowych projektów z zakresu bezpieczeństwa wewnętrznego i międzynarodowego oraz kryminalistyki. Redaktor naczelny „Przeglądu bezpieczeństwa wewnętrznego” a także Zastępca Szefa Instytutu Bezpieczeństwa Wewnętrznego w Poznaniu oraz współzałożyciel honorowy ogólnopolskiego Stowarzyszenia Wspierania Bezpieczeństwa Narodowego. |
| **Zainteresowania badawcze** |
| bezpieczeństwo wewnętrzne i międzynarodowe; służby specjalne we współczesnym państwie; organizacja i wdrażanie systemów bezpieczeństwa; zarządzanie sytuacjami kryzysowymi i terrorystycznymi; zarządzanie jakością w administracji; cyberbezpieczeństwo; dezinformacja oraz pozyskiwanie informacji; bezpieczeństwo informacji w biznesie; ochrona informacji niejawnych, danych osobowych i tajemnic prawnie chronionych; kryminalistyka. |

|  |
| --- |
| **dr inż. Bartłomiej Moszoro** |
| doktor nauk ekonomicznych (2007); pracownik dydaktyczny Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego; menedżer w NGO w kulturze i oświacie; 2007-2013 – pracownik naukowo-dydaktyczny w Katedrze Zarządzania Przedsiębiorstwami Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie; 1996-2001 – studia na Wydziale Zarządzania na Akademii Górniczo-Hutniczej w Krakowie; szkoła średnia i podstawowa w Rosario (Argentyna). |
| **Zainteresowania badawcze** |
| Innowacje, nowoczesna organizacja, modele biznesowe, VUCA, Human-Centered design, zarządzanie ludźmi w cyfrowej i post-pandemicznej transformacji |

|  |
| --- |
| **dr Paweł Kuczma** |
| Doktor nauk humanistycznych w zakresie nauk o mediach (2016); pracownik dydaktyczny Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego; w latach 2009-2021 doktorant, współpracownik, a następnie pracownik Wydziału Dziennikarstwa i Nauk Politycznych oraz Wydziału Dziennikarstwa, Informacji i Bibliologii Uniwersytetu Warszawskiego.Autor i współautor kilku publikacji z zakresu danych, mediów społecznościowych i marketingu internetowego. Prelegent na krajowych i międzynarodowych konferencjach naukowych i branżowych m. in. w Duesseldorfie, Mannheim, Kolonii, Lublinie, czy Warszawie. Specjalista w zakresie marketingu online. Między 2009 a 2010 r. pracownik agencji mediowej Mediacom, w latach 2011-2018 związany z grupą mediową Dentsu a od 2018 roku właściciel agencji mediowej Pure Play. |
| **Zainteresowania badawcze** |
| Dane, otwarte dane, marketing, reklama online, media społecznościowe, fake newsy. |

|  |
| --- |
| **dr Agnieszka Heba** |
| doktor nauk społecznych w zakresie nauk pedagogiki o specjalności nowoczesne technologie w edukacji (2019, nagroda III stopnia Rektora MUP Oświęcim, Microsoft Innovative Educator Expert (2021/2022)); pracownik dydaktyczny Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego; 2019-2021 - pracownik dydaktyczny Wydziału Dziennikarstwa, Informacji i Bibliologii Uniwersytetu Warszawskiego. Aktualnie członek zespołu w projekcie: „Identyfikacja, kolekcjonowanie i ocena nieprzyjaznych operacji dezinformacyjnych w cyberprzestrzeni, prowadzonych w oparciu o narzędzia teleinformatyczne (IKONA)”. Doświadczenie zawodowe zdobywała również współpracując z Ostrawskim Uniwersytetem w Ostrawie w Republice Czeskiej, Uniwersytetem Śląskim w Katowicach, Uniwersytetem Kardynała Stefana Wyszyńskiego w Warszawie. W 2019 roku uzyskała certyfikat e-nauczyciela, e-metodyka przyznany przez Stowarzyszenie E-learningu Akademickiego. Autorka publikacji z zakresu nowoczesnych technologii w edukacji, w szczególności w nauczaniu matematyki. Uczestniczka stażu w Centrum Nauczania na Odległość w Pradze |
| **Zainteresowania badawcze** |
| Technologie informacyjne i komunikacyjne w edukacji, nowe media, serwisy internetowe, narzędzia komunikacji internetowej, text mining w R i Statistice, metody wizualizacji i analizy danych w R i Statistice. |

|  |
| --- |
| **dr Wioletta Matosek** |
| Doktor nauk ekonomicznych w zakresie nauk o zarządzaniu (2002, nagroda II stopnia Rektora UG); pracownik dydaktyczny Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego; 1995-2006 – pracownik naukowo-dydaktyczny w Katedrze Informatyki Ekonomicznej Uniwersytetu Gdańskiego; 2007-2018 - pracownik Narodowego Centrum Badań i Rozwoju, uczestnik procesów tworzenia podstaw funkcjonowania instytucji zarządzającej projektami B+R oraz projektowania i wdrażania rozwiązań informatycznych podnoszących sprawność działania instytucji. Autorka publikacji z zakresu baz danych i zastosowania technologii informatycznych w zarządzaniu. Prowadziła badania własne w National Laboratory for Civil Engineering oraz Institute for Systems and Computer Engineering w Lizbonie. |
| **Zainteresowania badawcze** |
| bazy danych, język SQL, systemy informatyczne w zarządzaniu, analiza i projektowanie systemów (UML), modelowanie procesów biznesowych (BPMN), serwisy internetowe, narzędzia komunikacji internetowej, marketing w Internecie, nowe media, text mining, programowanie w języku R, metody wizualizacji danych |

|  |
| --- |
| **mgr inż. Piotr Celiński** |
| Absolwent wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej. Od 2022 Pracownik naukowo-techniczny Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. Pracownik naukowo-techniczny Wydziału Dziennikarstwa, Informacji i Bibliologii Uniwersytetu Warszawskiego (2017-2021); Współpracownik dydaktyczny na Wydziale Dziennikarstwa i Nauk Politycznych (2002 – 2017). Współtwórca studiów Zarządzanie Big Data na UW. Współtwórca programu oraz wykładowca szkoły letniej dla studentów z Uniwersytetu w Chengdu (2019). Doświadczenie zawodowe zdobywał również w Polskiej Agencji Prasowej, Polskiej Akademii Nauk (Instytut Geofizyki, członek XVI wyprawy PAN do Polskiej Stacji Polarnej na Svalbardzie) oraz prowadząc własną działalność gospodarczą. |
| **Zainteresowania badawcze** |
| Akwizycja i kolekcjonowanie informacji na potrzeby analiz Big Data; przetwarzanie języka naturalnego; rafinacja informacji; analizy Big Data; wizualizacja danych; nowe media; technologie mobilne; programowanie; bezpieczeństwo IT. |

|  |
| --- |
| **mgr inż. Tomasz Pawlicki** |
| Magister inżynier telekomunikacji – teleinformatyka (1992, Wydział Elektroniki, PW); dyplom MBA (2007, Akademia Leona Koźmińskiego w Warszawie); studia doktoranckie w zakresie nauk o zarządzaniu (2008-2011, ALK); pracownik dydaktyczny Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego; 2016-2021 – współpracownik i pracownik badawczo-techniczny w Katedrze Technologii Informacyjnych Mediów, Wydziału Dziennikarstwa, Informacji i Bibliologii, UW; 1997-2018 dyrektor marketingu w firmie Heidelberg Polska.Członek Rady Programowej wielu konferencji naukowo-technicznych organizowanych przez Polską Izbę Druku, Centralny Ośrodek Badawczo-Rozwojowy Przemysłu Poligraficznego oraz Sekcję Poligrafów SIMP. Autor licznych artykułów w prasie branżowej. Członek Rady Fundacji Rozwoju Kadr Poligraficznych. Kawaler Polskiego Bractwa Kawalerów Gutenberga. |
| **Zainteresowania badawcze** |
| Systemy informatyczne w branży wydawniczej i poligraficznej, zarządzaniu, serwisy internetowe, narzędzia komunikacji internetowej, marketing tradycyjny i cyfrowy, nowe media, analiza zbiorów danych. |

**Pozostałe osiągnięcia naukowe i dydaktyczne kadry znajdują się w Załączniku – szczegółowe osiągnięcia naukowe i dydaktyczne kadry**

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

Do współpracy planuje się również zaproszenie innych osób związanych zawodowo z obszarem bezpieczeństwa cybernetycznego, w tym pracowników innych jednostek UW – Wydziału Matematyki, Informatyki i Mechaniki, a także pracowników innych uczelni oraz praktyków.

**Infrastruktura niezbędną do realizacji przedstawionej koncepcji kształcenia oraz wskazać jednostkę/jednostki, która/e ją zapewni/ą**

Gmach Audytoryjny WNPiSM składa się z pięciu kondygnacji. Na samym dole, w podpiwniczeniu znajdują się pracownie: komputerowa. Sala komputerowa jest wyposażona w 21 komputerów z 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.Na parterze budynku Audytoryjnego mieści się dwukondygnacyjna reprezentacyjna aula ze składaną trybuną mogąca pomieścić do 150 osób. Na tyłach trybun są dwie kabiny tłumaczy. Aula jest nowoczesna, wyposażona w sprzęt multimedialny, w panele akustyczne, system pętli indukcyjnej dla niesłyszących itp.

Sale dydaktyczne znajdują się na parterze, 1, 2 i 3 piętrze budynku (15 sal dydaktycznych z nowoczesnym wyposażeniem multimedialnym).

Na czwartym piętrze, m.in. do dyspozycji wykładowców zagranicznych prowadzących kursy i wykłady gościnne, znajdują się 4 pokoje gościnne. Wydział dysponuje również salami dydaktycznymi w budynkach sąsiadujących z kampusem głównym przy ul. Krakowskie Przedmieście 3 (4 sale dydaktyczne), Krakowskie Przedmieście 1 (1 sala), Nowy Świat 67 (2 sale), Nowy Świat 69 (1 sala), Dawny BUW (6 sal). Wydział nie prowadzi zajęć poza UW. Wydział posiada sieć lokalną. We wszystkich budynkach uniwersyteckich dostępna jest bezpłatna sieć wifi Edurom. Istnieje możliwość tworzenia czasowych sieci wifi do obsługi wydarzeń i konferencji organizowanych w budynku Wydziału. 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 (TIM-4), CPU: 16-Core Processor, Passmark 25471 (16 core)

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

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 Centrum Rafinacji Informacji (spin-off UW), 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 planowany jest zakup 25-ciu komputerów do kwerend danych oraz serwera wirtualnego. Zakupione komputery będą mogły być wykorzystane 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). Serwer wirtualny z systemem operacyjnym Linux zawierał będzie dedykowane do zajęć oprogramowanie i umożliwiał założenie konta dla każdego studenta na cały 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.

Studenci posiadają przez konto biblioteczne dostęp do zasobów Biblioteki Uniwersyteckiej (jednej z największych bibliotek naukowych w Polsce). Oprócz tradycyjnych zbiorów BUW zapewnia studentom szeroki dostęp do publikacji w wersji elektronicznej bazy czasopism i książek elektronicznych https://www.buw.uw.edu.pl/zasoby-online/. E-zbiory BUW obejmują ponad 100 baz z artykułami naukowymi. Bazy te są wykorzystywane przez studentów jako źródła w pracach dyplomowych oraz zaliczeniowych wymagających wykorzystania literatury naukowej. Oprócz BUW studenci korzystają również z zasobów Biblioteki Wydziałowej. Biblioteka WNPiSM mieści się przy ul. Nowy Świat 69. Znajduje się w niej 9 stanowisk komputerowych z dostępem do Internetu. Biblioteka WNPiSM jest jedną z największych bibliotek wydziałowych na UW, zarówno pod względem wykorzystania zbiorów, jak i frekwencji w czytelni.. Księgozbiór liczy ok. 75 tys. woluminów (książek i czasopism) oraz 815 prac doktorskich. Prenumeratą objętych jest 67 tytułów czasopism (w tym 5 tytułów czasopism zagranicznych – od 2012 roku wybrano opcję prenumeraty online czasopism zagranicznych). Z czasopism elektronicznych udostępnionych w sieci UW można również korzystać na stanowiskach komputerowych w Czytelni Biblioteki WNPiSM UW (9 stanowisk).

1. Wykazy projektów realizowanych obecnie na WNPiSM UW dostępne są na stronach: <https://wnpism.uw.edu.pl/realizowane-granty>,
<https://wnpism.uw.edu.pl/o-wydziale/struktura-wydzialu/katedra-technologii-informacyjnych>, dostęp [2022-05-04] [↑](#footnote-ref-1)
2. <https://wnpism.uw.edu.pl>, dostęp [2022-05-04] [↑](#footnote-ref-2)
3. <https://bazawiedzy.wnpism.uw.edu.pl/>, dostęp [2022-05-04] [↑](#footnote-ref-3)
4. <https://cyberpolicy.nask.pl/wytyczne-dla-programow-studiow-z-cyberbezpieczenstwa-cybersecurity-curricula-2017/>, dostęp [2022-04-14] [↑](#footnote-ref-4)
5. https://crn.pl/aktualnosci/zarobki-it-30-tys-zl-za-cyberbezpieczenstwo/ [↑](#footnote-ref-5)
6. <https://www.inforafinacja.pl>, dostęp [2022-05-04] [↑](#footnote-ref-6)
7. <https://radon.nauka.gov.pl/>, dostęp [2022-04-14] [↑](#footnote-ref-7)
8. <https://cybersecurity.mimuw.edu.pl/>, dostęp [2022-04-14] [↑](#footnote-ref-8)
9. <https://studyportals.com/>, dostęp [2022-04-14] [↑](#footnote-ref-9)
10. https://www.bachelorsportal.com/search/bachelor/it-security?dg=bsc,prebachelor [↑](#footnote-ref-10)
11. stan na 19.04.2022 r. [↑](#footnote-ref-11)